WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

WYDZIAŁ BEZPIECZEŃSTWA, LOGISTYKI I ZARZĄDZANIA

Rozprawa doktorska

Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej

Autor:
mgr Grzegorz Mąkosa

Promotor:
prof. dr hab. Bogusław Jagusiak

Warszawa 2023

Ta strona celowo pozostała pusta

Streszczenie rozprawy doktorskiej pt. „Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej”

Cyberbezpieczeństwo państwa to proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych, prawnych i nieposiadających osobowości prawnej, a także zasobów informacyjnych i systemów teleinformatycznych cyberprzestrzeni. Bezpieczeństwo państwa w cyberprzestrzeni jest zapewniane poprzez zorganizowany system bezpieczeństwa, adresujący właściwe aspekty każdego z sektorów bezpieczeństwa i cyberbezpieczeństwa, jako kategorii bezpieczeństwa transsektorowego.

Przedmiotem badań rozprawy jest organizacja systemu cyberbezpieczeństwa RP zdefiniowana przez regulacje prawne i dokumenty strategiczne bezpieczeństwa państwa, w zakresie: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania, doboru sektorów i typów podmiotów oraz wskazania norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. Celem głównym rozprawy jest opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa.

Dysertacja składa się ze wstępu, rozdziału metodologicznego, pięciu rozdziałów merytorycznych, podsumowania i zakończenia. Rozdział pierwszy jest poświęcony zagadnieniom metodologicznym. W rozdziale drugim przeprowadzono rozważania nad istotą i pojęciami bezpieczeństwa narodowego i cyberbezpieczeństwa, dokonano analizy aktualnego stanu bezpieczeństwa polskiej cyberprzestrzeni, a także analizy regulacji prawnych i dokumentów strategicznych bezpieczeństwa w kontekście cyberbezpieczeństwa. Rozdział trzeci poświęcono zagadnieniom zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, rozdział czwarty poświęcono zorganizowaniu struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, rozdział piąty adresuje zagadnienia doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa, rozdział szósty obejmuje zagadnienia rozwiązań normatywnych bezpieczeństwa teleinformatycznego podmiotów systemu cyberbezpieczeństwa. Podsumowanie prezentuje w skondensowanej formie przeprowadzone działania w ramach rozdziałów od drugiego do szóstego wraz z prezentacją opracowanych rozwiązań. Zakończenie zawiera wnioski podsumowujące oraz rekomendacje do podjęcia dalszych badań.

Summary of the doctoral dissertation entitled: The concept of improving the organization of the cybersecurity system of the Republic of Poland"

State cybersecurity is the process of ensuring the safe functioning of the state as a whole in cyberspace, its structures, natural and legal persons and persons without legal personality, as well as information resources and ICT systems in cyberspace. State security in cyberspace is ensured through an organized security system, addressing the relevant aspects of each of the security sectors and cybersecurity as a of trans-sector security category.

The subject of the dissertation's research is the organization of the cybersecurity system of the Republic of Poland, defined by legal regulations and strategic documents of state security, in the field of: organization of cybersecurity management at the national level, organization of management structures and operational relations, selection of sectors and types of entities, and indication of norms, methodologies and standards of ICT security management systems for entities of the cybersecurity system. The main aim of the dissertation is to develop a concept for the improvement of the organization of the cybersecurity system of the Republic of Poland in order to improve its efficiency and increase the security of the state.

The dissertation consists of an introduction, a methodological chapter, five substantive chapters, a summary and an ending. The first chapter is devoted to methodological issues. The second chapter discusses the essence and concepts of national security and cybersecurity, analyzes the actual state of security of Polish cyberspace, as well as analyzes legal regulations and security strategic documents in the context of cybersecurity. The third chapter is devoted to the issues of organizing cybersecurity management at the national level, the fourth chapter is devoted to the organization of structures and operational relations of cybersecurity management at the national level, the fifth chapter addresses the issues of the selection of sectors and types of cybersecurity system entities, the sixth chapter covers the issues of normative ICT security solutions for cybersecurity system entities. The summary presents in a condensed form the activities carried out within the framework of chapters two to six, together with the presentation of the developed solutions. The ending contains summary conclusions and recommendations for further research.

Spis treści

WSTĘP

Współcześnie bezpieczeństwo państwa w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej zyskało dodatkowy wymiar, jakim, obok lądu, wody, powietrza i przestrzeni kosmicznej, jest cyberprzestrzeń oraz dodatkowy sektor bezpieczeństwa, jakim jest cyberbezpieczeństwo. Cyberprzestrzeń jest przestrzenią przetwarzania i wymiany danych i informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami. Cyberbezpieczeństwo państwa to proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w cyberprzestrzeni[1]. Cyberbezpieczeństwo odnosi się do bezpiecznego funkcjonowania państwa, jego struktur administracyjnych, podmiotów gospodarczych i obywateli w cyberprzestrzeni. Można stwierdzić, że dotyczy bezpieczeństwa informacyjnego państwa w cyberprzestrzeni. Cyberbezpieczeństwo jako najnowsza i najbardziej wymagająca składowa bezpieczeństwa narodowego i międzynarodowego, będąc jednocześnie bezpieczeństwem transsektorowym, jest coraz istotniejszym jego komponentem, a zapewnienie jego odpowiednio wysokiego poziomu jest kluczowym wyzwaniem państwa.

Bezpieczeństwo państwa jest zapewniane poprzez zorganizowany system bezpieczeństwa, adresujący właściwe aspekty każdego z sektorów bezpieczeństwa, w tym cyberbezpieczeństwa jako kategorii bezpieczeństwa transsektorowego.

Kwestie cyberbezpieczeństwa i bezpieczeństwa teleinformatycznego usług, systemów teleinformatycznych i podmiotów są przedmiotem oddziaływania regulacji prawnych

[1] Doktryna cyberbezpieczeństwa RP, BBN, 2015

i dokumentów strategicznych bezpieczeństwa państwa. Rozwiązania organizacyjne zdefiniowane w regulacjach prawnych i dokumentach strategicznych bezpieczeństwa tworzą system cyberbepieczeństwa, czy też system zarządzania cyberbezpieczeństwem państwa. W ramach polskiego porządku prawnego i zarządzania strategicznego bezpieczeństwem narodowych zostały ustanowione stosowne dokumenty adresujące bezpośrednio i intencjonalnie lub łącznie z innymi zagadnieniami, kompleksowo lub w wąskim zakresie przedmiotową problematykę cyberbezpieczeństwa i bezpieczeństwa podmiotów i systemów teleinformatycznych. Najistotniejszymi w tym zakresie są: ustawa o krajowym systemie cyberbezpieczeństwa wraz z towarzyszącymi rozporządzeniami wykonawczymi - stanowiące krajowy system cyberbezpieczeństwa, ustawa o zarządzaniu kryzysowym wraz z towarzyszącymi rozporządzeniami wykonawczymi i dokumentami operacyjnymi -stanowiące system zarządzania kryzysowego oraz ustawa o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącym rozporządzeniem wykonawczym -stanowiące system informatyzacji podmiotów publicznych[2], stanowiące, każde w swoim zakresie, komponenty składowe systemu bezpieczeństwa i cyberbezpieczeństwa narodowego. Rozwiązania organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej, zdefiniowane przez ww. regulacje prawne, odnoszą się między innymi do kwestii: zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie zorganizowania, planowania i dokumentowania, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie planowania i dokumentowania oraz zapewnienia cyberbezpieczeństwa i zarządzania incydentami, doboru sektorów i typów podmiotów systemu oraz wymaganych norm, metodyk i standardów zarządzania bezpieczeństwem teleinformatycznym, w tym rozwiązań organizacyjnych i technicznych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Zagadnienia organizacji systemu cyberbezpieczeństwa RP w zakresie: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa, doboru norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu

[2] Sformułowania: system zarządzania kryzysowego, krajowy system cyberbezpieczeństwa i system informatyzacji publicznych zostały użyty przez autora w: Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych (2020), Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne (2020), Organizacja systemu cyberbezpieczeństwa RP (2020)

cyberbezpieczeństwa są przedmiotem zainteresowania badawczego autora oraz przedmiotem niniejszej rozprawy.

Wobec tak zdefiniowanego przedmiotu badań sformułowano główny problem badawczy i odnoszącą się do niego hipotezę główną, brzmiącą:

Organizacja systemu cyberbezpieczeństwa RP nie jest optymalnie zdefiniowana, co w praktyce przyczynia się do braku skoordynowanych zadań różnych organów państwa. Obecnie obowiązujące rozwiązania podsystemów bezpieczeństwa są niekompletne, niespójne, niejednorodne i rozdzielne, i nie mogą tym samym zapewnić odpowiedniego poziomu bezpieczeństwa państwa, a ich ujednolicenie, zharmonizowanie i usprawnienie może przyczynić się do poprawy efektywności systemu cyberbezpieczeństwa RP i tym samym zwiększenia poziomu bezpieczeństwa państwa.

Założonym celem głównym rozprawy jest:

Opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia poziomu bezpieczeństwa państwa.

Przyjęte podejście metodologiczne rozwiązania problemu badawczego dotyczącego przedmiotu badań wobec sformułowanej hipotezy i celu rozprawy ukształtowało strukturę pracy. Dysertacja składa się ze wstępu, rozdziału metodologicznego, pięciu rozdziałów merytorycznych i zakończenia oraz bibliografii, wykazu tabel, wykazu rysunków, wykazu załączników, wykazu suplementów i załączników oraz suplementu.

Rozdział pierwszy obejmuje metodologię badań, uzasadniono w nim podjęcie badań, określono cel główny badań i cele szczegółowe, przedmiot badań, główny problem badawczy i problemy szczegółowe oraz hipotezę główną i hipotezy pomocnicze oraz scharakteryzowano metody, techniki i narzędzia badawcze, przedstawiono organizację procesu badawczego, założenia i ograniczenia badawcze, a także dokonano krytycznej analizy literatury.

Rozdział drugi stanowi przeprowadzone w podrozdziałach rozważania nad istotą i pojęciami bezpieczeństwa narodowego oraz współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą. Poświęcono uwagę zagadnieniom teoretycznym i aktualnemu faktycznemu stanowi bezpieczeństwa polskiej cyberprzestrzeni w odniesieniu do wyzwań, zagrożeń i incydentów cyberbezpieczeństwa. Przeprowadzono rekonstrukcję regulacji prawnych i strategicznych dokumentów normatywnych i ich analizę w zakresie zagadnień systemu cyberbezpieczeństwa oraz omówiono szereg norm, metodyk i standardów zarządzania bezpieczeństwem informacji i bezpieczeństwa systemów teleinformatycznych. Rozdział

drugi stanowi odpowiedź na postawiony problem badawczy: *Jakie są aktualne kontekst, warunki i środowisko prawne, strategiczne i normatywno-standaryzacyjne systemu cyberbezpieczeństwa RP i czy ich rozpoznanie stanowić będzie podstawę opracowania koncepcji doskonalenia systemu cyberbezpieczeństwa RP?* W rozdziale tym poddano weryfikacji hipotezę pomocniczą stanowiącą synergię z postawionym problemem badawczym. Rozdział kończy podsumowanie i wnioski, odnoszące się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W rozdziale trzecim dokonano próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym - *Jaka jest aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić jej efektywność?* W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu rozwiązań zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa, dokonano analizy porównawczej rozwiązań, przedstawiono także wyniki przeprowadzonych badań własnych w tym zakresie i dokonano ich analizy oraz przedstawiono opracowaną autorską koncepcję zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym. W rozdziale poddano weryfikacji hipotezę pomocniczą stanowiącą synergię z postawionym problemem badawczym. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W rozdziale czwartym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego struktur i relacji operacyjnych w systemie cyberbezpieczeństwa na poziomie krajowym - *Jakie są aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić ich efektywność?* Dla realizacji tego celu przeprowadzono kompleksowy, metodologiczny proces badawczy - dokonano przeglądu struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa oraz dokonano analizy porównawczej rozwiązań. Przedstawiono wyniki przeprowadzonych badań własnych w tym zakresie i dokonano ich analizy oraz przedstawiono opracowaną autorską koncepcję struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym. Poddano weryfikacji hipotezę pomocniczą powiązaną z postawionym problemem badawczym. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W rozdziale piątym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa - *Jakie sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP i jakie powinny zostać nim objęte, aby zapewnić jego efektywność i odpowiedni poziom bezpieczeństwa kraju?* W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu systemów, sektorów i typów podmiotów w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych, a także dokonano ich analizy porównawczej. Przedstawiono wyniki przeprowadzonych badań własnych w tym zakresie i dokonano ich analizy oraz przedstawiono opracowaną autorską koncepcję wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP. W rozdziale tym poddano weryfikacji hipotezę pomocniczą powiązaną z postawionym problemem badawczym. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W rozdziale szóstym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa - *Jakie międzynarodowe i krajowe normy, metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych są aktualnie wymagane i jakie powinny zostać wskazane do stosowania, aby zapewnić odpowiedni poziom bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP?* W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy. Dokonano przeglądu rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych oraz dokonano ich analizy porównawczej. Przedstawiono wyniki przeprowadzonych badań własnych w tym zakresie i dokonano ich analizy oraz przedstawiono opracowaną autorską koncepcję wykazu norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. W rozdziale poddano weryfikacji hipotezę pomocniczą stanowiącą synergię z postawionym problemem badawczym. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

Podsumowanie streszcza założenia metodologiczne rozprawy, prezentuje w skondensowanej formie przeprowadzone przez autora działania procesu badawczego w ramach

rozdziałów od drugiego do szóstego wraz z prezentacją opracowanych rozwiązań koncepcyjnych. W podsumowaniu przedstawiono aktualną strukturę i model krajowego systemu cyberbezpieczeństwa RP oraz strukturę i model koncepcji systemu cyberbezpieczeństwa RP.

W zakończeniu rozprawy przedstawiono syntezę wniosków z poszczególnych rozdziałów oraz nakreślono kierunki i rekomendacje do podjęcia dalszych badań. Podsumowano przeprowadzony proces badawczy, jego cel i efekty oraz określono wkład niniejszej rozprawy do nauk o bezpieczeństwie i jej wartość utylitarną.

Praca zawiera załączniki, którymi są: arkusz kwestionariusza wywiadu eksperckiego oraz zestawienia zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze. Praca zawiera suplement, na który składają się: arkusz kwestionariusza wywiadu eksperckiego, zestawienia zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze oraz zbiór arkuszy kwestionariusza wywiadu eksperckiego z odpowiedziami respondentów.

Rozdział I. METODOLOGICZNE PODSTAWY BADAŃ

1.1. Uzasadnienie podjęcia badań

Współcześnie bezpieczeństwo państwa w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej zyskało dodatkowy wymiar, jakim, obok lądu, wody, powietrza i przestrzeni kosmicznej, jest cyberprzestrzeń oraz dodatkowy sektor bezpieczeństwa, jakim jest cyberbezpieczeństwo.

Postępująca globalizacja i integracja, rozwój społeczeństwa informacyjnego i technologii teleinformatycznych zmieniły obecne środowisko bezpieczeństwa państw, w tym również Rzeczypospolitej Polskiej. Rozwój technologii teleinformatycznych korzystnie wpływa na rozwój społeczeństwa informacyjnego oraz rozwój gospodarczy. Niestety wpływa również na rozwój negatywnych zjawisk w cyberprzestrzeni, tj. cyberprzestępczości, cyberkonfliktów, cyberwalki, walki informacyjnej, czy cyberwojny. Postęp w teleinformatyce sprawił, że piąty wymiar konfrontacji, którym jest cyberprzestrzeń, nie tylko przyczynia się do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa. Ciągły rozwój technologii sprawia, że cyberataki są coraz bardziej wysublimowane, przyjmują nowe formy i są kierowane w coraz to nowsze obszary funkcjonalne otoczenia administracyjno-społeczno-gospodarczego państwa. Wyzwaniem jest więc stałe utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa. Warunkiem zapewniającym ciągłe utrzymywanie inicjatywy na poziomie strategicznym zarządzania bezpieczeństwem państwa jest przewaga informacyjna, która ma bezpośrednie przełożenie na koncepcje doktrynalne odnoszące się do infrastruktury cywilnej i wojskowej systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych[3]. Bezpieczeństwo informacyjne bywa określane jako zakres bezpieczeństwa przyjmujący wzrost znaczenia informacji w zachowaniu

[3] Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013, s. 447, 453, 460

stabilności współczesnych, międzynarodowych systemów ekonomicznych oraz uwzględniający zabezpieczenie przed atakami sieciowymi, a także skutkami ataków fizycznych i jest plasowane obok bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego i ekologicznego[4]. Bezpieczeństwo informacyjne staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej[5]. Sektory te mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej[6], realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[7], są realizowane w celu ochrony interesu publicznego[8].

Kwestie cyberbezpieczeństwa jako aspektu bezpieczeństwa narodowego, mającego coraz większy wpływ oraz coraz większy stopień dynamicznych zmian i skomplikowania technologicznego, stanowią istotne wyzwanie nie tylko na poziomie poszczególnych krajów, ale także na poziomie europejskim, np. w Unii Europejskiej. Kwestia zapewnienia bezpieczeństwa informacyjnego i cyberbezpieczeństwa jest przede wszystkim odpowiedzialnością i domeną państwa. Właściwe organy RP opracowały i wdrożyły dokumenty poziomu strategicznego i operacyjnego właściwe dla zapewnienia cyberbezpieczeństwa państwa i tworzące jego system cyberbezpieczeństwa. Dokumenty te wyznaczają strategiczną perspektywę, punkty odniesienia i ramy cyberbezpieczeństwa, a także cele i zadania do osiągnięcia odpowiedniego jego poziomu. Kwestie cyberbezpieczeństwa, z racji swojego znaczenia dla bezpieczeństwa państwa, są przedmiotem zainteresowania i wpływu regulacji prawnych, w tym, w szczególny sposób, ustawy o zarządzaniu kryzysowym, ustawy o krajowym systemie cyberbezpieczeństwa i ustawy o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącymi im aktami wykonawczymi i pomocniczymi (rozporządzeniami i dokumentami powstałymi na ich mocy). Regulacje prawne definiują zagadnienia cyberbezpieczeństwa, podmioty zaangażowane oraz ich odpowiedzialność, przedmiot zainteresowania danej regulacji oraz aspekty organizacyjne i struktury funkcjonowania

[4] Kowalkowski S. (red.) Niemilitarne zagrożenia bezpieczeństwa publicznego, AON, Warszawa 2011, s. 13, 14, 15
[5] Liderman K., B*ezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 23
[6] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560
[7] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 poz. 590
[8] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565

systemu cyberbezpieczeństwa[9]. Definiują również wymagania wobec podmiotów nimi objętych dotyczące wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa[10]. Wskazane powyżej regulacje prawne odnoszą się w pewnym zakresie - każda w innym - do kwestii cyberbezpieczeństwa, czy bezpieczeństwa systemów teleinformatycznych, niemniej obejmują one swoim zakresem sektory podległych podmiotów. Objęte regulacjami sektory i usługi mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej[11], realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[12], są realizowane w celu ochrony interesu publicznego[13].

Rozwiązania organizacji cyberbezpieczeństwa zawarte w ww. regulacjach prawnych, w toku badań autora nad nimi, wykazały znaczne równice w wielu istotnych obszarach, począwszy od organizacji bezpieczeństwa na poziomie krajowym, poprzez modele struktur i procesów organizowania, komunikowania i zarządzania incydentami i sytuacjami kryzysowymi związanymi z cyberbezpieczeństwem oraz zakres objętych nimi systemów i sektorów, i zaliczanych do nich podmiotów, aż do niejednolitych wymagań, co do norm i standardów mających służyć wdrożeniu systemu zarządzania i rozwiązań organizacyjnych i technicznych bezpieczeństwa systemów teleinformatycznych przez podmioty objęte przedmiotowymi regulacjami.

Bezpieczeństwo państwa wymaga nowych rozwiązań w zakresie bezpieczeństwa, w tym efektywnego systemu cyberbezpieczeństwa. Wyniki badań prowadzonych i zaprezentowanych w ramach niniejszej dysertacji mogą stanowić wkład i propozycję rozwiązań koncepcyjnych, których zastosowanie może przyczynić się do poprawy efektywności polskiego systemu cyberbezpieczeństwa i tym samym zwiększenia bezpieczeństwa państwa.

---

[9] Mąkosa G., *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 109

[10] Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, w: Studia Bezpieczeństwa Narodowego, 2020, 17(1), WAT, Warszawa 2020 s. 139

[11] adresowane przez Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

[12] adresowane przez Ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590

[13] adresowane przez Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

Należy stwierdzić, że istnieje uzasadniona potrzeba dokonania badań przedmiotowej problematyki dla zrealizowania celów poznawczych i utylitarnych przyjętych dla prowadzonej przez autora dysertacji.

1.2. Cel badań

Badania naukowe w obszarze bezpieczeństwa państwa, ze względu na rozległość powiązań strukturalno-funkcjonalnych oraz prawnych ograniczeń działających w niej systemów, są wielowymiarowe i często skomplikowane. Ich wieloaspektowość wynika ze złożoności i różnorodności tych systemów, które charakteryzują się:

- wielofunkcyjnością wynikającą z faktu, że ze względu na zasady bezpieczeństwa formułuje się zbiory różnych wymagań, które grupuje się stosownie do obszaru przyszłego, planowanego funkcjonowania systemów;
- złożonością struktury systemów działania (organizacji, instytucji, państwa);
- dużą liczbą podsystemów wchodzących w skład badanych systemów, pozostających w różnych relacjach (stosunkach, sprzężeniach) oraz dużą liczbą wielorakich relacji z bliższym i dalszym otoczeniem;
- dużym zasięgiem przestrzennym systemów, brakiem jednoznaczności;
- rozproszonym systemem sterowania procesami informacyjno-decyzyjnymi (np. wiele ośrodków decyzyjnych, brak jasnego zakresu odpowiedzialności, itp.);
- dynamiką procesów stosunków międzynarodowych.

Dlatego podjęte w rozprawie badania wymagają ograniczenia i mają zapewnić osiągnięcie typowych celów eksploracji, a mianowicie:

- zaspokojenia ciekawości badacza i jego pragnienia lepszego poznania przedmiotu badań;
- zbadania możliwości podjęcia szerszych kolejnych badań;
- wypracowania metod, narzędzi i technik, które posłużą do prowadzenia dalszych badań tego zagadnienia.

W ramach prowadzonego procesu badawczego określony został cel główny rozprawy.

Celem głównym prowadzonych badań jest opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia poziomu bezpieczeństwa państwa.

Ze sformułowanego celu głównego wynikają cele szczegółowe:

1. *Ukazanie uwarunkowań i środowiska systemu cyberbezpieczeństwa RP poprzez przedstawienie istoty i roli cyberbezpieczeństwa w systemie bezpieczeństwa narodowego, zrekonstruowanie obowiązujących przepisów prawnych i strategicznych dokumentów normatywnych w sposób formalny definiujących organizację systemu cyberbezpieczeństwa RP oraz rozpoznanie międzynarodowych i krajowych norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych, możliwych do zastosowania w systemie cyberbezpieczeństwa RP;*
2. *Opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym;*
3. *Opracowanie koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym;*
4. *Opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP;*
5. *Opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP*.

Opracowana w ramach realizacji celu głównego i celów szczegółowych rozprawy koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej ma być z założenia propozycją pewnych kierunkowych, koncepcyjnych rozwiązań w wybranych obszarach problemowych, nie zaś skonstruowaną definitywnie i ostatecznie koncepcją całościowego, kompleksowego modelu zorganizowania systemu cyberbezpieczeństwa RP. Posłuży ona jako propozycja wyjściowa do proponowanych zmian, unowocześnień, modernizacji i harmonizacji zmierzających w kierunku poprawy efektywności funkcjonowania systemu cyberbezpieczeństwa RP.

Przyjęte cele badawcze – główny i szczegółowe - stanowią podstawę do zdefiniowania przedmiotu badań oraz sformułowania problemów badawczych – głównego i szczegółowych, a następnie hipotez badawczych – głównej i cząstkowych, które zostaną poddane weryfikacji i falsyfikacji.

1.3. Przedmiot badań

Przedmiotem badań w odniesieniu do sformułowanego celu badań jest organizacja systemu cyberbezpieczeństwa RP, w zakresie:

- zarządzania cyberbezpieczeństwem na poziomie krajowym;
- struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym;
- sektorów i typów podmiotów systemu cyberbezpieczeństwa;
- norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

1.4. Problemy badawcze

Problem badawczy – to tyle, co pewne pytanie lub zespół pytań, na które odpowiedzi ma dostarczyć badanie[14]. Problem jest rodzajem zadania (sytuacji) wymagającego rozwiązania, rozstrzygnięcia lub wyjaśnienia. Nie można go rozwiązać za pomocą posiadanego zasobu wiedzy, a jego rozwiązanie jest możliwe dzięki czynności myślenia produktywnego, które prowadzi do wzbogacenia wiedzy podmiotu[15]. Sformułowanie problemu badawczego polega na określeniu i objaśnieniu pewnego obiektywnego stanu niewiedzy na gruncie dotychczasowej wiedzy. W ujęciu praktycznym określenie problemu badawczego to tyle, co pewne pytanie lub zespół pytań, na które odpowiedzi ma dostarczyć badanie[16]. Sformalizowane w formie pytań problemy powinny wyczerpywać zakres niewiedzy zawarty w temacie badań i spełniać warunki precyzyjnego kreślenia obszaru i przedmiotu badawczego oraz zdefiniowanie zależności między zidentyfikowanymi zmiennymi. Podstawowym warunkiem podejmowania badań naukowych jest świadomość problemów i hipotez roboczych, określających w sposób możliwie precyzyjny cel i zakres planowanych przedsięwzięć badawczych. Bez wyraźnie sformułowanych problemów i hipotez trudno byłoby o postęp lub nowe odkrycia w dziedzinie interesujących nas faktów i zjawisk[17].

[14] Nowak S., Metodologia badań socjologicznych, Warszawa 1970
[15] Kozielecki J., *Rozwiązywanie problemów*, Warszawa 1969
[16] Nowak S., Metodologia badań socjologicznych, wyd. cyt., Apanowicz J., *Metodologia,* wyd. cyt., s. 44
[17] Łobocki M., *Metody badań pedagogicznych*, Warszawa 1982, s. 55

Główny problem badawczy rozprawy został sformułowany następująco:

Czy organizacja systemu cyberbezpieczeństwa RP zapewnia odpowiedni poziom bezpieczeństwa państwa i jakie są możliwości usprawnienia organizacji tego systemu dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa?

Zdefiniowany problem badawczy pozwolił na wyodrębnienie obszarów badań, w których zlokalizowano szczegółowe problemy badawcze, określające kierunki i zakres badań. Sformułowane problemy szczegółowe:

1. *Jakie są aktualne uwarunkowania i środowisko prawne, strategiczne, funkcjonalne i normatywno-standaryzacyjne systemu cyberbezpieczeństwa RP i czy ich rozpoznanie stanowić będzie podstawę opracowania koncepcji doskonalenia systemu cyberbezpieczeństwa RP?*
2. *Jaka jest aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić jej efektywność?*
3. *Jakie są aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić ich efektywność?*
4. *Jakie sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP i jakie powinny zostać nim objęte, aby zapewnić jego efektywność i odpowiedni poziom bezpieczeństwa kraju?*
5. *Jakie międzynarodowe i krajowe normy, metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych są aktualnie wymagane i jakie powinny zostać wskazane do zastosowania, aby zapewnić odpowiedni poziom bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP?*

1.5. Hipotezy badawcze

Wyrażając w przedstawionych problemach szczegółowych i pytaniach problemowych założenie, konkluzję lub twierdzenie istnienia związków i zależności między poszczególnymi przedmiotami, faktami lub zjawiskami (procesami) w danym problemie badawczym, można określić przesłanki do sformułowania hipotez, których konkretyzacja i analiza zweryfikuje ich trafność i zgodność ze zidentyfikowanymi uwarunkowaniami.

Hipotezy stanowią stwierdzenia, co do których istnieje pewne prawdopodobieństwo, że są właściwym rozwiązaniem sformułowanych poprzednio problemów badawczych. Inaczej mówiąc są oczekiwanymi przez badacza wynikami planowanych badań[18]. Tworzy się je określając związek między zmiennymi zależnymi i niezależnymi. Hipotezy badawcze powinny być jasno sformułowane, konkretne (specyficzne), poddawać się weryfikacji empirycznej za pomocą metod badawczych oraz nie zawierać sądów wartościujących[19].

Adekwatnie do przyjętego celu pracy oraz problemów badawczych sformułowano hipotezę ogólną, która przedstawia się następująco:

Organizacja systemu cyberbezpieczeństwa RP nie jest optymalnie zdefiniowana, co w praktyce przyczynia się do braku skoordynowanych zadań różnych organów państwa. Obecnie obowiązujące rozwiązania podsystemów bezpieczeństwa są niekompletne, niespójne, niejednorodne i rozdzielne, i nie mogą tym samym zapewnić odpowiedniego poziomu bezpieczeństwa państwa, a ich ujednolicenie, zharmonizowanie i usprawnienie może przyczynić się do poprawy efektywności systemu cyberbezpieczeństwa RP i tym samym zwiększenia poziomu bezpieczeństwa państwa.

Na podstawie hipotezy głównej sformułowano hipotezy pomocnicze:

1. *Rozpoznanie aktualnych uwarunkowań i środowiska prawnego, strategicznego, funkcjonalnego i normatywno-standaryzacyjnego systemu cyberbezpieczeństwa umożliwi opracowanie koncepcji doskonalenia rozwiązań organizacji systemu cyberbezpieczeństwa RP i zapewni jego efektywność i odpowiedni poziom bezpieczeństwa państwa.*
2. *Ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego zapewnieni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*
3. *Ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

[18] „Hipotezą nazywa się wszelkie twierdzenia częściowo tylko uzasadnione, przeto także wszelki domysł, za pomocą którego tłumaczymy dane faktyczne, a więc też i domysł w postaci uogólnienia, osiągniętego (…) na podstawie danych wyjściowych". Kotarbiński T., *Elementy teorii poznania, logiki formalnej i metodologii nauk*, Wrocław 1961

[19] Frankfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001, s.78

4. *Objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.*
5. *Ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

1.6. Metody, techniki i narzędzia badawcze

Podstawowym warunkiem podejmowania wszelkich badań naukowych jest uświadomienie sobie problemów oraz hipotez roboczych, określających w sposób możliwie precyzyjny cel i zakres planowanych przedsięwzięć badawczych. Postępowanie badawcze jest więc następstwem logicznego myślenia ujętego w etapy badawcze. Proces poznania myślowego zmierza do wyjaśnienia istoty zgromadzonych faktów i zjawisk, uchwycenia tego, co jest w nich ogólne, a co szczegółowe. Ma on charakter złożony i jest rezultatem świadomego, a przy tym celowego wysiłku badawczego. Rezultaty poznawcze procesu poznania myślowego zapewniają takie operacje myślowe jak: analiza i synteza, dedukcja i indukcja, porównywanie i przeciwstawiane, uogólnianie i wnioskowanie[20]. Bez wyraźnie sformułowanych problemów i hipotez trudno byłoby o postęp lub nowe odkrycia w dziedzinie interesujących nas faktów i zjawisk[21].

Analiza faktów zawsze poprzedza założenia, wyjaśnienia teoretyczne oraz stosowane w badaniach pojęcia, metody, techniki i narzędzia badawcze. Zebrane i pogrupowane dane stanowią natomiast faktyczny ilościowy i jakościowy materiał źródłowy podlegający analizie i przedstawieniu w formie opisu. W procesie badawczym musi być zachowana kolejność, rzetelność i jasny układ tez zapewniający właściwą strukturę pracy badawczej[22].

[20] Apanowicz J., *Metodologia ogólna*, Gdynia 2002, s. 23.
[21] Łobocki M., *Metody badań pedagogicznych*, wyd. cyt, s. 55.
[22] Apanowicz J., *Metodologia*, wyd. cyt., s. 7.

Wzbogacając wiedzę o określony stan nowej wiedzy, w stosunku do sytuacji wyjściowej, tworzone są nowe rozwiązania, wyjaśniane nieznane fakty, zdarzenia i procesy, wysuwane wnioski i teorie, wskazując jednocześnie na skutki nowych osiągnięć badawczych i ich wprowadzenia do stanu wiedzy.

W trakcie realizacji procesu badawczego autor zastosował następujące metody, techniki i narzędzia badawcze oraz metody jakościowe:

1. teoretyczne metody badawcze:
    a. badania pierwotne: analiza (treści, krytyczna, porównawcza, strukturalna), synteza, definiowanie, porównywanie, wnioskowanie (indukcyjne i dedukcyjne), obserwacja, modelowanie struktur systemu, badanie dokumentów, studia literaturowe;
    b. badania wtórne (badania nad badaniami): desk research;
2. empiryczne metody badawcze: wywiad ekspercki;
3. techniki badawcze: obserwacja, wywiad ekspercki, badanie dokumentów;
4. narzędzia badawcze: standaryzowany arkusz wywiadu eksperckiego;
5. metody jakościowe: weryfikacja i walidacja.

W trakcie realizacji procesu badawczego autor zastosował komplementarne metody i techniki badawcze, teoretyczne i empiryczne. Proces badawczy wymagał zgromadzenia właściwych materiałów, odpowiednich merytorycznie do podejmowanych problemów i celów, a następnie ich przetwarzanie za pomocą wybranych metod i technik badawczych. Wśród teoretycznych metod badawczych, zastosowanych przez autora znalazły się metody badań pierwotnych, tj. badanie dokumentów i studia literaturowe, szczególnie w odniesieniu do literatury przedmiotu - artykułów i monografii, przepisów prawnych oraz norm, metodyk i standardów bezpieczeństwa teleinformatycznego. W tym procesie niezbędne było zastosowanie takich metod, jak analiza treści, analiza krytyczna, porównawcza i strukturalna, synteza, porównywanie, wnioskowanie (indukcyjne i dedukcyjne), modelowanie struktur systemu. Badanie w tym zakresie pozwoliło zidentyfikować, poddać procesom analizy i wnioskowania aktualne rozwiązania organizacji systemu cyberbezpieczeństwa Polski w kontekście aspektów wskazanych jako przedmiot badań, a także przeprowadzić i przedstawić ich analizę porównawczą. Przedstawiając aktualny stan bezpieczeństwa polskiej cyberprze-

strzeni autor bazował na opracowaniach publikowanych corocznych raportów, takich instytucji, jak CERT[23] Polska (CSIRT[24] NASK) prowadzony przez NASK Państwowy Instytut Badawczy (NASK-PIB) i CSIRT GOV, prowadzony przez Agencję Bezpieczeństwa Wewnętrznego (ABW), realizując badania wtórne z zastosowaniem analizy treści, analizy porównawczej i strukturalnej, syntezy, porównywania, wnioskowania indukcyjnego i dedukcyjnego. Autor rozprawy, pracując w przedsiębiorstwach będących podmiotami krajowego systemu bezpieczeństwa i instytucji podległej ministrowi właściwemu ds. informatyzacji, miał możliwość prowadzić obserwację oraz metodę badania w działaniu (action research), szczególnie wobec percepcji i realizacji wymagań prawnych w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów teleinformatycznych na podstawie wskazanych norm ISO[25], co umożliwiło prowadzenie analiz, porównywania i wnioskowania. W kolejnym etapie procesu badawczego, polegającego na pozyskaniu informacji empirycznych, opartych na doświadczeniu, indywidualnej percepcji i wnioskach ekspertów w dziedzinach odpowiadających zakresowi przedmiotu badań zastosowano empiryczną metodę badawczą w formie wywiadu eksperckiego i technikę standaryzowanego arkusza wywiadu eksperckiego. Uzyskane od respondentów informacje zostały poddanie analizie porównawczej i krytycznej oraz wnioskowaniu dedukcyjnemu, pozwalającym zrozumieć opinie i argumentację respondentów. Następnie na podstawie metod syntezy i wnioskowania indukcyjnego sformułowano rekomendacje i wnioski, co do opracowywanych koncepcji rozwiązań przedmiotowych aspektów organizacji systemu cyberbezpieczeństwa. Kolejnym etapem w procesie badawczym było sformułowanie, na podstawie wniosków z badań teoretycznych i empirycznych, propozycji i koncepcji rozwiązań przedmiotowych aspektów organizacji systemu cyberbezpieczeństwa, określonych jako przedmiot badań, w odniesieniu do postawionych problemów badawczych i sformułowanych hipotez. Do realizacji tego działania zastosowano metody analizy krytycznej, porównawczej i strukturalnej oraz wnioskowania dedukcyjnego

[23] CERT – ang. Computer Emergency Response Team (pol. Zespół Reagowania na Incydenty Komputerowe) – 1. zespół bezpieczeństwa komputerowego, którego zadaniem jest całodobowe nadzorowanie ruchu internetowego i podejmowanie natychmiastowych akcji w razie pojawienia się zagrożeń. 2. organizacja utworzona w listopadzie 1988 r. przez DARPA (Defense Advanced Research Projects Agency, pol. Agencja Zaawansowanych Projektów Badawczych Departamentu Obrony)

[24] CSIRT – ang. Computer Security Information / Incident Response Team (pol. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego), nazwa stosowana w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS) i Ustawie o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), stanowiącej implementację Dyrektywy NIS

[25] ISO – Międzynarodowa Organizacja Normalizacyjna (ang. International Organization for Standardization); ISO jest oficjalną nazwą, a nie skrótowcem [https://iso.org, dostęp 01.03.2023]

dla uchwycenia i zrozumienia istoty i struktury przedmiotowych zagadnień, a następnie z zastosowaniem metod syntezy, wnioskowania indukcyjnego i modelowania struktur systemu opracowano propozycje rozwiązań dla każdego z aspektów organizacji systemu cyberbezpieczeństwa, określonych jako przedmiot badań.

W realizacji badań empirycznych autor zastosował jakościową metodę badawczą – wywiad ekspercki w formie standaryzowanego arkusza wywiadu eksperckiego. Pytania wywiadu zostały opracowane w oparciu o i w odniesieniu do sformułowanych w pracy szczegółowych problemów badawczych. Arkusz składa się z 16 pytań w układzie czterech sekcji odpowiadających czterem problemom badawczym, przy czym 3 pytania dotyczą aspektów zorganizowania zarządzania cyberbezpieczeństwem, 6 pytań dotyczy zorganizowania struktur relacji operacyjnych zarządzania cyberbezpieczeństwem, 4 pytania dotyczą doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i 3 pytania dotyczą norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa Polski. Arkusz wywiadu zawiera krótki list wprowadzający z zaproszeniem ekspertów do udziału w badaniu, zawierający temat rozprawy, zakres i problematykę projektu badawczego oraz jego genezę. Część wstępna zawiera również informację o strukturze arkusza, wskazując część wywiadu i część metryki oraz wyjaśnienia i informacje o pseudonimizacji danych osobowych, zachowaniu ich w poufności i ich dalszym nieprzetwarzaniu. Opracowany arkusz wywiadu eksperckiego jest dołączony do pracy i stanowi Załącznik nr 1.

Autor z założenia zaklasyfikował jako respondentów ekspertów, których wiedza i doświadczenie będą adekwatne do badanej problematyki, a udzielone odpowiedzi pomocne w gromadzeniu wiedzy i opinii, a następnie do weryfikacji zgromadzonej wiedzy i przyjętych hipotez, uzyskania odpowiedzi na pytania badawcze oraz formułowania wniosków. Respondentami badania są eksperci, wobec których autor postawił następujące kryteria kwalifikacji:

1. mają kompetencje do dokonania oceny i przedstawienia propozycji rozwiązań w zakresie tematyki badania, tj.: organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym; efektywności struktur i relacji operacyjnych w systemie cyberbezpieczeństwa; doboru podmiotów krajowego systemu cyberbezpieczeństwa; bezpieczeństwa teleinformatycznego usług, systemów i podmiotów systemu cyberbezpieczeństwa RP;

2. znają i rozumieją zorganizowanie zarządzania cyberbezpieczeństwem na poziomie krajowym, wynikające z ustaw, rozporządzeń i dokumentów normatywnych, tj. regulacji dotyczących krajowego systemu cyberbezpieczeństwa i systemu zarządzania kryzysowego;
3. mają doświadczenie zawodowe, w tym menedżerskie i eksperckie, w sferze gospodarczej (w tym m.in.: w podmiotach typu operator infrastruktury krytycznej, operator usług kluczowych, dostawca usług cyfrowym), administracji państwowej lub w sferze nauki,
4. legitymizują się doświadczeniem zawodowym związanym z zarządzaniem publicznym, zarządzaniem bezpieczeństwem, zarządzaniem cyberbezpieczeństwem, zarządzaniem kryzysowym (w tym szczególnie bezpieczeństwem teleinformatycznym), systemami teleinformatycznymi, zarządzaniem ryzykiem, zgodnością w obszarze technologii teleinformatycznych i cyberbezpieczeństwa oraz obszarów pokrewnych – w aspektach procesowo-organizacyjnych lub technicznych.

Autor przewidywał pierwotnie przeprowadzenie wywiadu z grupą ekspercką 6-12 osób, jednakże w wyniku podjętych działań pozyskał 45 respondentów – ekspertów dziedzinowych odpowiednich dla przedmiotu badania - i ich stanowisk w przesłanych arkuszach wywiadu eksperckiego. Wybór uczestników badania był celowy. Zaproszenie do udziału w badaniu ekspertów, spełniających wg autora przyjęte kryteria, przesłano do kilku instytutów badawczych, uczelni wyższych, podmiotów gospodarczych, w tym podmiotów krajowego systemu cyberbezpieczeństwa, wyspecjalizowanych fundacji, organizacji typu think-tank i stowarzyszeń branżowych oraz do komórek odpowiedzialnych za bezpieczeństwo, zarządzanie kryzysowe i cyberbezpieczeństwo wszystkich 16 urzędów wojewódzkich i 16 organów administracji rządowej – KPRM i 15 ministerstw. Tak kierowane zaproszenie nie przyniosło oczekiwanych rezultatów, pomimo podejmowanych licznych i intensywnych działań brak było odpowiedniej ilości respondentów, udzielających odpowiedzi. Wobec takiej sytuacji autor skierował zaproszenie do ekspertów w sposób bardziej bezpośredni, poprzez portal społecznościowy LinkedIn o charakterze zawodowym. W pierwszej kolejności zaproszenia do udziału w badaniu zostały skierowane do grupy ekspertów, spełniających wg autora przyjęte kryteria, będących uczestnikami, w charakterze członków rad programowych i panelistów, konferencji branżowych poświęconych cyberbezpieczeństwu, tj.: KSC Forum, CyberGov, InfraSec Forum, Technology Risk Management Forum. W następnej kolejności zaproszenia zostały skierowane do szerokiego grona wytypowanych przez autora ekspertów, spełniających przyjęte kryteria, reprezentujących instytuty badawcze, uczelnie

wyższe, podmioty gospodarcze, w tym podmioty krajowego systemu cyberbezpieczeństwa i zarządzani kryzysowego, podmioty gospodarcze sektora teleinformatycznego, wyspecjalizowane fundacje i organizacje typu think-tank, kancelarie prawnicze, administrację. Tak kierowane zaproszenia po podjęciu intensywnych działań pozyskania respondentów przyniosło oczekiwany efekt i pozyskano odpowiednią ilość respondentów i ich odpowiedzi. Proces pozyskiwania respondentów i ich odpowiedzi w arkuszach wywiadu został przeprowadzony w okresie od 01 czerwca do 31 lipca 2022 r. W wyniku podjętych działań w celu pozyskania reprezentatywnej grupy autor pozyskał 45 respondentów – ekspertów dziedzinowych odpowiednich dla przedmiotu badania. Grupa badawcza wyniosła 45 osób, spośród których: 13 ekspertów reprezentuje uczelnie wyższe – w tej grupie 9 ekspertów zarówno uczelnie, jak i instytucje i biznes, 6 ekspertów reprezentuje administrację, przy czym: 3 respondentów reprezentuje ministerstwa, 3 respondentów reprezentuje urzędy wojewódzkie, 7 ekspertów reprezentuje instytucje państwowe i jednostki nadzorowane przez organy rządowe, w tym działające w sferze informatyzacji, w tym 3 respondentów reprezentuje jednocześnie instytucje i uczelnie wyższe, 28 ekspertów reprezentuje biznes – przedsiębiorstwa gospodarcze, w tym 6 ekspertów reprezentuje jednocześnie biznes i uczelnie wyższe.

Wszystkie uzyskane zwrotnie arkusze badawcze respondentów są imienne. Dane osobowe respondentów nie zostaną jednak ujawnione, zostały poddane pseudonimizacji. Przetwarzanie pozyskanych danych osobowych jest anonimowe, żadne dane identyfikujące lub mogące identyfikować eksperta, jako respondenta badania, nie są przetwarzane, ani udostępniane. Wyniki badania – uzyskane odpowiedzi respondentów – są przetwarzane zbiorczo dla uzyskania uogólnionych wniosków.

Autor w trakcie opracowywania dedykowanego badaniu, realizowanemu w ramach rozprawy, standaryzowanego arkusza wywiadu eksperckiego, projektowania jego układu, struktury i pytań badawczych oraz metryki (części arkusza dotyczącej danych o respondentach) zastosował metody jakościowe – weryfikację i walidację. W ramach procesu walidacji opracowany standaryzowany arkusz wywiadu eksperckiego został przesłany do trzech ekspertów, późniejszych respondentów badania. Eksperci podzielili się swoimi indywidualnymi spostrzeżeniami i uwagami, na podstawie których zostały dokonane pewne korekty w sformułowanych pytaniach i układzie arkusza wywiadu.

1.7. Założenia i ograniczenia badawcze

Świadomość potrzeby podjęcia badań nad zjawiskiem, którego istota została wyrażona w tytule rozprawy spowodowała konieczność przyjęcia założeń wyjściowych, ograniczeń i wymagań, zgodnie z postulatami racjonalizmu metodologicznego[26]. Zakres pojęciowy wynikający z podjętego tematu i sformułowanego problemu badawczego, wymagał konkretyzacji i koniecznych redukcji dla określenia przedmiotu badań.

W realizacji projektu badawczego niniejszej rozprawy przyjęto pewne założenia i ograniczenia:

1. ograniczenia przedmiotu i zakresu badań – przedmiotem badań jest organizacja systemu cyberbezpieczeństwa Polski, rozprawa nie porusza i nie adresuje aspektów organizacji systemów cyberbezpieczeństwa innych krajów, ani Unii Europejskiej;
2. ograniczenia zakresu wypracowanego rozwiązania jako celu badania – wypracowana koncepcja doskonalenia systemu cyberbezpieczeństwa RP ma obejmować tylko aspekty organizacji systemu cyberbezpieczeństwa zdefiniowane jako przedmiot badań. Wypracowana koncepcja nie może i nie będzie stanowiła kompleksowego, pełnego, całościowego rozwiązania organizacji systemu cyberbezpieczeństwa RP;
3. ograniczenia czasowe przedmiotu badań – przedmiot i zakres rozprawy ograniczony jest czasowo w okresie od roku 2018 do czasu aktualnego (rok 2022), ponieważ, będąca podstawą systemu cyberbezpieczeństwa RP, ustawa o krajowym systemie cyberbezpieczeństwa weszła do polskiego porządku prawnego w roku 2018, jako implementacja Dyrektywy NIS[27] – Dyrektywy Unii Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Oczywiście przed i po tej dacie istniały i istnieją inne regulacje prawne, adresujące kwestie bezpieczeństwa teleinformatycznego kluczowych usług publicznych i społeczno-gospodarczych, jak np. ustawa o zarządzaniu kryzysowych czy ustawa o informatyzacji podmiotów realizujących zadania publiczne, a także dokumenty strategiczne bezpieczeństwa, jednak dotychczasowe rozwiązania nie były traktowane jako system cyberbezpieczeństwa państwa;

[26] Według Sienkiewicza P. cechami konstytutywnymi racjonalizmu metodologicznego są: (1) logiczne uporządkowanie (dziedzin myśli, pojęć, twierdzeń, argumentów), (2) oparcie wiedzy na doświadczeniu, (3) esencjalizm (wnikanie w „istotę", analiza, szukanie tego, co ważne), (4) równowaga między wiedzą intersubiektywną, a indywidualnymi przekonaniami (źródło: *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością*. AON, Warszawa 2008, s.34)

[27] Dyrektywa PE i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. U. UE L 194/1

4. ograniczenia możliwości badań porównawczych – fakt powstania krajowego systemu cyberbezpieczeństwa w 2018 r., generuje kolejne związane ograniczenie – niemożliwości przeprowadzenia badań porównawczych różnych form i sposobów zorganizowania systemu cyberbezpieczeństwa państwa w dłuższym okresie.

1.8. Krytyczna analiza literatury

Problematyką badawczą, przyjętą przez autora w kontekście przedmiotu badań, zdefiniowaną w odniesieniu do sformułowanego celu badań, jest organizacja systemu cyberbezpieczeństwa RP, w zakresie:

- zarządzania cyberbezpieczeństwem, w zakresie procesów organizowania, planowania i dokumentowania, na poziomie krajowym;
- zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie planowania i dokumentowania oraz zapewnienia cyberbezpieczeństwa i zarządzania incydentami;
- doboru właściwych sektorów i typów podmiotów (instytucji, administracji, podmiotów publicznych i gospodarczych itp.) systemu cyberbezpieczeństwa;
- wymaganych norm, metodyk i standardów rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa.

Ze względu na dynamiczne zmiany i rozwój, zachodzące w obszarze cyberbezpieczeństwa oraz dopiero co kształtujące się rozwiązania organizacyjne cyberbezpieczeństwa państwa istnieje znacząca luka w zakresie opracowań dotyczących przedstawionej problematyki. Istniejące monografie i artykuły traktują o zagadnieniach powiązanych i pokrewnych, lecz nie adresują przedmiotowych zagadnień wprost i w odpowiednio znaczącym zakresie.

Wartościowe, choć niezupełnie zbieżne z problematyką niniejszej dysertacji są rozprawy doktorskie, dotyczące problematyki pokrewnej – koncepcji doskonalenia wymiany informacji o incydentach i zagrożeniach bezpieczeństwa w krajowym systemie cyberbezpieczeństwa, bezpieczeństwa informacji, modelu systemu zarządzania bezpieczeństwem informacyjnym wykorzystującego analizę systemową sytuacji zagrożeń informacyjnych i metody prognozowania zagrożeń i ewaluacji ryzyka, scenariuszy konfliktów w cyberprzestrzeni, szeroko podbudowane warstwą teoretyczną, dotyczącą bezpieczeństwa informacji,

bezpieczeństwa informacyjnego, bezpieczeństwa teleinformatycznego w aspektach technicznych, zagrożeń dla bezpieczeństwa zasobów informacyjnych i systemów teleinformatycznych.

Problemowo najbliższa, bo dotycząca doskonalenia krajowego systemu cyberbezpieczeństwa, jest rozprawa doktorska Olczak S. pt. Koncepcja obiegu informacji o zagrożeniach i incydentach w systemie bezpieczeństwa państwa z 2019 r. Praca ta skupia się jednak tylko na zasadach działania krajowego systemu cyberbezpieczeństwa dotyczących wymiany informacji o incydentach i zagrożeniach - zagadnieniach opisu incydentów i zagrożeń dla zasobów informacyjnych oraz obiegu informacji o incydentach i zagrożeniach w systemie bezpieczeństwa państwa. Innymi ciekawymi rozprawami, jednak mniej związanymi z problematyką niniejszej dysertacji są rozprawa Sieka M. pt. Analiza systemowa i prognozowanie stanu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni z 2020 r. oraz rozprawa Świebody H. pt. Zagrożenia informacyjne bezpieczeństwa RP z 2009 r. Rozprawy te poruszają się w problematyce aspektów technicznych bezpieczeństwa teleinformatycznego. Inne rozprawy, z którymi zapoznał się autor dotyczyły zagadnień bezpieczeństwa narodowego, jednak nie związanych z systemem cyberbezpieczeństwa państwa.

Literatura przedmiotu w zakresie zagadnień bezpieczeństwa i bezpieczeństwa narodowego jest bardzo szeroka, rozwijana od wielu lat. Podejmując rozważania nad istotą i pojęciami bezpieczeństwa narodowego poddano przeglądowi szereg publikacji wskazanych w bibliografii w tym pozycje zagraniczne, tj. Williams P.D., Security Studies. An Introduction, Buzan B., Wæver O., de Wilde J., Security: A New Framework for Analysis. W pracy bezpośrednio wykorzystano stanowiska i koncepcje bezpieczeństwa i bezpieczeństwa narodowego autorów następujących prac: Koziej S., Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, Kitler W., Bezpieczeństwo Narodowe RP – aspekty prawno-organizacyjne, Musioł M., Znaczenie sekurytyzacji i sektorów bezpieczeństwa w ramach krytycznych studiów nad bezpieczeństwem, Fehler W., Sektor bezpieczeństwa wewnętrznego – mechanizmy i praktyka zmian, Nepelski M., Zarządzanie w sytuacjach kryzysowych, Kowalkowski S., Niemilitarne zagrożenia bezpieczeństwa publicznego, Sobczak J., Nowa strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Kostecki W., Strach i potęga. Bezpieczeństwo międzynarodowe w XXI wieku, Więcaszek-Kuczyńska L., Zagrożenia bezpieczeństwa informacyjnego, Nowak E., Nowak M., Zarys teorii bezpieczeństwa narodowego, Kulisz M., Zarządzanie systemem bezpieczeństwa państwa, Wiśniewski B., Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej, Elak L., Uwarunkowania bezpieczeń-

stwa Polski na przełomie XX i XXI wieku, Stańczyk J., Środowisko bezpieczeństwa państwa w ujęciu strategicznym, Dobroczyński M., Stefanowicz J., Polityka zagraniczna, Ciekanowski Z., Ulijasz B., Zwalczanie terroryzmu w Unii Europejskiej, Ciekanowski Z., Nowicka J., Wyrębek H., Bezpieczeństwo państwa w obliczu współczesnych zagrożeń, Ciekanowski Z., Zagrożenia bezpieczeństwa państwa, Bąk T., Błażejewska B., Bezpieczeństwo publiczne, współczesne zagrożenia a bezpieczeństwo państwa, Sulowski S., Brzeziński M., Bezpieczeństwo wewnętrzne państwa, Wojtaszczyk K. A., Istota i dylematy bezpieczeństwa wewnętrznego, Słownik terminów z zakresu bezpieczeństwa narodowego. W pracy nie zostały wykorzystane bezpośrednio, ale zostały poddane przeglądowi i analizie prace Jagusiaka - Jagusiak B., Zagrożenia bezpieczeństwa państwa. Geneza i charakter uwarunkowań, Jagusiak B. (red.), Systemy bezpieczeństwa w teorii i praktyce, Jagusiak B. (red.), Współczesne wyzwania bezpieczeństwa Polski, Ciekanowskiego – Ciekanowski Z., Podstawy zarządzania bezpieczeństwem państwa, Ciekanowski Z., Nowicka J., Wyrębek H., Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych, Bąk T., Ciekanowski Z., Nowicka J., Współczesne zagrożenia bezpieczeństwa państwa, Bąk T., Ciekanowski Z., Bezpieczeństwo regionalne gwarantem rozwoju zasobów ludzkich, Ciekanowski Z., Krysiński S., Zarządzanie kryzysowe w Polsce w sytuacjach zagrożeń niemilitarnych jako sposób umacniania bezpieczeństwa państwa oraz Stańczyka - Stańczyk J., Współczesne pojmowanie bezpieczeństwa. Stańczyk J., Formułowanie kategorii pojęciowej bezpieczeństwa, Stańczyk J., Język w dyskursie o bezpieczeństwie, Stańczyk J., Strategiczne środowisko bezpieczeństwa doby globalizacji, Stańczyk J., Changes in the strategic security environment following the COVID-19 pandemic, Information, Moch N., Wereda W., Stańczyk J., Security and Society in the COVID-19 Pandemic. Wymienione pozycje oraz literatura pokrewna, zawarta w bibliografii dysertacji, odnoszą się, prowadzą rozważania nad istotą kategorii pojęciowej bezpieczeństwa i formułą jego definiowania, względnością i subiektywnością pojmowania i nieprecyzyjnością wyrażania w formułach języka wypowiedzi. Pozycje przywołują i prezentują definicje bezpieczeństwa, bezpieczeństwa narodowego, jego charakterystykę i różnorodność aspektów w ujęciu systemowym i sektorowym, prezentują zagadnienia bezpieczeństwa w szerokim kontekście geopolitycznym, globalizmu, przedstawiają je w ujęciu globalnym, regionalnym i krajowym, przedstawiają aspekty polityczne, społeczne czy kulturowe bezpieczeństwa. Charakteryzowane są rodzaje zagrożeń oraz przyczyny i skutki zagrożeń bezpieczeństwa państwa oraz metody zapewnienia bezpieczeństwa. Przedstawiana jest istota i skutki sytuacji kryzysowych, problematyka zarządzania kryzysowego na wielu poziomach

organizacyjnych, zarówno w perspektywie cywilnej, jak i militarnej. Prezentowane jest podejście strategiczne do środowiska bezpieczeństwa, ujmujące terytorium, jak i czynników przestrzenne i świadomościowe. Formułowane są również cele, zadania oraz zakres i charakter odpowiedzialności państwa w dziedzinie bezpieczeństwa. Charakteryzowany jest także, w ujęciu ogólnym, wysokopoziomowym, abstrakcyjnym, teoretycznym system bezpieczeństwa państwa w jego systemowym ujęciu oraz jego konstrukcja i struktura, ze wskazaniem na elementy tego systemu, tzn. jego podsystemy kierowania i wykonawcze, w tym operacyjne i wsparcia. W wymienionych pozycjach literatury brakuje propozycji i koncepcji systemu bezpieczeństwa państwa uwzględniających i wyodrębniających podsystem cyberbezpieczeństwa i jego integralny i transsektorowy charakter bezpieczeństwa państwa. Pozycje poruszające kwestie bezpieczeństwa w sytuacji pandemicznej – kryzysowej zwracają uwagę na konieczność ponownej oceny zasad i polityk zarządzania bezpieczeństwem, kryzysem i ryzykiem stosując holistyczne, interdyscyplinarne podejście do problematyki bezpieczeństwa, zwracając uwagę na aspekty polityczne, militarne, kulturowe, informacyjne, prawne, psychologiczne i społeczne.

Poddano przeglądowi i analizie publikacje dotyczące innych wymiarów bezpieczeństwa niż wymiar cyberprzestrzeni, tj. wymiaru lądowego i morskiego, koncentrujące swoją tematykę na tych wymiarach bezpieczeństwa w aspektach przede wszystkim militarnych, jak również i politycznych, tj. Brysiak K., Elak L., Zygo K., Geneza hegemoni: implikacja terminu na podstawie Machiavellego oraz analiza hegemoni wybranych państw na przestrzeni wieków, Klisz M., Elak L., The Total Defence 21st Century. COM – Building a Resilient Society: Introduction, Elak L., Karolewski A., Przyczyny wojen hybrydowych: wyniki badań empirycznych, Zagrożenia dla bezpieczeństwa Polski, Elak L. Kuranc-Szymczak M., Elak L., Rosłoń P., Iwanowski N., Zygo K., Wyzwania Sił Zbrojnych Rzeczypospolitej Polskiej w nowych uwarunkowaniach bezpieczeństwa, Czupryński A., Elak L., Schreiber H., Bezpieczeństwo dla rozwoju, Komunikacja międzykulturowa w operacjach reagowania kryzysowego, Elak L., Rola NATO w obszarze bezpieczeństwa europejskiego, Będźmirowski J., Bezpieczeństwo polskiej granicy morskiej w początkowym okresie funkcjonowania Układu Warszawskiego, Będźmirowski J., Jednostki Obrony Terytorialnej Marynarki Wojennej w systemie bezpieczeństwa morskiego Polski w okresie Zimnej Wojny, Będźmirowski J., Bezpieczeństwo Europy oraz państw nadbałtyckich w koncepcji Działu Spraw Morskich Ministerstwa Przemysłu, Handlu i Żeglugi, Rządu Emigracyjnego w Londynie, Będźmirowski J., Gac M., Polska Marynarka Wojenna w polityce bezpieczeństwa mor-

skiego państwa w drugiej połowie XX wieku: próba usystematyzowania. Publikacje z zakresu bezpieczeństwa w wymiarze lądowym, będące pracami zbiorowymi wielu autorów, podejmują kwestie bezpieczeństwa głównie w ujęciu politycznym i militarnym, międzynarodowym, jak i krajowym, w zakresie wojen, zagrożeń i wyzwań lądowych, jak i hybrydowych. Prezentują pojęcie hegemonii jej historycznych i współczesnych aspektów tj. władza, rozwój militarny, ekonomiczny, technologiczny i informacyjny oraz układy i sojusze na arenie międzynarodowej w odniesieniu do czynników geopolitycznych. Przedstawiają też uwarunkowania bezpieczeństwa jako pochodną środowiska, tj. warunków zewnętrznych i wewnętrznych, militarnych i niemilitarnych. Prezentują koncepcję skutecznej obrony totalnej/kompleksowej małych i średnich państw, pożądających własnego państwa, niepodległości i tożsamości wobec zderzenia z tendencjami imperialnymi i poliarchicznymi państw dużych. Podejmują również problematykę wojny hybrydowej, ich przyczyn i determinujących ją czynników geopolitycznych, społecznych, kulturowych i innych. Podejmuje kwestię wyzwań i działalności Sił Zbrojnych RP i NATO w kontekście współczesnych aspektów bezpieczeństwa państwa, uwzględniając konieczność współpracy międzynarodowej oraz współdziałania podmiotów cywilnych i wojskowych. Publikacje z zakresu bezpieczeństwa w wymiarze morskim, reprezentowane przez Będźmirowskiego, koncentrują się na bezpieczeństwie morskim, ujmując tej wymiar bezpieczeństwa w perspektywach i aspektach politycznych i militarnych, tak strategicznych i taktycznych, jaki i organizacyjnych. Walorem jest ujęcie historyczne okresu międzywojennego po powojennego kształtowania bezpieczeństwa morskiego RP. Zagadnienia bezpieczeństwa lądowego i morskiego nie przystają i nie są porównywalne do zagadnień bezpieczeństwa cyberprzestrzeni, a przez to nie jest możliwe aplikowanie rozwiązań i koncepcji wypracowywanych dla tych wymiarów do formułowania koncepcji i rozwiązań mogących mieć zastosowanie w wymiarze cyberprzestrzeni dla celów zapewnienia cyberbezpieczeństwa państwa. Dlatego też nie wykorzystano w rozprawie publikacji tych autorów.

Literatura przedmiotu w zakresie zagadnień cyberbezpieczeństwa i cyberbezpieczeństwa w bezpieczeństwie narodowym jest również bardzo szeroka, rozwijana od kilku lat. Podejmując rozważania nad współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą oraz poruszając zagadnienia teoretyczne i aktualnego, faktycznego stanu cyberbezpieczeństwa kraju w odniesieniu do wyzwań, zagrożeń i incydentów cyberbezpieczeństwa poddano przeglądowi i analizie szeroką pulę publikacji wskazanych w bibliografii. W rozprawie wykorzystano stanowiska, wywody i koncepcje autorów następujących prac: Żebrowski A., Bezpieczeństwo informacyjne Polski a walka informacyjna, Liderman K., Bezpieczeństwo

informacyjne. Nowe wyzwania, Liderman K., Bezpieczeństwo informacyjne, Siek M., Wojna informacyjna w cyberprzestrzeni, Sienkiewicz P., Marszałek A., Świeboda H. (red.), Metodologia badań bezpieczeństwa narodowego, Sienkiewicz P., Wizje i modele wojny informacyjnej, Sienkiewicz P., Bezpieczeństwo cyberprzestrzeni, Bernacik B., Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej, Brzostek A., Organy władzy publicznej w zakresie ochrony cyberbezpieczeństwa w wybranych strategiach cyberbezpieczeństwa, Zalewski S., Strategia jako instrument bezpieczeństwa politycznego państwa, Oleksiewicz I., Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne Rzeczypospolitej Polskiej. Nie wykorzystano w pracy, ale poddano analizie prace następujących autorów: Ciekanowski Z., Wojciechowska-Filipek S., Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki - organizacji – państwa oraz Stańczyk J., Nadmiarowość informacji wyzwaniem dla bezpieczeństwa w społeczeństwie informacyjnym. Wymienione powyżej pozycje oraz literatura pokrewna, zawarta w bibliografii dysertacji, podejmują zagadnienia rozwoju technologii informacyjno-komunikacyjnych i funkcjonowania społeczeństwa, gospodarki państwa w cyberprzestrzeni, prezentują zagadnienia bezpieczeństwa informacyjnego i teleinformatycznego, bezpieczeństwa przestrzeni informacyjnej, cyberbezpieczeństwa i ich charakteru gwarantującego bezpieczeństwo pozostałych sektorów. Prezentują także zagadnienia dotyczące wielowymiarowych ryzyk naruszenia bezpieczeństwa, cyberzagrożeń, ich predykcji i prognozowania występowania w przestrzeni cybernetycznej oraz zdarzeń incydentów naruszeń bezpieczeństwa systemów teleinformatycznych cyberprzestrzeni. Literatura charakteryzuje zagadnienie społeczeństwa informacyjnego, systemy informacyjne i aspekty ich bezpieczeństwa, genezę i rozwój wykorzystywania danych i informacji w aktywnościach społecznych i państwowych, takich jak cyberprzestępczość, cyberkonflikt, cyberaktywizm, cyberwalka, walka informacyjna, czy cyberwojna. Literatura zagraniczna podejmująca wskazane powyżej zagadnienia cyberbezpieczeństwa w bezpieczeństwie narodowych oraz poruszające szeroki zakres zagadnień bezpieczeństwa cyberprzestrzeni, wyzwań, zagrożeń, incydentów oraz reakcji na nie, poprzez budowanie rozwiązań bezpieczeństwa cyberprzestrzeni i w cyberprzestrzeni, to m.in. Van Puyvelde D., Brantly A., US National Cybersecurity International Politics, Concepts and Organization, Guiora A. N., Cybersecurity Geopolitics, Law, and Policy, Fowler B., Maranga K., Cybersecurity Public Policy. SWOT Analysis Conducted on 43 Countries, Tikk E., Kerttunen M., Routledge Handbook of International Cybersecurity, Priyadarshini I., Cotton C., Cybersecurity. Ethics, Legal, Risks, and Policies, Johnson T. A., Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,

Manjikian M., Cybersecurity Ethics. An Introduction, Andreasson K. J., Cybersecurity. Public Sector Threats and Responses. Wskazana literatura pokazuje różnorodność podejść i zagadnień kształtujących współczesne rozumienie cyberbezpieczeństwa na Zachodzie, takich jak odstraszanie i zarządzanie, cyberwywiad i duże zbiory danych, współpraca międzynarodowa i publiczno-prywatna. Podejmuje ona próbę uporządkowania pola wokół trzech głównych tematów dotyczących polityki międzynarodowej, koncepcji i organizacji współczesnego cyberbezpieczeństwa z perspektywy USA. Podjęte zostały prawne i polityczne aspekty cyberbezpieczeństwa, również z perspektywy geopolitycznej, uwzględniając odniesienie do jednostek, korporacji, organów ścigania i organów regulacyjnych oraz zarządzanie złożonymi relacjami między nimi. Podejmowane są zagadnienia formułowania wytycznych ochrony zasobów i systemów informacyjnych oraz formułowania polityki publicznej w zakresie cyberbezpieczeństwa. W kontekście złożoności pojęć pokoju i bezpieczeństwa podejmuje zagadnienie określenia, które kwestie cyberbezpieczeństwa są rzeczywiście istotne dla międzynarodowego pokoju i bezpieczeństwa, a które, choć wymagają międzynarodowej uwagi, są kwestiami współczesnego zarządzania lub rozwoju. Literatura ta przedstawia integralność zagadnień etyki, prawa oraz zagrożeń i zasad w cyberprzestrzeni, zapewnia zrozumienie etycznych i prawnych aspektów cyberprzestrzeni oraz związanych z nią zagrożeń. Odnosi się również do aktualnych i proponowanych polityk i regulacji cyberbezpieczeństwa. Literatura analizuje obecny krajobraz zagrożeń cybernetycznych i omawia strategie stosowane przez rządy i korporacje w celu ochrony przed tymi zagrożeniami. Przedstawiane są ramy etyczne podejmowania decyzji dotyczących cyberbezpieczeństwa, kluczowe kwestie etyczne związane z bezpieczeństwem komputerowym, podkreśla związek między wartościami i przekonaniami a kodeksem etyki zawodowej w zakresie cyberbezpieczeństwa. Literatura przedstawia także cyberbezpieczeństwo sektora publicznego w ujęciu zagrożeń i reakcji na nie, koncentruje się na konwergencji globalizacji, łączności i migracji funkcji sektora publicznego do obszaru online. Przedstawiane są wyzwania oraz pojawiające się trendy i strategie z całego świata, przedstawia wskazówki dotyczące radzenia sobie ze współczesnymi zagrożeniami. Literatura przedmiotu w zakresie wyżej poruszonej problematyki zagadnień bezpieczeństwa cyberprzestrzeni, wyzwań, zagrożeń, zdarzeń incydentów, a także rozwiązań cyberbezpieczeństwa nie porusza zagadnień dotyczących systemowego zorganizowania procesów i działań w tym zakresie, relacji i struktur zarządczych i operacyjnych podmiotów i instytucji państwa oraz wyznaczania zakresu uczestniczących podmiotów i sektorów. W wymienionych pozycjach literatury brakuje propozycji i koncepcji systemu cyberbezpieczeństwa w całościowym systemie bezpieczeństwa państwa, jego

kompleksowego, całościowego modelu, jako systemu zbudowanego z podsystemów kierowania i wykonawczych, w tym operacyjnych i wsparcia, w praktycznym i aplikowalnym ujęciu metodycznym i strukturalnym, wskazujących niezbędne w takim systemie organy i podmioty, ich struktury i relacje organizacyjne i operacyjne, a także kształtującej strukturę procesów i dokumentów zarządzania strategicznego i operacyjnego cyberbezpieczeństwem państwa. Zaadresowanie wymienionych zagadnień i sformułowanie adekwatnych kierunkowych zaleceń mogłoby być podstawą budowy odpowiednio i optymalnie zorganizowanego systemu cyberbezpieczeństwa państwa.

W zakresie problematyki bezpieczeństwa teleinformatycznego, bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych w ujęciu zagadnień technicznych i organizacyjnych jest również dostępny szeroki zakres literatury. Można tu wymienić takie pozycje jak m.in.: Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Pankowski T., Bezpieczeństwo w systemach informatycznych, Bartczak A., Sidoruk T., Bezpieczeństwo systemów informatycznych, Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, Liderman K., Bezpieczeństwo teleinformatyczne, Wołowski F, Zawiła-Niedźwiecki J., Bezpieczeństwo systemów informacyjnych, Zawiła-Niedźwiecki J., Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji, Jagusiak B., Żukowski P., Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa. Zagadnienia wybrane, Ciekanowski, Z., Starczewski, J., Uwarunkowania bezpieczeństwa informacji i systemów teleinformatycznych. Problematyka bezpieczeństwa teleinformatycznego jest również poruszana w publikacjach zagranicznych, jak np.: Denning D., Wojna informacyjna i bezpieczeństwo informacji, Santos H. M. D., Cybersecurity. A Practical Engineering Approach, Moallem A., Understanding Cybersecurity Technologies. A Guide to Selecting the Right Cybersecurity Tools, Kostopoulos G., Cyberspace and Cybersecurity. Literatura przywołanego powyżej zakresu obejmuje zagadnienia zabezpieczania i ochrony informacji i przetwarzających je systemów teleinformatycznych odnosząc się do zagadnień teoretycznych i rozwiązań praktycznych zapewnienia poufności, dostępności, integralności i rozliczalności informacji, w tym informacji prawnie chronionych, w systemach teleinformatycznych. Autorzy przedstawiają metody i rozwiązania techniczne i technologiczne bezpieczeństwa teleinformatycznego, zasady budowy architektury bezpiecznych systemów oraz procesy bezpośrednio z nimi związane. Opracowania z tego zakresu ze względu na swoje czysto techniczne odniesienia nie są użyteczne w kontekście celów i problematyki badawczej niniejszej rozprawy. Poruszanie problemów i zagadnień

stricte technicznych i organizacyjnych aspektów bezpieczeństwa systemów teleinformatycznych zmieniałoby charakter i cel rozprawy. Problematykę zarządzania informacją, roli informacji w organizacji i w zarządzaniu nią, strategii informacyjnej, informacyjnej ciągłością działania, jak również wpływu technologii informatycznych na zarządzanie organizacjami i zapewnieni ich bezpieczeństwa podejmowali m.in. Stefanowicz B., Informacja, Stefanowicz B., O pojęciach i terminach informatycznych – polemika, Stefanowicz B., Rola informacji, Zaskórski P., Strategie informacyjne w zarządzaniu organizacjami gospodarczymi, Zaskórski P., Systemy informacji menedżerskiej, Zaskórski P., Zarządzanie zasobami informacyjnymi w firmie, Zaskórski P. Informacyjna ciągłość działania determinantą bezpieczeństwa organizacji, Zaskórski P., Środowisko IT w zapewnianiu bezpieczeństwa organizacji rozproszonych, jak również Zaskórski P., Szwarc K., Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania czy Woźniak J., Zaskórski P., Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej. Autor nie korzystał z tych pozycji w dysertacji. Literatura ta nie porusza zagadnień dotyczących doboru norm, metodyk i standardów ujmujących systemowo i całościowo rozwiązania organizacyjne i techniczne z zakresu bezpieczeństwa teleinformatycznego, dzięki zastosowaniu których w sposób spójny i kompleksowy podmioty operujące w cyberprzestrzeni mogłyby zaprojektować i zbudować architekturę bezpiecznych systemów i system bezpieczeństwa stosowanych rozwiązań teleinformatycznych, a przez to przyczynić się do zapewnienia odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni.

Badając bezpieczeństwo polskiej cyberprzestrzeni wykorzystano w rozprawie raporty krajowych organów powołanych do zapewniania bezpieczeństwa w cyberprzestrzeni, powołanych również do pełnienia funkcji CSIRT poziomu krajowego na mocy Ustawy o krajowym systemie cyberbezpieczeństwa – CERT Polska (CSIRT NASK) i CSIRT GOV (ABW). Wykorzystano coroczne raporty: CERT Polska (CSIRT NASK) - Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska, NASK-PIB z lat 2022, 2021, 2020 i 2019 oraz raporty ABW (CSIRT GOV) - Raport o stanie bezpieczeństwa cyberprzestrzeni RP, CSIRT-GOV ABW z lat 2022, 2021, 2020 i 2019. Poruszona problematyka jest przedstawiana również w innych raportach, m.in. corocznych raportach CERT Orange (dedykowanej jednostki firmy Orange Polska) oraz w raportach międzynarodowych producentów sieciowego sprzętu teleinformatycznego czy raportach z badań prowadzonych przez międzynarodowe firmy konsultingowe. Zdaniem autora zaprezentowanie i poddanie analizie danych z raportów dwóch organów polskiego systemu cyberbezpieczeństwa, będących CSIRTami poziomu krajowego daje wystarczającą ilość informacji na temat

stanu bezpieczeństwa polskiej cyberprzestrzeni. Zaprezentowanie danych również z pozostałych raportów nie wniosłoby istotnej zmiany w wartości informacyjnej, byłoby natomiast przytłaczające informacyjnie i zmieniałoby charakter i cel rozprawy.

Diagnozując ujęcie aspektów cyberbezpieczeństwa w strategicznych dokumentach normatywnych państwa wykorzystano następujące dokumenty: Strategia Bezpieczeństwa Narodowego RP, Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, Doktryna Cyberbezpieczeństwa RP, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2013).

Badając wymagania prawne w zakresie zorganizowania systemu cyberbezpieczeństwa Polski dotyczące:

- organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie procesów i dokumentów strategicznego planowania i zarządzania bezpieczeństwem oraz zapewnienia bezpieczeństwa i zarządzania cyberincydentami i sytuacjami kryzysowymi na poziomie krajowym;
- organów i podmiotów oraz struktur i relacji operacyjnych systemu cyberbezpieczeństwa zaangażowanych w zakresie procesów i dokumentów zarządzania cyberbezpieczeństwem oraz zapewnienia bezpieczeństwa i zarządzania cyberincydentami i sytuacjami kryzysowymi na poziomie krajowym;
- wykazu właściwych sektorów, systemów i typów podmiotów (instytucji, administracji, podmiotów publicznych i gospodarczych itp.) systemu cyberbezpieczeństwa;
- norm, metodyk i standardów rozwiązań organizacyjnych i technicznych bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa,

zidentyfikowano, poddano analizie i wykorzystano następujące regulacje – ustawy, rozporządzenia i dokumenty wykonawcze: Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Ustawa o krajowym systemie cyberbezpieczeństwa, Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzial-

nych za cyberbezpieczeństwo, Rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Ustawa o zarządzaniu kryzysowym, Rozporządzenie w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Rozporządzenie w sprawie planów ochrony infrastruktury krytycznej oraz Narodowy Program Ochrony Infrastruktury Krytycznej 2018, Załącznik 1 do Narodowy Program Ochrony Infrastruktury Krytycznej - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Krajowy Plan Zarządzania Kryzysowego. Odniesiono się również do Dyrektywy PE i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Analizując normy metodyki i standardy zarządzania bezpieczeństwem informacji, bezpieczeństwem teleinformatycznym i cyberbezpieczeństwem oraz rozwiązań organizacyjnych i technicznych bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa w poszukiwaniu najbardziej efektywnego i optymalnego zbioru takich dokumentów, na podstawie których podmioty systemu cyberbezpieczeństwa kraju powinny wdrożyć system zarządzania bezpieczeństwem teleinformatycznym, zidentyfikowano, rozpoznano, poddano analizie i wykorzystano szeroką pulę dokumentów normatywnych i standaryzujących: normy ISO, Narodowe Standardy Cyberbezpieczeństwa, normy NIST, standardy ITIL i Resilia.

W opracowaniu niniejszej rozprawy uwzględniono następujące normy ISO: ISO/IEC 27000 Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji - Wymagania, ISO/IEC 27002 Praktyczne zasady zabezpieczenia informacji, ISO/IEC 27005 Information security risk management, ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications, ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002, ISO/IEC 27014 Governance of information security, ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27018 Code of practice for protection of personally identifiable information (IIP) in public clouds acting as IPP processors, ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity,

ISO/IEC 27032:2012 Guidelines for cybersecurity, ISO/IEC 27033 Network security, ISO/IEC 27034 Application security, ISO/IEC 27035 Information security incident management, ISO/IEC 27036 Information security in relations with suppliers, PN-EN ISO/IEC 27037 Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych, ISO/IEC 27040 Storage security, ISO/IEC 20000-1 Service management system requirements, ISO/IEC 20000-2, PN-EN ISO 22301 Systemy zarządzania ciągłością działania – Wymagania, ISO 22316 Organizational resilience — Principles and attributes, ISO 28000:2007 Specification for security management systems for the supply chain.

W niniejszej rozprawie uwzględniono następujące Narodowe Standardy Cyberbezpieczeństwa: Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0), Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0), Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0), Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne (NSC 800-30 wer. 1.0), Poradnik Planowania Awaryjnego (NSC 800-34 wer. 1.0), Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0), Zarządzanie ryzykiem bezpieczeństwa informacji (NSC 800-39 wer. 1.0), Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0), Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0), Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0), Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0), Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0), Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część II (NSC 800-60 cz. 2 wer. 1.0), Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer.1.0), Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania” (NSC 800-207 wer. 1.0), Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (NSC 7298 wer. 1.0), Standardy Cyberbezpieczeństwa Chmur Obliczeniowych.

W opracowaniu niniejszej rozprawy uwzględniono następujące normy NIST: FIPS PUB 199 Standardy Kategoryzacji Bezpieczeństwa, FIPS PUB 200 Minimalne wymagania

bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych, NIST SP 800-18 rev. 1, Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych, NIST SP 800-30 rev. 1 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne, SP 800-37, Rev. 2 Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu, NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego, NIST SP 800-46 rev. 2 Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD), NIST SP 800-53, Rev. 5 Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji, NIST SP 800-53B Zabezpieczenia bazowe systemów informatycznych oraz organizacji, NIST SP 800-60 vol. 1, Rev. 1, vol. 2, Rev. 1 Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego, NSC 800-61, Rev. 2 Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego, NIST SP 800-207Architektura bezpieczeństwa systemów w modelu „Zero zaufania".

W rozprawie uwzględniono i wykorzystano również artykuły własne autora: Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne, Krajowy system cyberbezpieczeństwa, Organizacja systemu cyberbezpieczeństwa RP, Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa, Bezpieczeństwo cybernetyczne systemów w czwartej rewolucji przemysłowej, Bezpieczeństwo cyberprzestrzeni RP, Zapewnienie bezpieczeństwa i cyberbezpieczeństwa organizacjom – perspektywa empiryczna, ściśle powiązane w ramach poruszanej problematyki z przedmiotem i problemami badawczymi rozprawy.

Przeprowadzona kwerenda przepisów prawnych adresujących zagadnienia problematyki niniejszej rozprawy i definiujących sposób zorganizowania systemu cyberbezpieczeństwa wykazała, że organizacja systemu cyberbezpieczeństwa Polski nie jest optymalna dla zapewnienia jego efektywności i odpowiedniego poziomu bezpieczeństwa państwa. Przeprowadzona kwerenda szerokiego zakresu literatury nie przyniosła wyników w postaci opublikowanych opracowań w zakresie problematyki zbieżnej lub zbliżonej do problematyki niniejszej rozprawy – organizacji systemu cyberbezpieczeństwa państwa – w zakresie aspektów sformułowanych jako problemy badawcze: zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbez-

pieczeństwem na poziomie krajowym i zarządzania incydentami, doboru właściwych sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz doboru wymaganych norm, metodyk i standardów bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa. Potwierdza to założoną w koncepcji pracy lukę badawczą, uzasadniającą podjęcie badań w zdefiniowanym obszarze i zakresie.

Rozdział II. CYBERBEZPIECZEŃSTWO W BEZPIECZEŃSTWIE NARODOWYM RP

Cyberbezpieczeństwo jest jednym z atrybutów bezpieczeństwa państwa, ujmowanego jako bezpieczeństwo narodowe. Jest również jednym z jego komponentów, w ujęciu sektorowym bezpieczeństwa cyberbezpieczeństwo ma charakter transsektorowy, ze względu na powszechną zależność podmiotów i struktur organizacyjnych wszelkiej działalności w państwie w obszarze administracji i instytucji publicznych, podmiotów gospodarczych, organizacji politycznych i społecznych oraz obywateli, od systemów teleinformatycznych, a przez to od tworzonej przez nie cyberprzestrzeni. Tak więc bezpieczeństwo cyberprzestrzeni jest jednym z podstawowych i istotnych komponentów bezpieczeństwa narodowego. Bezpieczeństwo państwa jest zapewniane w ramach systemu bezpieczeństwa, którego integralnym komponentem jest podsystem cyberbezpieczeństwa. System bezpieczeństwa można rozpatrywać jako złożony system składający się z podsystemu (systemu) kierowania bezpieczeństwem narodowym oraz podsystemów (systemów) wykonawczych. System cyberbezpieczeństwa powinien mieć strukturę zgodną ze strukturą systemu bezpieczeństwa. System bezpieczeństwa powinien być kompletny, spójny, funkcjonalny oraz wydolny, sprawny, skuteczny i efektywny, a jego komponenty powinny być wewnętrznie wzajemnie powiązane, skoordynowane i zsynchronizowane w celu działania na rzecz zapewnienia trwałego i niezakłóconego rozwoju kraju i społeczeństwa oraz odpowiedniego poziomu bezpieczeństwa.

Państwo, jego struktury i organy administracyjne i instytucjonalne, podmioty sfery gospodarczej, społecznej i politycznej funkcjonują w pewnym kontekście, w pewnych warunkach i środowisku prawnym, strategicznym, funkcjonalnym, społecznym, technologicznym i normatywno-standaryzacyjnym, tak wewnętrznym, jak międzynarodowym – regionalnym i globalnym, kształtującym i definiującym jego system bezpieczeństwa, w tym system cyberbezpieczeństwa oraz warunkującym jego wydolność, sprawność, funkcjonalność, skuteczność i efektywność w stałym zapewnianiu odpowiedniego poziomu bezpieczeństwa. Państwo i struktury, z których się składa są stale poddawane presji, naciskom i działaniom,

które mają lub mogą mieć charakter naruszających bezpieczeństwo. Cyberprzestrzeń państwa również jest pod stałą presją wrogich i szkodliwych działań różnorodnych aktorów, w tym zorganizowanych grup cyberprzestępczych i cyberterrorystycznych oraz państw. Państwo dla zapewnienia swego cyberbezpieczeństwa buduje i rozwija system cyberbezpieczeństwa i rozwiązania technologiczne systemów teleinformatycznych.

System bezpieczeństwa państwa, w tym system cyberbezpieczeństwa, kształtowany jest przez dokumenty strategiczne, takie jak strategie, doktryny, polityki bezpieczeństwa oraz przez regulacje prawne. W niniejszym rozdziale poddano przeglądowi i analizie z perspektywy zagadnień cyberbezpieczeństwa i bezpieczeństwa kluczowych dla państwa systemów teleinformatycznych regulacje prawne kształtujące system zarządzania kryzysowego, krajowy system cyberbezpieczeństwa i system informatyzacji podmiotów realizujących zadania publiczne. Bezpieczeństwo systemów teleinformatycznych cyberprzestrzeni oraz architektura tego systemu bezpieczeństwa są budowane w oparciu o najlepszą wiedzę i doświadczenia branżowe, które są lokowane w międzynarodowych i branżowych normach, metodykach i standardach. W niniejszym rozdziale dokonano przeglądu dokumentów standaryzujących kwestie organizacyjne i techniczne bezpieczeństwa informacji, systemów teleinformatycznych i cyberbezpieczeństwa.

Niniejszy rozdział stanowi szeroki kontekst do ujęcia pojęcia cyberbezpieczeństwa jako ulokowanego w ramach bezpieczeństwa narodowego oraz osadzenia systemu cyberbezpieczeństwa państwa w ramach całościowego systemu bezpieczeństwa, w określonych, zmiennych, stale formowanych warunkach i środowisku bezpieczeństwa. Celem rozdziału, w kontekście celu rozprawy, jest przybliżenie kontekstu, warunków i środowiska systemu cyberbezpieczeństwa RP poprzez przedstawienie istoty i roli cyberbezpieczeństwa w systemie bezpieczeństwa narodowego, zrekonstruowanie obowiązujących przepisów prawnych i strategicznych dokumentów normatywnych w sposób formalny definiujących organizację systemu cyberbezpieczeństwa RP oraz poprzez rozpoznanie międzynarodowych i krajowych norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych, możliwych do zastosowania w systemie cyberbezpieczeństwa RP.

Rozdział niniejszy stanowi przeprowadzone w podrozdziałach rozważania nad istotą i pojęciami bezpieczeństwa narodowego oraz współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą w bezpieczeństwie narodowym. Kolejne podrozdziały poświęcono zagadnieniom teoretycznym i aktualnemu faktycznemu stanowi cyberbezpieczeństwa w odniesieniu do wyzwań, zagrożeń i incydentów cyberbezpieczeństwa, i bezpieczeństwa polskiej cyberprzestrzeni. Przeprowadzono rekonstrukcję regulacji prawnych i strategicznych

dokumentów normatywnych i ich analizę w zakresie zagadnień systemu cyberbezpieczeństwa oraz omówiono szereg norm, metodyk i standardów zarządzania bezpieczeństwem informacji, teleinformatycznym i cyberbezpieczeństwem.

2.1. Istota i pojęcia bezpieczeństwa narodowego

Bezpieczeństwo, jak też bezpieczeństwo narodowe mają wiele definicji i ujęć, z których warto przytoczyć kilka, jako szeroki kontekst do ujęcia pojęcia cyberbezpieczeństwa, ulokowanego w ramach bezpieczeństwa i bezpieczeństwa narodowego. Bezpieczeństwo, czy też bezpieczeństwo narodowe lub bezpieczeństwo państwa nie są pojęciami tożsamymi i mają swoje odrębne definicje.

Bezpieczeństwo to stan, który daje poczucie pewności istnienia i gwarancje jego zachowania oraz szanse na doskonalenie. Odznacza się akceptowalnym poziomem ryzyka utraty czegoś dla podmiotu szczególnie cennego – życia, zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych[28]. Bezpieczeństwo jest naczelną potrzebą człowieka i grup społecznych, jest także podstawową potrzebą państw i systemów międzynarodowych, jego brak wywołuje niepokój i poczucie zagrożenia. Człowiek, grupa społeczna, państwo czy organizacja międzynarodowa starają się oddziaływać na swoje otoczenie zewnętrzne i sferę wewnętrzną, by usuwać, a przynajmniej oddalać zagrożenia, eliminując własny lęk, obawy, niepokój i niepewność. Zagrożenia mogą być skierowane na zewnątrz i do wewnątrz, tak samo powinny być skierowane działania w celu ich likwidowania. Istota bezpieczeństwa jest określana jako zapewnienie egzystencji i swobody realizacji interesów aktorów w kontekście szans, wyzwań oraz ryzyk i zagrożeń. Najczęściej bezpieczeństwo definiuje się zarówno jako stan (osiągnięte poczucie bezpieczeństwa danego podmiotu), jak i proces (zapewnianie poczucia bezpieczeństwa podmiotu). Bezpieczeństwo traktowane jako proces odzwierciedla naturalny, dynamiczny charakter zjawiska bezpieczeństwa. W tym sensie bezpieczeństwo danego podmiotu to ta dziedzina jego aktywności, której treścią jest zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla

[28] Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2008, s. 14

podmiotu i jego interesów. Koziej stwierdza, że bezpieczeństwo przejawia się we wszystkich dziedzinach aktywności podmiotu. Stąd też struktura bezpieczeństwa jest w istocie tożsama ze strukturą funkcjonowania podmiotu. W ramach bezpieczeństwa międzynarodowego i narodowego możemy zatem wyodrębnić takie dziedziny bezpieczeństwa, jak np. bezpieczeństwo ekonomiczne, społeczne, militarne, publiczne, ekologiczne, informacyjne itp. Wyróżnia się także bezpieczeństwo wewnętrzne i zewnętrzne w zależności od tego, gdzie są umiejscowione i skąd się wywodzą (od wewnątrz czy z zewnątrz podmiotu) szanse, wyzwania, ryzyka i zagrożenia[29]. Ciekanowski wskazuje kilka głównych ujęć (wymiarów) bezpieczeństwa, a mianowicie: podmiotowe, przedmiotowe i funkcjonalne (procesualne). Wymiar podmiotowy obejmuje bezpieczeństwo narodowe, które jest kategorią jednostkową i odnosi się do pojedynczych państw oraz ich społeczeństw i narodów oraz bezpieczeństwo międzynarodowe, które jest terminem służącym zwykle do charakterystyki bezpieczeństwa określonej zbiorowości państw, w tym charakterystyki systemu międzynarodowego. Według kryterium przedmiotowego wyodrębnia się takie rodzaje bezpieczeństwa jak: polityczne, militarne, ekonomiczne, kulturowe, humanistyczne, ekologiczne, ideologiczne itp. W wymiarze funkcjonalnym bezpieczeństwo to proces, w którym ścierają się funkcjonalne wyzwania i zagrożenia, percepcja społeczna i koncepcje ich rozwiązywania oraz działania i oddziaływania państw oraz instytucji międzynarodowych zmierzających do budowania ich pewności przetrwania, posiadania i swobód rozwojowych[30]. Przedstawione rodzaje bezpieczeństwa wg kryterium przedmiotowego zdaniem autora są zbieżne z sektorami bezpieczeństwa, zdefiniowanymi w ramach ukształtowanego ujęcia sektorowego. Ciekanowski przywołuje również określenie bezpieczeństwa jako zarazem stanu i procesu oraz bezpieczeństwa jako naczelnej potrzeby i wartości człowieka i grup społecznych, a zarazem ich najważniejszego celu[31]. Autor podziela zdanie, że bezpieczeństwo należy ujmować i traktować równocześnie jako stan i proces, ponieważ ciągły proces bezpieczeństwa służy zapewnieniu stanu bezpieczeństwa i poczucia bezpieczeństwa, choćby w pewnych przedziałach czasu. Bąk i Błażejewska definiują bezpieczeństwo jako zdolność władz i narodu do ochrony jego wewnętrznej wartości, a do najważniejszych wartości chronionych przez państwo zaliczają:

[29] Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Bezpieczeństwo Narodowe II – 2011/18, Polityczno-strategiczne aspekty bezpieczeństwa, Warszawa 2011, s. 19, 20
[30] Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2016, s. 18, 19, 21
[31] tamże, s. 15, 16

przetrwanie państwa jako instytucji, narodu jako grupy etnicznej, biologiczne przeżycie ludności, integralność terytorialna państwa, jego niezależność polityczna i swoboda działania międzynarodowego, spokój, ochrona własności oraz jakości życia obywateli[32]. Stańczyk stwierdza, że istotą bezpieczeństwa są gwarancje nienaruszalnego przetrwania i swobody rozwojowe, których podstawą i warunkiem jest pewność, która może być obiektywna lub subiektywna, i stwierdza, że bezpieczeństwo w syntetycznym ujęciu można więc określić jako obiektywną pewność gwarancji nienaruszalnego przetrwania i swobód rozwojowych[33].

Bezpieczeństwo narodowe jest stanem uzyskanym w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa[34]. Wg Kitlera bezpieczeństwo narodowe to najważniejsza wartość, potrzeba narodowa i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym obronę państwa, jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie[35]. Ciekanowski stwierdza, że bezpieczeństwo narodowe to nie tylko ochrona i obrona istnienia państwa jako takiego przed zagrożeniami, lecz także pomyślnego bytu i rozwoju oraz ochrona wartości bliskich poszczególnym członkom społeczności, które nawet bez istnienia państwa posiadają znaczenie[36]. Bezpieczeństwo narodowe to także ogół warunków i instytucji chroniących suwerenność państwa, życie i zdrowie obywateli oraz mienie i majątek narodowy. To stan lub warunki, w których zapewniona jest ochrona narodu i terytorium państwa przed atakiem nieprzyjaciela, to zapewnienie stabilnego i harmonijnego rozwoju państwa oraz realizacji jego strategicznych interesów politycznych i ekonomicznych. Bezpieczeństwo narodowe rozumiane jest również jako stan równowagi pomiędzy potencjałem obronnym kraju, a zagrożeniem wywołanym możliwością powstania konfliktu. To także pewien stan świadomości społecznej, w którym powstający poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi lęku czy obaw o zachowanie uznanych warunków. Bezpieczeństwo narodowe w literaturze definiuje się

[32] Bąk T., Błażejewska B., *Bezpieczeństwo publiczne*, wyd. cyt., s. 14
[33] Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa*, wyd. cyt., s. 16
[34] Słownik terminów z zakresu bezpieczeństwa narodowego, wyd. cyt., s. 169
[35] Kitler W: *Bezpieczeństwo Narodowe RP – aspekty prawno-organizacyjne*, Wiedza Obronna Vol. 268 No. 3, 2019, ISSN: 2658-0829 (Online) 0209-0031, Akademia Sztuki Wojennej, Warszawa, 2019, s. 22-31
[36] Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa*, wyd. cyt., s. 27

również jako obiektywny stan pewności fizycznego przetrwania i swobód rozwojowych, stan będący zarazem żywotną potrzebą, a więc również celem i interesem narodowym (racją stanu), zakładającym zabezpieczenie oraz umacnianie żywotnych wartości, realizowanych w sferze zewnętrznej i wewnętrznej[37]. Kitler uważa, że bezpieczeństwo narodowe rozpatrywane w różnych kontekstach jest wartością i potrzebą narodową, celem działalności państwa i całego narodu. Postrzegane jest jednak przede wszystkim jako wytwór o charakterze organizacyjnym lub jako system społeczny. Jedno i drugie podejście pozwala na dostrzeżenie złożonej materii zjawiska, traktowanego jako szczególnego rodzaju przedmiot realny stworzony przez człowieka do realizacji określonych celów, a także jako uporządkowany zbiór elementów organizacyjnych, społecznych, kulturowych i materialno-technicznych oraz powiązań między nimi[38]. Ciekanowski stwierdza, że bezpieczeństwo każdego państwa zawiera w sobie, oprócz treści wspólnych dla wszystkich krajów, pewne specyficzne elementy wnikające z uwarunkowań wewnętrznych i zewnętrznych, historii, tradycji, kultury i wartości uznawanych za nadrzędne. Uważa on, że fundamentalne znaczenie mają dwa elementy bezpieczeństwa: nietykalność terytorialna i niepodległość polityczna - na nich opierają się pozostałe atrybuty niezawisłego państwa, głównie suwerenność i zdolność do zachowania podstawowych ideałów i wartości narodu i państwa[39]. Sobczak wywodzi, że bezpieczeństwo państwa jest postrzegane jako gwarant integralności terytorialnej państwa i jego suwerenności oraz jego rozwoju politycznego, społecznego i gospodarczego. Bezpieczeństwo państwa jest to również zdolność państwa i społeczeństwa do zapewnienia warunków jego przetrwania, jako instytucji wspólnoty obywatelskiej, biologicznego przeżycia ludności, integralności terytorialnej, niezależności politycznej, stabilności wewnętrznej oraz jakości życia, jest ona kształtowana poprzez działania polegające na wykorzystywaniu szans, podejmowaniu wyzwań, redukowaniu ryzyka oraz eliminowaniu zagrożeń zewnętrznych i wewnętrznych, co zapewni trwanie, tożsamość, funkcjonowanie i swobody rozwojowe państwa i narodu (społeczeństwa)[40].

Zdaniem autora bezpieczeństwo państwa jest kształtowane przez i zależne od polityki bezpieczeństwa państwa. Bezpieczeństwo państwa zależne jest od realizacji efektywnej analizy strategicznej środowiska bezpieczeństwa - międzynarodowego i wewnętrznego -

[37] Sobczak J., *Nowa strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Cybersecurity and Law, Nr 2(4) 2020, Akademia Sztuki Wojennej, Warszawa 2020, s. 10
[38] Kitler W., *System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne*, Wiedza Obronna Vol. 268 No. 3, 2019, ISSN: 2658-0829 (Online) 0209-0031, Akademia Sztuki Wojennej, Warszawa, 2019, s. 6
[39] Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa*, wyd. cyt., s. 9, 10
[40] Sobczak J., *Nowa strategia*, wyd. cyt., s. 10

oraz od formułowanych na jej podstawie polityki bezpieczeństwa państwa i polityk sektorowych bezpieczeństwa, od regulacji prawnych i ich skutecznej implementacji we wszystkich wymiarach, w tym administracyjnym, organizacyjnym, osobowym i zasobowym. Dobroczyński i Stefanowicz stwierdzili, że na kształt i sposoby urzeczywistniania polityki bezpieczeństwa składają się[41]:

- wspólne wszystkim państwom dążenie do obrony i umacniania interesów egzystencjalnych, szczególnie suwerenności i integralności terytorialnej;
- specyficzne uwarunkowania podmiotowe (narodowe);
- fundamentalny wybór miejsca w strukturze stosunków międzynarodowych (uczestnictwo w sojuszach lub niesprzymierzanie się pod postacią neutralności, „niezaangażowania" albo „polegania na własnych siłach");
- ranga i rola spełniana przez państwo w tych układach strukturalnych;
- inne okoliczności faktyczne (militarne, polityczne, ekonomiczne i w pewnym stopniu kulturowe), w których państwo realizuje swoją politykę bezpieczeństwa;
- wizja pożądanej ewolucji stosunków międzynarodowych (światowych, regionalnych, wspólnotowych, sąsiedzkich), preferowana przez dany naród i państwo;
- ideologiczny i pragmatyczny stosunek do pokoju i wojny.

Bezpieczeństwo państwa wg Ciekanowskiego zależne jest w dużej mierze od decyzji i działań podejmowanych przez władze państwowe. Polityka bezpieczeństwa państwa, aby utrzymać na odpowiednim poziomie stan bezpieczeństwa powinna być tak prowadzona, aby nie sprzyjała powstawaniu sytuacji i zjawisk konfliktotwórczych, doprowadzających do destabilizacji wewnętrznej kraju oraz powinna zmierzać do ochrony i gwarantowania zaspokajania podstawowych potrzeb egzystencjalnych społeczeństwa, a także niepodległości i suwerenności państwa[42]. Bąk i Błażejewska stwierdzają, że polityka bezpieczeństwa państwa, oprócz zwalczania zagrożeń i dbania o porządek publiczny, powinna uwzględniać również działania prewencyjne, polegające na rozpoznawaniu zagrożeń mających charakter wewnętrzny. Stan bezpieczeństwa wewnętrznego państwa uzależniony jest od sytuacji w poszczególnych dziedzinach życia społeczeństwa, dlatego polityka bezpieczeństwa państwa powinna uwzględniać różne determinujące ją czynniki[43].

[41] Dobroczyński M., Stefanowicz J., *Polityka zagraniczna*, PWN, Warszawa 1984, s. 127
[42] Ciekanowski Z., Ulijasz B., *Zwalczanie terroryzmu w Unii Europejskiej*, PWSTE, Jarosław 2015, s. 73
[43] Bąk T., Błażejewska B., *Bezpieczeństwo publiczne*, wyd. cyt., s. 17

W ramach teorii bezpieczeństwa narodowego i bezpieczeństwa wewnętrznego Fehler wskazuje wiązany z nim sektor bezpieczeństwa wewnętrznego państwa, który stanowią instytucje państwowe, których zasadniczą i przeważnie jedyną misją jest działanie na rzecz ochrony bezpieczeństwa państwa i jego obywateli w wymiarze międzynarodowym, narodowym i jednostkowym. Do instytucji państwowych tworzących rdzeń sektora bezpieczeństwa należy zaliczyć: sądownictwo, prokuraturę, siły zbrojne, formacje policyjne, służby specjalne, straże i służby ochronne, służby ratownicze, służby celne, część administracji specjalnej oraz występujące pod różnymi nazwami i posiadające różne kompetencje instytucje stanowiące zaplecze eksperckie głów państw i szefów rządów[44]. Podsystem wewnętrzny, według Wiśniewskiego, to zbiór organów władzy i administracji publicznej, metod i sposobów działania związanych z ochroną porządku konstytucyjnego, życia i zdrowia obywateli oraz majątku narodowego przed bezprawnymi działaniami a także skutkami klęsk żywiołowych i katastrof technicznych[45]. Wojtaszczyk zwraca uwagę na instytucjonalny wymiar bezpieczeństwa, który obejmuje wyspecjalizowane organy państwowe wyposażone w rożnego rodzaju kompetencje, umożliwiające utrzymywanie stanu bezpieczeństwa wewnętrznego oraz na ściśle z nim powiązany wymiar funkcjonalny, który dotyczy praktyki funkcjonowania norm i instytucji odpowiedzialnych za stan bezpieczeństwa wewnętrznego i stosowanego przez nich dostępnego arsenału działań operacyjnych[46]. Sulowski i Brzeziński formułują stwierdzenie, że bezpieczeństwo wewnętrzne łączy wiele sektorów i składa się z wielu pojęć cząstkowych o różnych zakresach, wśród których wyróżnia się m.in. bezpieczeństwo i porządek publiczny, bezpieczeństwo powszechne i bezpieczeństwo ustrojowe[47].

Bezpieczeństwo jest realizowane w ramach środowiska bezpieczeństwa. Zdaniem autora środowisko bezpieczeństwa stanowią środowisko wewnętrzne danego kraju, jak i środowisko zewnętrzne – międzynarodowe, regionalne i globalne oraz zachodzące w nich procesy i zdarzenia polityczne, militarne, gospodarcze, społeczne czy prawne. Kluczowe znaczenie ma perspektywa integralnego postrzegania ww. procesów, zdarzeń i działań z ich lokalizacją geograficzną, co jest wyrażane jako geopolityka. Pozwala to ujmować środowisko bezpieczeństwa w wymiarach strategicznych dla interesów państwa i definiować strate-

[44] Fehler W., *Sektor bezpieczeństwa wewnętrznego – mechanizmy i praktyka zmian*, DOCTRINA, Nr 6 Studia Społeczno-Polityczne 2009, s. 73
[45] Wiśniewski B. (red.), *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej*, AON, Warszawa 2004, s. 62
[46] Wojtaszczyk K. A., *Istota i dylematy bezpieczeństwa wewnętrznego*, Przegląd Bezpieczeństwa Wewnętrznego, Nr 1/09, s. 15
[47] Sulowski S., Brzeziński M., *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Dom Wydawniczy Elipsa, Warszawa 2009, s. 40

giczne środowisko bezpieczeństwa. Zdefiniowanie środowiska bezpieczeństwa i strategicznego środowiska bezpieczeństwa pozwala na dokonywanie strategicznych analiz bezpieczeństwa i podejmowanie decyzji oraz formułowanie polityk bezpieczeństwa. Stańczyk formułuje stwierdzenie, że środowisko funkcjonowania danego państwa rozpatrywane z perspektywy wyzwań i zagrożeń staje się jego środowiskiem bezpieczeństwa w stosunkach międzynarodowych. Środowisko bezpieczeństwa postrzegane jest jako system kształtowany przez wiele czynników pozostających między sobą w różnych relacjach, m.in.: położenie geograficzne (geopolityczne), interakcje pomiędzy państwami, ich miejsce i rola w strukturach międzynarodowych, a także stopień technicznego zaawansowania posiadanych sił zbrojnych. Strategiczne środowisko bezpieczeństwa ma szeroki wymiar i jest odnoszone zarówno do przestrzeni terytorialnych, jak i do systemów wartości, potrzeb oraz interesów, jakie funkcjonują w ludzkiej świadomości, kreując świadomościowe wymiary intelektualne czy emocjonalne w odniesieniu do pojmowania bezpieczeństwa, odnosi się też do kultury strategicznej i kultury bezpieczeństwa[48]. Strategiczne środowisko bezpieczeństwa cechuje się złożonością, poprzez takie procesy i zjawiska jak: anarchiczność środowiska międzynarodowego i jego turbulencyjność, wrażliwość i podatność podmiotów na negatywne impulsy płynące ze środowiska, normatywność stosunków międzynarodowych i ich instytucjonalizacja, stosunek do wojny napastniczej oraz kontroli zbrojeń, rozwój wielostronnych form współpracy międzynarodowej, napięcia związane z terroryzmem międzynarodowym, problemy zagrożeń ekologicznych, potrzeba ograniczania przestępczości zorganizowanej, wyhamowania konfrontacji cywilizacyjno-kulturowej, a także rozwoju badań na rzecz zmniejszenia śmiertelności na skutek chorób epidemiologicznych[49]. Strategiczne środowisko bezpieczeństwa należy rozpatrywać z różnych perspektyw, np. określonego państwa, regionu, podsystemu międzynarodowego czy systemu globalnego, jak również danej sytuacji, aktualnej fazy rozwoju lub stanu bezpieczeństwa międzynarodowego. Dostrzegane jest w nim współwystępowanie takich cech jak: zmienność (volatility), niepewność (uncertainty), złożoność (complexity) i niejasność (ambiguity)[50]. Elak stwierdza, że uwarunkowania bezpieczeństwa są pochodną środowiska, w jakim funkcjonuje dany podmiot, uwzględniając aspekt strategicznego środowiska bezpieczeństwa, które należy rozumieć jako jego nadrzędne i priorytetowe z punktu widzenia podmiotu. W strategicznym środowisku bezpieczeństwa można wyróżnić trzy grupy podmiotów, które je kształtują: podmioty państwowe,

[48] tamże, s. 146, 147
[49] tamże, s. 147
[50] tamże, s. 156

organizacje podmiotów państwowych – organizacje międzynarodowe o charakterze społecznym, gospodarczym, politycznym, podmioty niepaństwowe – korporacje ponadnarodowe, organizacje społeczne, organizacje przestępcze, ekstremistyczne ruchy społeczne i inne. Strategiczne środowisko bezpieczeństwa ma charakter dynamiczny, wyrażający się głównie w kryzysach i konfliktach, gdyż nawet te toczące się w dalekim sąsiedztwie geograficznym, stanowią największe zagrożenie dla bezpieczeństwa państwa i jego suwerenności[51]. Środowisko bezpieczeństwa należy rozpatrywać z uwzględnieniem problematyki wyzwań i zagrożeń dla bezpieczeństwa w konkretnych uwarunkowaniach środowiskowych[52].

W ramach rozwoju teorii bezpieczeństwa wykształciło się całościowe, holistyczne, systemowe podejście do bezpieczeństwa i pojęcie systemu bezpieczeństwa narodowego. Bezpieczeństwo narodowe jest zapewniane przez system bezpieczeństwa narodowego, który składa się z podsystemu kierowania i podsystemów wykonawczych, jak też, w innym ujęciu, z podsystemów bezpieczeństwa wewnętrznego i zewnętrznego.

System bezpieczeństwa narodowego, wg Kulisza, składa się z podsystemu bezpieczeństwa wewnętrznego, który przeciwdziała zagrożeniom mogących ograniczać lub uniemożliwiać swobodny i stabilny rozwój głównych dziedzin życia społecznego i podsystemu bezpieczeństwa zewnętrznego, gwarantującego stabilność bytu narodu w trwałych granicach państwa. Podsystem powinien się składać ze skoordynowanych wewnętrznie i wzajemnie powiązanych elementów organizacyjnych, ludzkich i materialnych, które powinny działać na rzecz zapewnienia trwałego i niezakłóconego rozwoju kraju i społeczeństwa we wszystkich aspektach życia. Kulisz proponuje modułowy system bezpieczeństwa, w skład którego wchodzą: podsystem kierowania bezpieczeństwem państwa, jako zbiór elementów i relacji mających za zadanie zachowanie ciągłości podejmowania decyzji i prowadzenie działań utrzymujących bezpieczeństwo państwa, w którego skład wchodzą: prezydent, rząd wraz z podległymi mu urzędami, organy doradcze prezydenta i rządu, ministrowie kierujący określonymi działami administracji rządowej, główne organy administracji rządowej, na które nałożono zadania z obszaru bezpieczeństwa państwa, wojewodowie oraz organy samorządu terytorialnego wraz z obsługującymi ich urzędami oraz podsystem bezpieczeństwa społecznego, podsystem bezpieczeństwa gospodarczego, podsystem bezpieczeństwa militarnego. Każdy z podsystemów można zdefiniować jako skoordynowany wewnętrznie zbiór elemen-

[51] Elak L., *Uwarunkowania bezpieczeństwa Polski na przełomie XX i XXI wieku*, Bezpieczeństwo. Teoria i Praktyka, 2020, No 2 (XXXIX), Oficyna Wydawnicza KA AFM, Kraków 2020, s. 33, 34, 35
[52] tamże, s. 45

tów, takich jak: struktury, wykonawcy i środki, którymi dysponują, wyróżnionych w środowisku bezpieczeństwa państwa ze względu na wzajemne powiązania i zachodzące między nimi relacje przyczynowo – skutkowe, wyrażające jakieś uporządkowanie w strukturze organizacyjnej[53].

Koziej stwierdza, że system bezpieczeństwa narodowego stanowi całość sił, środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana, utrzymywana i przygotowywana. Składa się z systemu kierowania i szeregu podsystemów wykonawczych[54].

System bezpieczeństwa narodowego, wg Kitlera, powinien swoim zasięgiem obejmować wszelkie dziedziny działalności związane z zapewnieniem bezpieczeństwa narodowego. Jego zakres przedmiotowy powinien obejmować m.in. zagadnienia bezpieczeństwa politycznego, militarnego, ekonomicznego, ekologicznego, kulturowego, społecznego, powszechnego, publicznego i informacyjnego. Innymi słowy, powinien uwzględniać aspekty bezpieczeństwa zewnętrznego i wewnętrznego, militarnego i niemilitarnego, kwestie pokojowe, kryzysowe i wojenne, a także poszczególne szczeble swojej organizacji (struktury) – od szczebla centralnego po szczebel lokalny. System bezpieczeństwa narodowego to celowo wyodrębniony z „systemu państwowego" i wzajemnie powiązany, kolektywny zbiór podmiotów sektora państwowego, samorządowego, rynkowego i pozarządowego, a także obywateli, wykonujący określone w ustawach zadania na rzecz zapewnienia bezpieczeństwa narodowego. Misją nadrzędną systemu bezpieczeństwa narodowego jest zapewnienie istnienia w nienaruszalnych granicach suwerennego, niepodległego i demokratycznego narodu zorganizowanego w państwo, rozumiane jako rzeczywisty stan stabilności wewnętrznej zapewniony poprzez posiadanie i wykorzystywanie realnych zdolności do ochrony i obrony terytorium, społeczeństwa, władzy politycznej, utrzymywania i kreowania warunków rozwoju oraz układu stosunków zewnętrznych gwarantujących trwanie i przetrwanie w środowisku międzynarodowym. Kitler definiuje system bezpieczeństwa narodowego jako celowo wyodrębniona ze zbioru różnorodnych podmiotów, z jakich się składa państwo, i uporządkowana całość, złożona z różnych elementów, przeznaczonych do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana na mocy zadanych relacji porządkujących (w podsystemy), utrzymywana i doskonalona. W ujęciu funkcjonalnym system bezpieczeństwa narodowego składa się z zasadniczych elementów (podsystemów),

[53] Kulisz M., *Zarządzanie systemem bezpieczeństwa państwa*, Rocznik bezpieczeństwa międzynarodowego 2010/2011, s. 100, 101, 102
[54] Koziej S., *Bezpieczeństwo,* wyd. cyt., s. 32

które mogą być odrębnie rozpatrywane jako systemy, tj.: podsystemu (systemu) kierowania bezpieczeństwem narodowym oraz podsystemów (systemów) wykonawczych. Relacje porządkujące system bezpieczeństwa narodowego można traktować jako odrębny podsystem (system) podstaw prawnych bezpieczeństwa narodowego[55].

System to każdy złożony obiekt wyróżniony w badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) między nimi[56]. System jest również definiowany jako zbiór wzajemnie powiązanych lub oddziałujących na siebie elementów[57].

Dokumenty strategiczne bezpieczeństwa również definiują i charakteryzują system bezpieczeństwa narodowego. Dokumentami takimi są np. Doktryna Cyberbezpieczeństwa RP i Biała Księga Bezpieczeństwa Narodowego.

Biała Księga Bezpieczeństwa Narodowego definiuje system bezpieczeństwa narodowego (bezpieczeństwa państwa) - rozumie się go jako całość sił (podmiotów), środków i zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana (w podsystemy i ogniwa), utrzymywana i przygotowywana. Składa się z podsystemu (systemu) kierowania i szeregu podsystemów (systemów) wykonawczych, w tym podsystemów operacyjnych (obronny i ochronne) i podsystemów wsparcia (społeczne i gospodarcze). System bezpieczeństwa narodowego RP ma strukturę terytorialną, można w nim wyróżnić gminne, powiatowe i wojewódzkie podsystemy bezpieczeństwa terytorialnego. Ze względu na funkcjonalną strukturę państwa można także wyróżnić resortowe (działowe) systemy bezpieczeństwa. System jest wielopłaszczyznowy i wielowymiarowy. Uwzględnia stosunki wewnątrz państwa i jego relacje z podmiotami zewnętrznymi oraz obejmuje ich różne sfery i płaszczyzny: stosunki polityczne, prawne, wojskowe, gospodarcze, społeczne, kulturowe, naukowe itp. Podsystem kierowania jest kluczowym elementem systemu bezpieczeństwa narodowego. Stanowi on część systemu bezpieczeństwa narodowego przeznaczoną do kierowania jego funkcjonowaniem, obejmującą organy władzy publicznej i kierowników jednostek organizacyjnych, które wykonują zadania związane z bezpieczeństwem narodowym (w tym organy dowodzenia Sił Zbrojnych RP) wraz z organami doradczymi i aparatem administracyjnym (sztabowym) oraz procedurami funkcjonowania i infrastrukturą (stanowiska i centra kierowania oraz zarządzania, system łączności). Ma on żywotne znaczenie dla całego systemu bezpieczeństwa w czasie pokoju,

[55] Kitler W., *System bezpieczeństwa,* wyd. cyt., s. 23, 24, 25
[56] Sienkiewicz P., *Analiza systemowa i podstawy zastosowania*, Wydawnictwo Bellona, Warszawa 1994, s. 16
[57] na podstawie PN-EN-ISO/IEC 27000, PN-EN-ISO 9000

kryzysu i wojny. Zapewnia uzyskiwanie wiedzy o zagrożeniach i ich analizę, planowanie przygotowania i działania podsystemów operacyjnych i wsparcia oraz zarządzanie (dowodzenie) nimi w trakcie działań. Można wyodrębnić cztery strategiczne obszary zadaniowe podsystemu kierowania: monitorowanie zagrożeń, z uwzględnieniem ich skali, rodzaju i miejsca występowania, zapobieganie powstawaniu zagrożeń, zarówno na terytorium kraju, jak i poza jego granicami, usuwanie skutków zagrożeń, gdy nie udało się im zapobiec, kierowanie obroną państwa w razie bezpośredniej agresji militarnej. Podsystemy wykonawcze systemu bezpieczeństwa narodowego (bezpieczeństwa państwa) to siły i środki przewidziane do realizacji ustawowo kreślonych zadań w dziedzinie bezpieczeństwa, pozostające w dyspozycji organów kierowania bezpieczeństwem. Wyróżnia się ich dwa rodzaje: operacyjne oraz wsparcia. Podsystemy operacyjne tworzą: podsystem obronny państwa (obronności, obrony narodowej, bezpieczeństwa militarnego) – przeznaczony do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym zagrożeniom o charakterze polityczno-militarnym – oraz podsystemy ochronne państwa i ludności (bezpieczeństwa cywilnego, pozamilitarnego) – przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym i wewnętrznym zagrożeniom o charakterze niemilitarnym (cywilnym). Podsystemy wsparcia to podmioty społeczne i gospodarcze przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym i wewnętrznym zagrożeniom o charakterze społecznym i gospodarczym, a także do społecznego i gospodarczego zasilania operacyjnych podsystemów bezpieczeństwa narodowego w czasie pokoju, kryzysu i wojny[58].

Doktryna Cyberbezpieczeństwa RP wskazuje na zintegrowany, zarządzany (koordynowany) ponadresortowo system cyberbezpieczeństwa RP obejmujący: podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa oraz podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych. Zgodnie z przyjętą Doktryną Cyberbezpieczeństwa zapewnienie bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej powinno być realizowane

[58] Biała Księga Bezpieczeństwa Narodowego, wyd. cyt., s. 36, 37, 38

w kilku płaszczyznach przez sektor publiczny, sektor komercyjny, obywatelski oraz w wymiarze transsektorowym[59].

Teoria bezpieczeństwa w toku badań wykształciła koncepcję sektorów bezpieczeństwa i sekurytyzacji, wypracowaną w ramach Kopenhaskiej Szkoły Studiów nad Bezpieczeństwem. Szkoła kopenhaska składa się z trzech segmentów: analizy sektorowej, teorii kompleksów bezpieczeństwa i koncepcji sekurytyzacji. Analiza sektorowa szkoły kopenhaskiej polega na teoretycznym podzieleniu badań nad bezpieczeństwem oraz stosunkami międzynarodowymi na sektory: wojskowy, polityczny, gospodarczy, ekologiczny i społeczny. Głównym powodem takiego ujęcia problemu bezpieczeństwa było odejście od dominującej interpretacji sektorów (dziedzin bezpieczeństwa, sfer, rodzajów stosunków międzynarodowych itp.), jako źródeł zagrożeń i potraktowanie ich, jako obiektów albo „celów" zagrożenia[60]. „Sektory bezpieczeństwa to obszary/pola aktywności lub areny, które pociągają za sobą szczególne formy interakcji bezpieczeństwa i szczególne definicje obiektów odniesienia"[61]. Przedstawiciele Szkoły Kopenhaskiej w toku badań wyodrębnili następujące sektory bezpieczeństwa: militarny, państwowy/polityczny, społeczny, ekonomiczny, ochrony środowiska naturalnego[62]. Koziej S. przedstawił inne ujęcie sektorów bezpieczeństwa, niż zrobiła to szkoła kopenhaska. Sektory bezpieczeństwa, w znacznie bardziej granularnym ujęciu, powiązał z czterema dziedzinami bezpieczeństwa, tj.: obronna, ochronna, społeczna i gospodarcza. Koziej, co znamienne i bardzo istotne z perspektywy przedmiotu niniejszej dysertacji, wyszczególnił transsektorowe obszary bezpieczeństwa, do których zaliczył cyberbezpieczeństwo, bezpieczeństwo informacyjne i kierowanie bezpieczeństwem[63]. Podobne ujęcie dziedzin i sektorów bezpieczeństwa zostało zawarte w koncepcji bezpieczeństwa narodowego ujętej w Białej Księdze Bezpieczeństwa Narodowego RP, gdzie wyodrębniono poszczególne dziedziny bezpieczeństwa: obronną, ochronną, społeczną i gospodarczą, którym przyporządkowano określone sektory, a także wyodrębniono transsektorowe obszary bezpieczeństwa[64]. Podział obszarów bezpieczeństwa uwzględniający dziedziny i sek-

[59] Doktryna Cyberbezpieczeństwa RP, wyd. cyt., s. 9
[60] Kostecki W., *Strach i potęga. Bezpieczeństwo międzynarodowe w XXI wieku,* Warszawa, Poltext, 2012
[61] Williams P. D., *Security Studies. An Introduction*. London, New York: Routledge 2008 za Musioł M., *Znaczenie sekurytyzacji,* wyd. cyt., s. 47
[62] Buzan B., Wæver O., de Wilde J., *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers 1998 za Musioł M., *Znaczenie sekurytyzacji,* wyd. cyt., s. 47
[63] Mąkosa G., *Cyberbezpieczeństwo,* wyd. cyt., s. 114
[64] Biała Księga Bezpieczeństwa Narodowego, wyd. cyt., s. 19

tory bezpieczeństwa oraz obszary transsektorowe wyszczególnione w Białej Księdze Bezpieczeństwa Narodowego i zbieżne z koncepcją sformułowaną przez Kozieja przedstawia poniższy rysunek 1:

Rys. 1. Dziedziny i sektory bezpieczeństwa narodowego

Dziedziny bezpieczeństwa narodowego																	
obronna			ochronna			społeczna						gospodarcza					
Sektory bezpieczeństwa narodowego																	
dyplomatyczny	militarny	wywiadowczy	kontrwywiadowczy	porządku publicznego i prawa	ratownictwa	kulturowy	edukacyjny	socjalny	demograficzny	migracyjny	inne	finansowy	energetyczny	transportowy	infrastruktury krytycznej	środowiska naturalnego	inne
Transsektorowe obszary bezpieczeństwa: cyberbezpieczeństwo, bezpieczeństwo antyterrorystyczne																	

Źródło: Biała Księga Bezpieczeństwa Narodowego, s. 19

Z analizy powyższych koncepcji i definicji można wywnioskować, że niektóre definicje bezpieczeństwa narodowego w istocie rzeczy definiują bezpieczeństwo państwa. Należy przyjąć, że dzieje się tak z powodu powszechnego przyjęcia kategorii pojęciowej bezpieczeństwa narodowego, jako kategorii najwyższej i najszerszej, zawierającej w sobie inne kategorie bezpieczeństwa[65].

Współczesne postrzeganie bezpieczeństwa charakteryzuje odejście od historycznie utrwalonych przekonań o bezpieczeństwie państwa jako wolności od zewnętrznych zagrożeń i skierowanie większej uwagi na proces budowania i utrzymywania (gwarantowania) warunków rozwoju, stabilności i dobrobytu zarówno państwa, całego społeczeństwa, jak i poszczególnych obywateli wraz z ich dobrami materialnymi i niematerialnymi. Zmiana w pojmowaniu istoty współczesnego systemu bezpieczeństwa narodowego podkreśla trwanie i znaczenie wszystkich tradycyjnych zadań państwa w tym zakresie, ale rozszerza jego zakres funkcjonalny na szereg zadań społecznych i ekonomicznych, istotnych dla bezpieczeństwa poszczególnych grup społecznych i każdego obywatela z osobna[66].

[65] Mąkosa G., *Strategiczne ujęcie cyberbezpieczeństwa RP,* w: Lizakowski P. (red.), Securitologiczna panorama bezpieczeństwa, WAT, Wydawnictwo FNCE, Poznań 2022, s. 118
[66] Kitler W., *System bezpieczeństwa,* wyd. cyt., s. 20

2.2. Współczesne pojęcie cyberbezpieczeństwa, jego rola i istota

Współcześnie bezpieczeństwo państwa w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej zyskało dodatkowy wymiar, jakim, obok lądu, wody, powietrza i przestrzeni kosmicznej, jest cyberprzestrzeń i skojarzone z nią cyberbezpieczeństwo. Charakterystykę, wymiar i skalę oddziaływania cyberbezpieczeństwa na bezpieczeństwo narodowe prezentują niżej przedstawione definicje i problemowe ujęcie zagadnienia.

Przyjmując, że bezpieczeństwo narodowe jest stanem uzyskanym w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa[67], należy zauważyć, że cyberbezpieczeństwo mieści się w zdefiniowanych granicach pojęcia bezpieczeństwa narodowego[68]. Cyberbezpieczeństwo jest składową bezpieczeństwa narodowego i międzynarodowego, jest bezpieczeństwem transsektorowym i jest ich coraz istotniejszym komponentem, a zapewnienie odpowiednio wysokiego poziomu cyberbezpieczeństwa jest kluczowym wyzwaniem stojącym przed państwami. Cyberbezpieczeństwo jako dziedzina bezpieczeństwa narodowego, w dobie powszechnej informatyzacji i operowania w cyberprzestrzeni, jest jednym z kluczowych sektorów bezpieczeństwa. Bezpieczeństwo w cyberprzestrzeni, jako kategoria transsektorowa, łączy wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny, dlatego też najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane i kompleksowe, obejmujące wszystkie te obszary. Takie zintegrowane i kompleksowe podejście do bezpieczeństwa, w tym cyberbezpieczeństwa, może być realizowane, poprzez polityki i strategie bezpieczeństwa, w systemie bezpieczeństwa narodowego.

Doktryna Cyberbezpieczeństwa RP formułuje problemowe ujęcie cyberbezpieczeństwa w bezpieczeństwie narodowym, traktując, że cyberbezpieczeństwo odnosi się do bezpiecznego funkcjonowania państwa, jego struktur administracyjnych, podmiotów gospodarczych i obywateli w cyberprzestrzeni. Cyberprzestrzeń jest jednym z obszarów aktywności państwa, podmiotów prywatnych i obywateli. Cyberprzestrzeń jest przestrzenią konfliktu, w której kraje mierzą się nie tylko z innymi państwami, ale także z wrogimi organizacjami,

[67] Słownik terminów z zakresu bezpieczeństwa narodowego, wyd. cyt., s. 169
[68] Mąkosa G., *Krajowy system cyberbezpieczeństwa RP*, w: A. Chabasińska, A. Warchał (red.), Perspektywy bezpieczeństwa w teorii i praktyce, WAT, Warszawa 2019, s. 230

jak choćby z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi[69].

Doktryna Cyberbezpieczeństwa RP zawiera zbiór definicji zagadnień dotyczących cyberbezpieczeństwa, które łącznie dość spójnie i kompletnie przedstawiają jego istotę, środowisko i kontekst funkcjonowania. Cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) to proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni. Bezpieczeństwo cyberprzestrzeni RP to część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych. Cyberprzestrzeń RP to cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji). Cyberprzestrzeń z kolei jest definiowana jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami. Środowisko cyberbezpieczeństwa to ogół warunków funkcjonowania danego podmiotu w cyberprzestrzeni charakteryzowany przez wyzwania (szanse i ryzyka) oraz zagrożenia dla osiągania przyjętych celów. Zagrożenia cyberbezpieczeństwa stanowią pośrednie lub bezpośrednie zakłócające lub destrukcyjne oddziaływania na podmiot w cyberprzestrzeni. Wyzwania cyberbezpieczeństwa to sytuacje problemowe w dziedzinie cyberbezpieczeństwa, stwarzane zwłaszcza przez szanse i ryzyka oraz generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw cyberbezpieczeństwa. Szanse cyberbezpieczeństwa stanowią niezależne od woli podmiotu

[69] Doktryna cyberbezpieczeństwa RP, wyd. cyt., s. 4

okoliczności (zjawiska i procesy w środowisku bezpieczeństwa) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w dziedzinie cyberbezpieczeństwa. Ryzyka cyberbezpieczeństwa to możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze cyberbezpieczeństwa[70].

Zagadnienia cyberbezpieczeństwa i aspektów z nim związanych zostały również uwzględnione i zaadresowane w dedykowanych im, międzynarodowych normach ISO. Cyberbezpieczeństwo to stan ochrony przed fizycznymi, społecznymi, duchowymi, finansowymi, politycznymi, emocjonalnymi, zawodowymi, psychologicznymi, edukacyjnymi lub innymi rodzajami lub konsekwencjami niepowodzenia, uszkodzenia, błędu, wypadków, krzywdy lub jakiegokolwiek innego zdarzenia w cyberprzestrzeni, które można uznać za niepożądany, może przybrać formę ochrony przed zdarzeniem lub narażeniem na coś, co powoduje straty zdrowotne lub ekonomiczne, może obejmować ochronę osób lub mienia. Cyberbezpieczeństwo, jako aspekt bezpieczeństwa, może przyjąć definicję bezpieczeństwa jako stanu pewności, że niekorzystne skutki nie zostaną wywołane przez jakiś czynnik w określonych warunkach. Cyberbezpieczeństwo to bezpieczeństwo cyberprzestrzeni, czyli zachowanie poufności, integralności i dostępności (jak również innych właściwości: autentyczności, rozliczalności, niezaprzeczalności i wiarygodności) informacji w cyberprzestrzeni. Cyberprzestrzeń jest zdefiniowana jako złożone środowisko wynikające z interakcji ludzi, oprogramowania i usług w Internecie za pomocą podłączonych do niego urządzeń technologicznych i sieci, które nie istnieje w żadnej fizycznej formie[71].

Zagadnienia cyberbezpieczeństwa są przedmiotem regulacji prawnych, ustawy definiują cyberbezpieczeństwo i związane z nim aspekty, zjawiska i pojęcia, jak np. ustawa o krajowym systemie cyberbezpieczeństwa czy ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[72]. Cyberbezpieczeństwo to działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami[73]. Cyberprze-

[70] Doktryna cyberbezpieczeństwa RP, wyd. cyt., s. 4, 7, 8
[71] ISO/IEC 27032 (ang. cybersafety, cybersecurity, cyberspace security, cyberspace), s. 4
[72] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 2
[73] Projekt z dnia 15 marca 2022 r. Ustawy o zmianie Ustawy o krajowym systemie cyberbezpieczeństwa, art. 1, pkt 3

strzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[74]. Definicje cyberbezpieczeństwa i cyberprzestrzeni w regulacjach prawnych odnoszą się do systemów informacyjnych i ich odporności, ochrony i bezpieczeństwa. Bezpieczeństwo systemów informacyjnych to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[75]. System informacyjny to system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej[76]. System teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[77]. Bezpieczeństwo sieci i usług komunikacji elektronicznej to zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci lub usług, przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej, innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy[78]. Cyberzagrożenie to wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz na inne podmioty[79]. Zagrożenie cyberbezpieczeństwa to potencjalna przyczyna wystąpienia incydentu - zdarzenia, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo[80].

Problemowe ujęcie i definicje cyberbezpieczeństwa można również spotkać w literaturze przedmiotu. Cyberbezpieczeństwo to zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Cyberbezpieczeństwo to między innymi ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych. Cyberbezpieczeństwo to ogół technik, procesów i praktyk stosowanych w celu

[74] Ustawa o informatyzacji, wyd. cyt., art. 3
[75] Projekt z dnia 15 marca 2022 r. Ustawy, wyd. cyt., art. 1, pkt 3
[76] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 2
[77] Ustawa o informatyzacji, wyd. cyt., art. 3
[78] Projekt z dnia 15 marca 2022 r. Ustawy, wyd. cyt., art. 1, pkt 3
[79] tamże, art. 1, pkt 3
[80] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 2

ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem. Cyberbezpieczeństwo bywa także określane jako bezpieczeństwo technologii informatycznych czy też bezpieczeństwo teleinformatyczne. Wg Lidermana bezpieczeństwo teleinformatyczne oznacza poziom uzasadnionego (np. analizą ryzyka) zaufania, że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych nie zostaną poniesione[81]. Bezpieczeństwo teleinformatyczne jest również zdefiniowane jako zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności.

Autor definiuje cyberbezpieczeństwo jako bezpieczeństwo systemu teleinformatycznego, realizowanych przez niego procesów przetwarzania i przetwarzanych danych oraz systemów od nich zależnych. Cyberbezpieczeństwo to też bezpieczeństwo systemu teleinformatycznego w cyberprzestrzeni. Cyberbezpieczeństwo może być również zdefiniowane jako bezpieczeństwo cyberprzestrzeni. Cyberprzestrzeń zaś autor definiuje jako powiązane logicznie i fizycznie systemy teleinformatyczne. Ilość systemów teleinformatycznych cyberprzestrzeni jest stale zmienna w czasie, nie stanowi zamkniętego, skończonego zbioru. Zatem cyberbezpieczeństwo może być zdefiniowane jako bezpieczeństwo systemu teleinformatycznego, realizowanych przez niego procesów przetwarzania i przetwarzanych danych oraz systemów od nich zależnych w przestrzeni powiązanych logicznie i fizycznie systemów teleinformatycznych. Cyberbezpieczeństwo państwa z założenia musi się odnosić do systemów teleinformatycznych będących we władaniu państwa (jako całościowego organizmu administracji, instytucji, podmiotów i osób) lub zlokalizowanych w jego przestrzeni. Z tego autor wywodzi, że cyberprzestrzeń państwa to możliwa do wydzielenia, identyfikowalna część cyberprzestrzeni, której granice mogą zostać jednoznacznie określone. Cyberprzestrzeń państwa to możliwa do wydzielenia i określenia identyfikowalnych granic, stale zmienna w czasie struktura powiązanych logicznie i fizycznie systemów teleinformatycznych przynależna do państwa. Cyberbezpieczeństwo państwa jest zatem definiowane przez autora jako bezpieczeństwo możliwej do wydzielenia i określenia identyfikowalnych granic, stale zmiennej w czasie struktury powiązanych logicznie i fizycznie systemów teleinformatycznych, realizowanych przez nie procesów przetwarzania i przetwarzanych danych oraz

[81] Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012

systemów od nich zależnych, przynależnej do tego państwa, w przestrzeni powiązanych logicznie i fizycznie systemów teleinformatycznych.

Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej - prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni, wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców, prowadzenie walki informacyjnej w cyberprzestrzeni, współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych[82]. Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym[83].

Autor uważa również, że domeną oddziaływania cyberbezpieczeństwa jest cyberprzestrzeń i składające się na nią zasoby informacyjne i systemy teleinformatyczne realizujące usługi cyfrowe społeczeństwa informacyjnego, wspomagające działalność administracji i podmiotów realizujących zadania publiczne oraz stanowiące publiczną i prywatną teleinformatyczną infrastrukturę krytyczną, infrastrukturę teleinformatyczną wspomagającą funkcjonowanie pozostałych systemów infrastruktury krytycznej, czyli tzw. usług kluczowych[84]. Autor definiuje cyberprzestrzeń państwa również jako krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi[85]. Zapewnienie cyberbezpieczeństwa jest coraz istotniejszym i co-

[82] Strategia Bezpieczeństwa Narodowego RP (2014), BBN 2014, s. 35
[83] Doktryna cyberbezpieczeństwa RP, wyd. cyt., s. 14
[84] Mąkosa G., *Cyberbezpieczeństwo*, wyd. cyt., s. 111
[85] Mąkosa G., *Bezpieczeństwo cybernetyczne,* wyd. cyt., s. 123

raz trudniejszym zadaniem i wyzwaniem ze względu na dynamiczny rozwój technologii informatycznych, w tym technologii stosowanych do realizacji złośliwych i wrogich działań naruszających bezpieczeństwo cybernetyczne podmiotów, organizacji, instytucji i państw. Postęp w teleinformatyce sprawił, że cyberprzestrzeń nie tylko przyczynia się do rozwoju podmiotów państwowych i pozapaństwowych, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa[86]. Zdaniem autora rozwój technologii teleinformatycznych wpływa na rozwój negatywnych zjawisk w cyberprzestrzeni, tj. cyberprzestępczości, cyberkonfliktów, cyberwalki, walki informacyjnej, czy cyberwojny[87]. Realizowane ataki na systemy teleinformatyczne są formą materializacji zagrożeń, których źródłami mogą być hakerzy, przestępcy komputerowi, terroryści, szpiedzy przemysłowi czy specjalnie powoływane prywatne i państwowe grupy cyberprzestępcze. Działają oni z własnej motywacji lub na zlecenie innych osób, podmiotów, czy nawet państw[88]. Autor uważa, że odpowiedzialność w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni spoczywa na poszczególnych państwach i, w ramach zapewnienia bezpieczeństwa regionalnego lub sojuszniczego, na organizacjach bezpieczeństwa zrzeszających te państwa, jak np. NATO, a także na związkach państw, jak np. Unia Europejska, których członkiem jest Polska. Zapewnienie bezpieczeństwa cyberprzestrzeni jest aspektem technicznym, zależnym od technologii teleinformatycznych i telekomunikacyjnych i aspektem prawno-organizacyjnym, zależnym od europejskich i krajowych przepisów regulacji prawnych[89]. Najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane i kompleksowe, obejmujące wszystkie te obszary łączące wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny.

Cyberbezpieczeństwo jako obszar transsektorowy, odnosi się do bezpiecznego funkcjonowania państwa, jego struktur administracyjnych, podmiotów gospodarczych i obywateli w cyberprzestrzeni. Jak to ujmuje Doktryna cyberbezpieczeństwa RP, cyberprzestrzeń jest jednym z obszarów aktywności państwa, podmiotów prywatnych i obywateli. Cyberbezpieczeństwo państwa jako transsektorowy element bezpieczeństwa narodowego również powinno być zapewniane przez system bezpieczeństwa. System cyberbezpieczeństwa powi-

[86] Żebrowski A., *Bezpieczeństwo informacyjne,* wyd. cyt., **s**. 453
[87] Mąkosa G., *Cyberbezpieczeństwo*, wyd. cyt., s. 117
[88] Mąkosa G., *Bezpieczeństwo cybernetyczne systemów w czwartej rewolucji przemysłowej*, [w:] Czwarta rewolucja przemysłowa. Mity, paradygmaty i zastosowania. Tom 1 Kompetencje i baza narzędziowa Przemysłu 4.0, Wojciechowski Z., Zaskórski P. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 124
[89] Mąkosa G., *Bezpieczeństwo cyberprzestrzeni RP*, w: Studia Bezpieczeństwa Narodowego, Zeszyt 22, 2021, WAT, Warszawa 2020, s. 83

nien być zintegrowany, zarządzany (koordynowany) ponadresortowo i obejmować: podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa oraz podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych[90].

Cyberbezpieczeństwo jest ściśle związane z bezpieczeństwem systemów informacyjnych i bezpieczeństwem informacyjnym. Autor stwierdza, że cyberbezpieczeństwo państwa obejmuje bezpieczeństwo systemów teleinformatycznych oraz danych w nich przetwarzanych, stosowanych w przestrzeni cyfrowej, tak przez administrację, podmioty publiczne i gospodarcze, jak i przez obywateli. Cyberbezpieczeństwo dotyczy bezpieczeństwa systemu informacyjnego państwa lub inaczej ujmując zbioru wszystkich systemów informacyjnych kraju, a więc także bezpieczeństwa informacyjnego państwa w cyberprzestrzeni[91]. Bezpieczeństwo informacyjne państwa ma ścisły związek z jego bezpieczeństwem wewnętrznym i zewnętrznym. Wszechobecna globalizacja, rozwój społeczeństwa informacyjnego i technologii teleinformatycznych zmieniły obecne środowisko bezpieczeństwa państw, w tym również Rzeczypospolitej Polskiej[92]. Bezpieczeństwo informacyjne jest pojęciem szerokim, którego granice są trudne do zdefiniowania. Bezpieczeństwo informacyjne jak dotąd nie doczekało się jednoznacznej wykładni i wraz z towarzyszącym mu terminem bezpieczeństwo informacji jest używane w różnych znaczeniach[93]. Bezpieczeństwo informacyjne bywa określane jako zakres bezpieczeństwa przyjmujący wzrost znaczenia informacji w zachowaniu stabilności współczesnych, międzynarodowych systemów ekonomicznych oraz uwzględniający zabezpieczenie przed atakami sieciowymi, a także skutkami ataków fizycznych i jest plasowane obok bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego i ekologicznego[94]. Liderman K. uważa, że bezpieczeństwo informacyjne to uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji, pojęcie bezpieczeństwa informacyjnego dotyczy zatem podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych albo

[90] Doktryna Cyberbezpieczeństwa RP, wyd. cyt., s. 4, 9
[91] Mąkosa G., *Krajowy system cyberbezpieczeństwa RP*, s. 231
[92] Żebrowski A., *Bezpieczeństwo informacyjne,* wyd. cyt., s. 447
[93] Liderman K., *Bezpieczeństwo informacyjne*, wyd. cyt., s. 13
[94] Kowalkowski S. (red.), Niemilitarne zagrożenia bezpieczeństwa publicznego, AON, Warszawa 2011, s. 13, 14, 15

otrzymaniem informacji o nieodpowiedniej jakości[95]. Zdaniem Nowak E. i Nowak M. bezpieczeństwo informacyjne to stan warunków zewnętrznych i wewnętrznych dopuszczających, aby państwo swobodnie rozwijało swoje społeczeństwo informacyjne. Warunkami osiągnięcia bezpieczeństwa informacyjnego są:

- niezagrożone strategiczne zasoby państwa;
- decyzje organów władzy podjęte na podstawie wiarygodnych, istotnych informacji,
- niezakłócony przepływ informacji pomiędzy organami państwa;
- niezakłócone funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa;
- zagwarantowaną przez państwo ochronę informacji niejawnych i danych osobowych obywateli;
- zasadę, że prawo do prywatności obywateli jest nienaruszane przez instytucje publiczne;
- swobodny dostęp obywateli do informacji publicznej[96].

Rozwój technologii teleinformatycznych korzystnie wpływa na rozwój społeczeństwa informacyjnego oraz rozwój gospodarczy, niestety wpływa również na rozwój negatywnych zjawisk w cyberprzestrzeni. Żebrowski stwierdza, że postęp w teleinformatyce sprawił, że piąty wymiar konfrontacji, którym jest cyberprzestrzeń, nie tylko przyczynia się do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa[97].

2.3. Wyzwania, zagrożenia i incydenty cyberbezpieczeństwa

Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi stanowią cyberprzestrzeń. W cyberprzestrzeni realizowane są usługi cyfrowe obywateli - jako społeczeństwa informacyjnego, podmiotów gospodarczych i różnych organizacji, usługi wspomagające działalność administracji i podmiotów realizujących zadania publiczne. Równolegle do realizowanych działań o charakterze rozwojowym w cyberprzestrzeni realizowane są szkodliwe działania i działalność przestępcza, wywołująca ogromne szkody procesowe, finansowe, społeczne,

[95] tamże, s. 22
[96] Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin SA, Warszawa 2011, s. 103
[97] Żebrowski A., *Bezpieczeństwo informacyjne,* wyd. cyt., s. 453

w tym ograniczenie wzajemnego zaufania. Zagrożenia cybernetyczne dla systemów teleinformatycznych są powiązane z rozwojem technologii informatycznych i komunikacyjnych. Dzięki ogromnym możliwościom komunikacyjnym współczesnych mediów i przeniesieniu do Internetu aktywności biznesowej i prywatnej, cyberprzestępczość rozwija się szczególnie dynamicznie. W wyniku cyberprzestępczości podmioty gospodarcze, instytucje publiczne tracą ważne dla swojej działalności dane, co negatywnie wpływa na ich działalność, a ponadto skutkuje stratami wizerunkowymi, reputacyjnymi i relacyjnymi względem klientów. Ataki komputerowe bywają także wymierzone w systemy teleinformatyczne organizacji strategicznych dla gospodarki narodowej, co może wywoływać ogromne szkody systemowe, finansowe i wizerunkowe, ale również technologiczne, ekologiczne czy zdrowotne w skali kraju. Szkodliwa i przestępcza działalność w przestrzeni teleinformatycznej, stanowiącej połączenie m.in. komputerowych sieci firmowych, Internetu, urządzeń IoT (Internetu rzeczy) i osobistych urządzeń komputerowych (smartfonów, laptopów, tabletów, komputerów) osób prywatnych wywołuje ogromne szkody i zakłócenia funkcjonalne. Bezpieczeństwo cybernetyczne systemów teleinformatycznych jest podstawowym i koniecznym warunkiem dalszego rozwoju technologicznego, gospodarczego i społecznego państwa[98].

Ciągły rozwój technologii sprawia, że cyberataki są coraz bardziej wysublimowane, przyjmują nowe formy i są kierowane w coraz to nowsze obszary funkcjonalne otoczenia administracyjno-społeczno-gospodarczego państwa. Wyzwaniem jest więc zapewnienie odpowiednio wysokiego poziomu bezpieczeństwa. Warunkiem zapewniającym ciągłe utrzymywanie inicjatywy na poziomie strategicznym zarządzania bezpieczeństwem państwa jest przewaga informacyjna, która ma bezpośrednie przełożenie na koncepcje doktrynalne odnoszące się do infrastruktury cywilnej i wojskowej systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych[99]. Bezpieczeństwo informacyjne staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej[100]. Cyberprzestrzeń przenika do życia codziennego, jest obszarem działalności państwa, przedsiębiorstw, działalności międzynarodowej oraz, a może przede wszystkim, cyberprzestrzeń stała się także wymiarem prowadzenia walki. Coraz dokładniej w cyberprzestrzeni odbija się fizyczna rzeczywistość, występują w niej te same problemy, które od zarania dziejów nękają świat realny. Jednak, jako zupełnie nowa przestrzeń społeczna,

[98] Mąkosa G., *Bezpieczeństwo cybernetyczne,* wyd. cyt., s. 123
[99] Żebrowski A., *Bezpieczeństwo informacyjne,* wyd. cyt., s. 460
[100] Liderman K., *Bezpieczeństwo informacyjne*, wyd. cyt., s. 23

niesie ze sobą także nowe, niewystępujące dotąd zagrożenia, a ich rozpoznanie, zdiagnozowanie oraz opracowanie skutecznych sposobów przeciwdziałania to także nowe wyzwanie współczesności[101].

2.3.1. Cyberzagrożenia

Prowadzone ataki na systemy teleinformatyczne są formą materializacji zagrożeń stwarzanych przez ich źródła, którymi mogą być hakerzy, przestępcy komputerowi, terroryści, szpiedzy przemysłowi. Działają oni z własnej motywacji lub na zlecenie innych osób, podmiotów czy nawet państw[102]. Atakujący kierują się różnymi motywacjami, a ich działania mają różnorodne konsekwencje, zależnie od postawionego celu realizowanych złośliwych, szkodliwych czy wręcz przestępczych działań. Osoby indywidualne, podejmujące tego typu działalność, to najczęściej hakerzy czy crakerzy, których motywuje swoistego rodzaju wyzwanie, ego, zbudowanie swoistego rodzaju statusu, bunt, a także chęć zdobycia pieniędzy. Często działalność osób czy grup ma charakter przestępczy, a jej celem jest zniszczenie informacji, nielegalne ujawnienie informacji, korzyść finansowa, nieautoryzowana zmiana danych. Inną grupą zajmującą się cyberprzestępczością są szpiedzy przemysłowi reprezentujący agencje wywiadu, firmy, zagraniczne rządy czy inne służby rządowe, a ich motywacją jest np. zdobywanie przewagi konkurencyjnej czy szpiegostwo gospodarcze. Bardzo dużą grupę stanowią osoby z wewnątrz przedsiębiorstwa, są to na ogół osoby o niskich kompetencjach w zakresie bezpieczeństwa czy niestarannie wykonujące obowiązki w tym zakresie lub osoby niezadowolone, złośliwe, nieuczciwe czy zwolnieni pracownicy, które chcą wyrządzić krzywdę pracodawcy. Te osoby motywuje ciekawość, chęć podniesienia ego, działanie na rzecz wywiadu, spodziewana korzyść finansowa, zemsta. Przyczynami incydentów są również niezamierzone błędy i pomyłki. Inną, niezwykle ważną i niebezpieczną grupą są obce państwa i podmioty działające na ich zlecenie. Poprzez działalność w cyberprzestrzeni realizują oni swoje cele polityczne, gospodarcze czy (geo)strategiczne. Kolejną niezwykle niebezpieczną grupą są terroryści, którzy swoją działalność realizują z takich pobudek, jak szantaż, chęć zniszczenia, wykorzystania czy zemsta, a także pobudki polityczne i chęć zdobycia rozgłosu medialnego, i zwrócenia uwagi na siebie i głoszone

[101] Siek M., *Wojna informacyjna w cyberprzestrzeni*, [w:] Wybrane zagadnienia bezpieczeństwa międzynarodowego, Załoga W. (red.), Wydawnictwo: Wojskowa Akademia Techniczna, Warszawa 2018, s. 133
[102] Mąkosa G., *Bezpieczeństwo cybernetyczne,* wyd. cyt., s. 124

hasła[103]. Źródła zagrożeń, ich motywacje i odpowiadające im możliwe następstwa przedstawia tabela 1.

Tabela 1. Źródła zagrożeń, motywacje i możliwe następstwa

Źródła zagrożeń	Motywacja	Możliwe następstwa
Haker, cracker	Wyzwanie, ego, rebelia, status, pieniądze.	Haking, inżynieria społeczna, wtargnięcie do systemu, włamania, nieautoryzowany dostęp do systemu.
Przestępca komputerowy	Zniszczenie informacji, nielegalne ujawnienie informacji, korzyść finansowa, nieautoryzowana zmiana danych.	Przestępstwa komputerowe (np. cybernetyczne prześladowanie), czyn przestępczy (np. powtórne odtworzenie, podszycie się, przechwycenie), przekupstwo informacyjne, atak sieciowy (np. sfałszowanie adresu źródłowego), w targnięcie do systemu.
Terrorysta	Szantaż, zniszczenie, wykorzystanie, zemsta, korzyść polityczna, rozgłos medialny.	Bomba, terroryzm, wojna informacyjna, atak na system (np. rozproszona odmowa usługi DoS), penetracja systemu, naruszenie bezpieczeństwa systemu.
Szpiedzy przemysłowi (wywiad, firmy, zagraniczne rządy, inne służby rządowe)	Przewaga konkurencyjna, szpiegostwo gospodarcze.	Przewaga obronna, przewaga polityczna, wykorzystanie ekonomiczne, kradzież informacji, naruszenie prywatności, inżynieria społeczna, penetracja systemu, nieautoryzowany dostęp do systemu (dostęp do informacji klasyfikowanej, wewnętrznej i/lub związanej z technologią).
Osoby wewnętrzne (źle wyszkolone, niezadowolone, złośliwe, niedbałe, nieuczciwe, zwolnieni pracownicy)	Ciekawość, ego, wywiad, korzyść finansowa, zemsta, niezamierzone błędy i pomyłki (np. błąd wprowadzania danych, błąd programisty).	Napaść na pracownika, szantaż, przeszukiwanie informacji stanowiących własność, nadużycie komputerowe, oszustwo, kradzież, przekupstwo informacyjne, wprowadzanie fałszywych, zniekształconych danych, przechwycenie, złośliwy kod (np. wirus, bomba logiczna, koń trojański), sprzedaż danych osobowych, błędy w systemie, wtargnięcie do systemu, sabotaż systemu, nieautoryzowany dostęp do systemu.
Obce państwa i podmioty działające na ich zlecenie	Cele gospodarcze, polityczne, (geo)strategiczne.	Wojna informacyjna, cyberwojna, atak na system – paraliż działania, penetracja systemu, naruszenie bezpieczeństwa systemu, przewaga obronna, przewaga polityczna, wykorzystanie ekonomiczne, kradzież informacji, naruszenie prywatności, inżynieria społeczna, penetracja systemu, nieautoryzowany dostęp do systemu (dostęp do informacji klasyfikowanej, wewnętrznej i/lub związanej z technologią).

Źródło: opracowanie własne na podstawie PN-ISO/IEC 27005:2018

[103]Sołek-Borowska C., Mąkosa G., *Zapewnienie bezpieczeństwa i cyberbezpieczeństwa organizacjom – perspektywa empiryczna*, [w:] Gonciarski W., Woźniak J. (red.), Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Difin, Warszawa 2021, s. 155

Bezpieczeństwo cyberprzestrzeni, zdaniem Sienkiewicza, jest definiowane w odniesieniu do istniejących niebezpieczeństw, czyli zagrożeń, a więc sytuacji niepewnych i ryzykownych, w których możliwa i prawdopodobna jest utrata wartościowych zasobów (informacyjnych, technicznych, programowych) częściowo lub w pełni przez określonego ich dysponenta (właściciela, operatora, twórcy). Można mówić o bezpieczeństwie cyberprzestrzeni na poziomie[104]:

- społecznym (utrata określonych wartości w wyniku destrukcyjnych działań na określone zasoby infosfery i technosfery);
- informacyjnym (utrata wartościowych danych, informacji, wiedzy bądź skutki niepożądanych destrukcyjnych działań na zasobach infosfery);
- technicznym (utrata bądź obniżenie niezawodności zasobów technologicznych i programowych tworzących technosferę).

Podstawowe rodzaje zagrożeń cyberprzestrzeni zidentyfikowanych przez Sienkiewicza zostały przedstawione w tabeli 2 poniżej.

Tabela 2. Podstawowe rodzaje cyberzagrożeń

Zjawisko	Cechy charakterystyczne
Cyberprzemoc	Wykorzystanie cyberprzestrzeni w celu wymuszania odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści) sprzecznych z wartościami adresata.
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania aktów kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji).
Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) (efekt „Big Brother").
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych).
Cyberautorytaryzm	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa zgodnie z zasadami demokracji liberalnej (przeciwieństwem – cyberdemokracja).
Cyberwojna	Wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (cyberwarriors) i skierowane na zasoby i struktury państwa przeciwnika (również w działaniach innych niż wojna).

Źródło: Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni*, [w:] Metodologia badań bezpieczeństwa narodowego, Sienkiewicz P., M. Marszałek, H. Świeboda (red.), Tom III, Warszawa, 2012, s. 330

[104] Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni*, [w:] Metodologia badań bezpieczeństwa narodowego, Sienkiewicz P., M. Marszałek, H. Świeboda (red.), Tom III, Warszawa, 2012, s. 329

Jak to formułuje Sienkiewicz, cyberprzestrzeń jest przestrzenią realizacji podstawowych wartości ludzkich we wszystkich sferach działań społecznych. Jest swoistą zapowiedzią nowej cywilizacji informacyjnej, której obecnym przejawem jest rozwój społeczeństwa informacyjnego. Jest także „ciemna strona" cyberprzestrzeni jako źródła zagrożeń dla bezpieczeństwa międzynarodowego i narodowego. Musi być zatem przedmiotem racjonalnej polityki państwa, gdyż „cyberbezpieczeństwo" stanowi obecnie jeden z podstawowych filarów (segmentów) systemów bezpieczeństwa narodowego (regionalnego, globalnego). Istnieją bowiem systemy „cyberbroni" (*cyberweapons*), które w charakterze „broni" masowej dezorganizacji mogą być efektywnym środkiem „cyberwojny" (cyberwar, netwar)[105]. Cyberprzestrzeń stała się szerokim polem walki i wojny informacyjnej rozumianej jako „całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest[106]:

1. zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych;
2. zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych".

Technologie telekomunikacyjne i informatyczne rozwijają się niezwykle dynamicznie. Postęp w teleinformatyce sprawił, że cyberprzestrzeń nie tylko przyczynia się do rozwoju podmiotów państwowych i pozapaństwowych, czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa[107].

2.3.2. Cyberataki

Cyberprzestrzeń jest miejscem prowadzenia różnorodnych działań wymierzonych przeciwko instytucjom społecznym, gospodarczym, administracji, grupom społecznym i państwom. Cyberprzestrzeń jest o tyle istotna dla funkcjonowania państwa, że działania w niej prowadzone mają bezpośredni wpływ na wszystkie jego kluczowe elementy skła-

[105] tamże, s. 335
[106] Sienkiewicz P., *Wizje i modele wojny informacyjnej*, [w:] Społeczeństwo informacyjne – wizja czy rzeczywistość?, Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003, s. 375
[107] Żebrowski A., *Bezpieczeństwo informacyjne,* wyd. cyt., **s**. 453,

dowe. wykorzystywane w tym celu są takie narzędzia, jak: cyberterroryzm, cyberszpiegostwo, haktywizm oraz operacje zbrojne w cyberprzestrzeni, jak zauważa Bernacik [108]. Zdaniem Sieka w cyberprzestrzeni miesza się to, co fizyczne, z tym, co wirtualne, zacierają się też granice między tym, co militarne, a tym, co cywilne, co ma istotne znaczenie z perspektywy definiowania działań prowadzonych w tym środowisku. Działania w cyberprzestrzeni mogą przybierać formę ataków z zastosowaniem prostych, powszechnych metod jak i działań zawansowanych, wyrafinowanych i długotrwałych. Największym wyzwaniem stają się jednak ataki - kampanie typu APT (Advanced Persistent Threat), które wg Sieka, można uznać za przejawy walki w cyberprzestrzeni. Ataki typu APT nie są zwykle pojedynczymi działaniami, ale są realizowane jako całe kampanie dobrze skoordynowane, wykorzystujące różne techniki ataków, które mają jasno określony cel, a ich prowadzenie może być rozciągnięte w czasie. Stopień zaawansowania ataków to niejedyny wyróżnik cyberwojny, liczy się również to, jak wysoce jest ustrukturyzowany podmiot przeprowadzający działania w cyberprzestrzeni. Wysoko ustrukturalizowane ataki cyfrowe w cyberprzestrzeni stanowią największe zagrożenie dla bezpieczeństwa państwa i obywateli, a jednocześnie obrona przed nimi jest dziś wyzwaniem, jakie każde państwo na świecie oraz organizacje muszą podjąć dla zwiększenia bezpieczeństwa[109]. Ataki w cyberprzestrzeni odznaczają się dużą dynamiką zmian, cechują je: asymetryczność, problem atrybucji, a także dostępność i podatność celów, co powoduje narastanie zainteresowania cyberwojną grup wysoce ustrukturyzowanych, w tym również organów państwowych. Graczami cyberwojny jest wiele państw, które nie tylko prowadzą agresję w cyberprzestrzeni (działając siłą przymusu), lecz także stosują techniki uzależniania od siebie słabszych (działając siłą gospodarki rynkowej). To wszystko sprawia, że zjawiska wysoce ustrukturyzowanych ataków cyfrowych powinny być uznane za jedno z największych zagrożeń współczesności, a przeciwstawienie się im oraz zabezpieczenie przed nimi za jedno z największych wyzwań[110].

Cyberataki i cyberprzestępczość są obecne w przestrzeni politycznej i gospodarczej, odkąd upowszechniła się technologia telekomunikacyjna i niestety będą nam towarzyszyć również w przyszłości. W ostatnich 25 latach miało miejsce wiele aktów cyberprzestępczości, cyberkonfliktów, cyberwalki czy cyberwojny, które ciągle ewoluują, również w zakresie

[108] Bernacik B., *Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej*, [w:] Roman Ł, Krassowski K., Sagan S., Wróblewski D. (red.), Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2018, s. 13
[109] Siek M., Wojna informacyjna, wyd. cyt., s. 137, 138, 139
[110] tamże, s. 146

stosowanej technologii informatycznej. Przegląd zdarzeń zaistniałych w przeszłości powinien przyczynić się do zaprogramowania i wdrożenia odpowiednich działań, aby zapewnić cyberbezpieczeństwo w obecnym czasie i najbliższej przyszłości. Zestawienie przykładowych, znanych w domenie publicznej, cyberataków na świecie oraz ich charakteru, skali i skutków z okresu ostatnich 25 lat przedstawia tabela 3.

Tabela 3. Wybrane cyberataki na świecie w latach 1997 - 2022

1997, Stany Zjednoczone, Transport lotniczy. Wyłączenie na lotnisku w Worcester linii telefonicznych obsługujących wieżę kontrolną, służby ochrony lotniska, lotniskowej straży pożarnej, służby pogodowej. Unieruchomiony system oświetlenia pasa startowego.	1998-2000, Stany Zjednoczone, Atak rosyjskich hakerów na serwery wielu amerykańskich instytucji rządowych i prywatnych, w tym m.in. Pentagonu, NASA, Departamentu Energii uniwersytetów oraz instytucji badawczych.
1999, Australia, Dezaktywacja systemu alarmowego, co wprowadziło zakłócenia w dostawie wody pitnej i jej zanieczyszczenie.	1999, Serbia, Infrastruktura teleinformatyczna. NATO dokonało wielu ataków, których celem było zablokowanie infrastruktury teleinformatycznej Serbii. W odwecie serbscy hakerzy podjęli wiele prób zablokowania serwerów Paktu Północnoatlantyckiego.
2003, Stany Zjednoczone, Serwery rządowe i korporacyjne. Ataków chińskich hakerów w celu pozyskania poufnych informacji m.in. z NASA, Lockheed-Martin czy Redstone Arsenal. Chińczycy zdobyli informacje m.in. na temat programu F-35 Joint Strike Fighter.	2003, Stany Zjednoczone, Kanada, Awaria systemu energetycznego dotyczyła obszaru zamieszkałego przez około 50 mln osób na terytorium dwóch krajów. Całkowity koszt strat wyniósł między 4 a 10 mld dolarów amerykańskich.
2003, Stany Zjednoczone, Infekcja systemu obsługującego ruch kolejowy kompanii CSX, obsługującej 23 stany amerykańskie. Awaria spowodowała odwołania pociągów i opóźnienia w transporcie kolejowym.	2006, Stany Zjednoczone, Przejęcie kontroli nad głównym serwerem zarządzającym systemem filtracji wody, zainstalowanie wirusa i oprogramowania szpiegującego.
2007, Estonia, Rosja sparaliżowała na pewien czas funkcjonowanie ważnych instytucji państwowych i prywatnych, sieci energetycznych i banków.	2007, Syria, Izrael zaatakował sieci komputerowe i telekomunikacyjne, przejął kontrolę m.in. nad systemami radarowymi obrony powietrznej. Dokonał bombardowania syryjskiego ośrodka wojskowego bez zaalarmowania syryjskiej obrony przeciwlotniczej.
2008, Gruzja, Osetia, Gruzja przejęła osetyńskie media i nadawała treści. Rosja – przejęcie gruzińskich stron www instytucji rządowych, naukowych i komercyjnych.	2008, Bliski Wschód - transfer tajnych danych wojskowych z amerykańskich sieci wojskowych.
2008, Turcja, Atak na rurociąg - wyłączenie systemu alarmowego i wywołanie znacznego wzrostu ciśnienia i eksplozji.	2009, Sieci informatyczne instytucji państwowych, polityków, korporacji czy instytucji badawczych 103 krajów.
2009, Stany Zjednoczone, atak na amerykańskie korporacje - uzyskanie nowoczesnych technologii oraz specjalistycznego oprogramowania.	2010, Iran, Elektrownia atomowa – zakłócenia funkcjonowania.
2014, Niemcy, Atak na hutę - nieplanowane wyłączenie pieca i duże zniszczenia.	2015-2016, Ukraina, cyberataki na sektor energetyczny Ukrainy. W ich wyniku, dostępu do energii elektrycznej zostało pozbawionych kilka milionów obywateli.

2016, USA, zmasowane ataki DDoS zainfekowanymi kamerkami internetowymi. Serwisy Netlifx, Payplay czy Twitter miały duże problemy z działaniem.	2017, świat, Ataki ransomware: WannaCry - częściowy paraliż brytyjskiej służby zdrowia, swym zasięgiem objął ponad 300 tys. komputerów w 99 krajach. NotPetya - dotknięte atakiem zostały największe firmy na świecie, straty rzędu 10 mld.
2018, Arabia Saudyjska, atak na przedsiębiorstwo petrochemiczne. Niemal doszło do całkowitego zniszczenia i śmierci wielu pracowników.	08.2018, Finlandia, atak DDoS na fińskie strony rządowe i ich paraliż.
12.2018, USA, Irański cyberodwet za nałożenie kolejnych sankcji przez USA, włamanie do wiadomości e-mail urzędników.	12.2018/01.2019, Niemcy, wyciek danych osobowych oraz dokumentów przedstawicieli Bundestagu.
12.2020, Finlandia, cyberatak hakerski na parlament i pocztę e-mail pracowników i posłów. Celem kampanii mogło być szpiegostwo.	12.2020 (wykrycie – działanie trwało ok. 3 lat), USA, cyberatak na infrastrukturę IT rządu i podmioty odpowiadające za infrastrukturę krytyczną (nim. 15), platformę Microsoft 365 Cloud. Działania o charakterze „klasycznego szpiegostwa". Wykorzystano oprogramowanie do zarządzania IT firmy SolarWinds, bazujące na Microsoft. Rosja.
12.2020, USA, m. Independence, atak hakerski ransomware, sparaliżowane zostały podstawowe usługi świadczone przez lokalną administrację.	02.2021, EU, USA, ataki hakerów na sieci komputerowe 150 firm w Europie i USA. Szkody oszacowano na ponad 80 mln dolarów.
02.2021 (wykrycie), EU, USA, ataki na banki i instytucje finansowe - międzynarodowa grupa hakerska (botnet Emotet). Doprowadziły do łącznych strat w wysokości 2,5 mld dolarów.	01.2021, Węgry, seria cyberataków na strony rządowe. Spowodowały zakłócenia w działaniu niektórych portali rządu i administracji publicznej.
02.2021, Brazylia, spółka Eletrobras odpowiedzialna za produkcję i przesył energii elektrycznej została zhakowana, a część jej systemów zainfekowana złośliwym oprogramowaniem ransomware. Skutecznie udało się zneutralizować wirusa.	02-03.2021, Ukraina, seria ataków na rządowe strony internetowe organów bezpieczeństwa i obrony, innych instytucji państwowych i przedsiębiorstw strategicznych; ataki na elektroniczny system obiegu dokumentów w administracji publicznej, duży atak na tajne rządowe zasoby.
02.2021(wykrycie), Francja, włamanie do firm działających w obszarach IT oraz hostingu– działanie 2017-20. Hakerzy współpracujący z rosyjskim wywiadem wojskowym GRU.	01.2020-02.2021, kampania hakerów rządu Korei Północnej w podmioty sektora przemysłu obronnego z kilkunastu państw. Ich głównym celem była kradzież poufnych danych.
02.2021 (wykrycie), Pakistan, kraje Azji Płd, Cyberkonflikt indyjsko-pakistański. Działania Indii wymierzone w personel powiązany z pakistańskimi władzami wojskowymi, członkami administracji związanej z badaniami nuklearnymi oraz indyjskimi urzędnikami wyborczymi w Kaszmirze.	02.2021, Polska, Kraków, zhakowano Urząd Marszałkowski w Krakowie. Zaszyfrowana została część systemów instytucji, a hakerzy zażądali okupu za ich odblokowanie. Doszło do naruszenia bezpieczeństwa danych osobowych m.in. klientów.
02.2021, Francja, firma Bombardier padł ofiarą hakerów - uzyskali dostęp do wewnętrznych danych na temat pracowników, klientów oraz dostawców koncernu.	02-03.2021, Francja, atak na szpitale złośliwym ransomware – blokada systemów IT szpitali, paraliż pracy, żądania okupu.
03.2021, Czechy, Praga, atak na systemy administracji publicznej miasta, czasowa blokada pracy.	08.2020, 03.2021, Norwegia, ataki na norweski parlament, kradzież danych. Rosja.
03.2021 Australia, atak na stację telewizyjną - emisja została przerwana, zaatakowano wewnętrzny system IT i strony internetowe stacji.	03.2021, USA, atak na firmę (Honeywell) produkującą dla sektora energetycznego i lotniczego.

01.2020-03.2021, Indie, chińska grupa hakerów uderza w infrastrukturę krytyczną Indii – energetykę i porty morskie.	04.2021, Francja, chińskie i rosyjskie cyberataki na edukacyjne platformy do zdalnego nauczania.
04.2021 USA, wyciek danych osobowych z facebook (500 mln) i linkedin (500 mln).	04.2021, EU, Bruksela, cyberataki na wiele instytucji EU, w tym Komisję Europejską.
04.2021, Portugalia, Rosja i Chiny przeprowadziły wiele cyberataków na infrastrukturę urzędów państwowych. Paraliż pracy państwowych instytucji, kradzież poufnych informacji. Chińskie ataki na infrastrukturę informatyczną służby zdrowia. Rosyjskie ataki na główne instytucje państwowe.	05.2021, USA, Rosja przeprowadziła atak ransomware na systemy przesyłowe paliw płynnych dwóch korporacji w południowych stanach USA paraliżując dostawy surowców do rafinerii i dystrybucje paliw do stacji, co wywołało paraliż. Atak skuteczny dzięki zainfekowaniu ok. 2 lat wcześniej oprogramowania służącego do realizacji usług serwisowych IT. Każda z amerykańskich korporacji zapłaciła rosyjskim hakerom okup w wysokości ok. 5 mln USD.
od 02.2022, Ukraina, Rosja zaatakowała w sposób konwencjonalny – kinetyczny i cybernetyczny Ukrainę. Prowadzi ataki na systemy teleinformatyczne infrastruktury krytycznej oraz m.in. na strony internetowe administracji państwowej i mediów. Ukraina broni swoich systemów teleinformatycznych, atakując również systemy strony rosyjskiej. W akcję obrony Ukrainy włączyły się międzynarodowe społeczności, takie jak m.in. Anonymouse, które prowadzą ataki cybernetyczne na rosyjskie systemy teleinformatyczne infrastruktury krytycznej oraz m.in. ataki na strony internetowe administracji państwowej i mediów. Rosja w odwecie za pomoc Ukrainie atakuje kraje sąsiedzkie, należące do UE i NATO oraz inne kraje, niosące pomoc, w tym Polskę.	

Źródło: Opracowanie własne na podstawie: Narodowy Program Ochrony Infrastruktury Krytycznej 2018, Załącznik 1 Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, RCB; www.cyberdefence24.pl [dostęp 20.03.2021, 30.10.2022]

Działania cyberprzestępcze mają również miejsce w polskiej cyberprzestrzeni. Zestawienie przykładowych, znanych w domenie publicznej, działań przestępczych w Polsce i ich skutków z okresu 2017-2019 przedstawia tabela 4.

Zestawienie zawiera tylko informacje o zdarzeniach, o których informowały media. Należy zdawać sobie sprawę, że ogromna ilość zdarzeń nie zostaje nigdy wykryta przez ofiary ataków, a zdarzenia wykryte są nieujawniane do wiadomości publicznej z obawy przed negatywnymi skutkami na prowadzoną działalność, stratami wizerunkowymi, reputacyjnymi i relacyjnymi względem klientów i partnerów biznesowych.

Tabela 4. Wybrane cyberataki w Polsce w latach 2017/2019

2017 Polska, Infekcja strony KNF - umieszczono oprogramowanie szpiegowskie nakierowane na dane wrażliwe dla sektora finansowego.	2017 Polska**,** z jednego z polskich szpitali wyciekły dane 50 tys. pacjentów**.**
2018 Polska, BackSwap atakujący klientów pięciu czołowych polskich banków - program zmieniał numery rachunków i wykradał pieniądze posiadacza konta.	2018 Polska, Podszywanie się pod banki – kradzież danych uwierzytelniających, instalowanie złośliwego oprogramowania, przejmowanie kontroli **(**BZ WBK (Santander Bank Polska), mBank, ING Bank Ślaski, PKO Bank Polski).
2018 Polska, Aplikacja „Bankowość uniwersalna Polska" w Google Play – kradzież danych uwierzytelniających**.**	2018 Polska, Podszywanie się pod DotPay i Przelewy24.pl – kradzież danych i opróżnienie kont bankowych.
2021, Polska, wyciek danych studentów Politechniki Warszawskiej ze strony portalu edukacyjnego PW.	04.2019 Polska, Kradzież danych osób z loterii "PIT w Gdańsku. Się opłaca!"
02.2021, Polska, Kraków, zhakowano Urząd Marszałkowski w Krakowie. zaszyfrowana została część systemów instytucji, a hakerzy zażądali okupu za ich odblokowanie. Doszło do naruszenia bezpieczeństwa danych osobowych m.in. klientów.	07.2021, Polska, kradzież i upublicznianie w serwisach zagranicznych korespondencji elektronicznej członków rządu i rządzącej partii politycznej, prowadzonej z serwerów dostawcy usług pocztowych wp.pl, dzięki przejęciu środków uwierzytelniających posiadaczy kont.

Źródło: Opracowanie własne na podstawie: www.cyberdefence24.pl [dostęp 20.03.2021, 30.10.2022]

Z analizy przedstawionych zestawień wynika, że ataki przeprowadzone na świecie mają charakter cyberprzestępczości, cyberkonfliktów, cyberwalki czy wręcz cyberwojny, a incydenty, które wystąpiły w Polsce i zostały ujawnione, to akty cyberprzestępczości. Jednakże, niezależnie od charakteru ujawnionych incydentów trzeba zdawać sobie sprawę, że systemy teleinformatyczne funkcjonujące w Polsce, a więc polska cyberprzestrzeń, są w trybie ciągłym poddawane różnorodnym atakom[111].

Bogate w informacje o incydentach cyberbezpieczeństwa są raporty powołanych do monitorowania bezpieczeństwa polskiej cyberprzestrzeni jednostek CERT/CSIRT – CSIRT GOV, prowadzony przez ABW, CERT Polska/CSIRT NASK, prowadzony przez NASK-PIB oraz CERT Orange, prowadzony przez Orange Polska. Dane te nie zostały tu przytoczone, żeby nie generować natłoku danych i szumu informacyjnego. Przedstawienie dodatkowych informacji o incydentach nie wniosłoby nic nowego, ponieważ informacje o incydentach cyberbezpieczeństwa są przedstawiane, żeby dać pogląd, że w polskiej cyberprzestrzeni również zachodzą szkodliwe i wrogie zdarzenia. Wątek incydentów w polskiej cyberprzestrzeni zostanie rozwinięty w dedykowanym temu kolejnym podrozdziale.

[111] Mąkosa G., *Cyberbezpieczeństwo,* wyd. cyt., s. 119

Ataki cybernetyczne ciągle ewoluują, również w zakresie stosowanej technologii informatycznej. Przegląd zdarzeń zaistniałych w przeszłości powinien przyczynić się do zaprogramowania i wdrożenia odpowiednich działań, aby zapewnić cyberbezpieczeństwo w obecnym czasie i najbliższej przyszłości.

2.3.3. Cyberwalka i cyberwojna

Działania w przestrzeni informacyjnej, operujące zarówno w sferze informacji, jak i w sferach społecznej i technologicznej są znamienne dla obecnych czasów, związanych z dynamicznym rozwojem technologii informacyjnych i ich wszechstronnego zastosowania, w tym wykorzystania w działaniach walki lub wojny informacyjnej. Termin walki informacyjnej został użyty w 1976 roku przez Thomasa Rona, definiującego walkę informacyjną jako działania prowadzone na poziomie strategicznym, operacyjnym i taktycznym w pełnym spektrum, tj. w czasie pokoju, kryzysu, eskalacji kryzysu, konfliktu, wojny, zakończenia wojny i rekonstrukcji/odbudowy, realizowane między konkurentami, przeciwnikami lub wrogimi stronami używającymi informacji do osiągnięcia zamierzonych celów[112].

Wojna w Zatoce Perskiej (1991) została określona, jako pierwsza wojna informacyjna („The First Information War") z powodu roli i wielości użytych na polu walki – w niespotykanej wcześniej skali – systemów i technologii informacyjnych. W publikacjach naukowych pojawiły się liczne propozycje kategorii opisu tego nowego zjawiska, takie jak infowar, cyberwar, netwar w kręgu RAND, a przede wszystkim tzw. Model walki Wardena, w którym zaproponowano nowy, piąty (obok: lądu, wody, powietrza, i kosmosu) wymiar – cyberprzestrzeń (*cyberspace*)[113]. Na szczycie NATO w Warszawie w lipcu 2016 r. oficjalnie uznano, że cyberprzestrzeń jest nowym, piątym środowiskiem walki po obszarze lądowym, przestrzeni powietrznej, obszarach morskich i kosmosie, w której można toczyć walkę i wojnę informacyjną. Cyberprzestrzeń jest obecnie traktowana jako przestrzeń, w której już w tej chwili prowadzone są działania zbrojne, mające na celu wpływanie na inne państwa w celu osiągnięcia własnych celów. Jest to niezmiernie obiecujący obszar dla wszystkich aktywnych „graczy", których celem jest np. destabilizacja gospodarcza, wpływ polityczny na wybrane kraje (wpływ na wyniki wyborów), jak również tworzenie przewagi informacyjnej nad pozostałymi państwami[114].

---

[112] Siek M., *Wojna informacyjna,* wyd. cyt., s. 135
[113] Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni,* wyd. cyt., s. 321
[114] Bernacik B., *Nauka i najnowsze narzędzia, wyd. cyt.*, s. 12

Materializacją zjawiska walki w cyberprzestrzeni był atak przeprowadzony przez Rosję na Estonię w 2007 r., w wyniku którego w czasie trwającej trzy tygodnie kampanii cyberataków zablokowano strony internetowe wielu instytucji publicznych i banków oraz naruszono elementy infrastruktury krytycznej. W 2008 r. nastąpiły kolejne działania w cyberprzestrzeni nakierowane na działanie poszczególnych państw. W pierwszym przypadku dotyczyły Gruzji i Osetii - Gruzja przejęła osetyńskie media i nadawała swoje treści. W reakcji Rosja przejęła strony www gruzińskich instytucji rządowych, naukowych i komercyjnych. W drugim przypadku wrogie działania w cyberprzestrzeni skierowano przeciwko Kirgistanowi. Zdarzenia w Estonii zostały nazwane pierwszą wojną w cyberprzestrzeni lub też pierwszą cyberwojną, a wydarzenia w Gruzji – drugą. Wydarzenia te zapoczątkowały powszechność tego typu zjawisk w cyberprzestrzeni. Działania w cyberprzestrzeni prowadzone są w sposób zorganizowany i przemyślany na niekorzyść drugiej strony, również przez aktorów państwowych. W lutym 2022 r. Rosja zaatakowała w sposób konwencjonalny – kinetyczny i cybernetyczny Ukrainę. Agresja rosyjska w sferze cybernetycznej przyjęła formę ataków na systemy teleinformatyczne infrastruktury krytycznej oraz m.in. ataki na strony internetowe administracji państwowej i mediów. Strona ukraińska prowadziła i prowadzi obronę swoich systemów teleinformatycznych, atakując również systemy strony rosyjskiej. W akcję obrony Ukrainy włączyły się międzynarodowe społeczności, takie jak m.in. Anonymouse, które prowadzą ataki cybernetyczne na rosyjskie systemy teleinformatyczne infrastruktury krytycznej oraz m.in. ataki na strony internetowe administracji państwowej i mediów. Rosja w odwecie za pomoc Ukrainie atakuje kraje sąsiedzkie, należące do UE i NATO oraz inne kraje, niosące pomoc, w tym Polskę. Działania w cyberprzestrzeni w związku z agresją Rosji na Ukrainę i zaangażowanie szerszego grona krajów zostały nazwane w mediach „pierwszą wojną światową w cyberprzestrzeni”[115], czyli pierwszą cyberwojną światową.

Definicje cyberwojny wyprowadzone przez badaczy zostały zestawione w tabeli 5 poniżej.

[115] Przykładowe publikacje, gdzie użyto zwrotów „cyberwojna światowa”, „wojna w cyberprzestrzeni”: https://pap-mediaroom.pl/nauka-i-technologie/cybersec-2022-trwa-pierwsza-cyberwojna-swiatowa (18.05.2022), https://spidersweb.pl/plus/2022/03/cyberwojna-rosja-ukraina-anonymus-cyberataki (03.2022), https://www.rp.pl/publicystyka/art36702071-izabela-albrycht-pierwsza-cyberwojna-swiatowa (15.07.2022), https://www.money.pl/gospodarka/trwa-wojna-w-cyberprzestrzeni-hakerzy-zaatakowali-ponad-6-tys-rosyjskich-stron-6796770060237312a.html (01.08.2022)

Tabela 5. Definicje cyberwojny

Lp.	Autor (rok)	Definicja cyberwojny
1	L. Alford (2001)	Wszelkie działania zmierzające do zmuszenia przeciwnika do wypełnienia woli narodowej, realizowane przeciwko procesom sterującym oprogramowaniem w systemach przeciwników.
2	J. Carr (2012)	Sztuka i nauka walki bez walki; pokonania przeciwników bez rozlewania krwi.
3	R. Parks D. Duggan (2011)	Kombinacja ataku i obrony komputerowej oraz specjalnych operacji technicznych.
4	J. Arquilla D. Ronfeldt (1993)	Prowadzenie i przygotowanie do prowadzenia operacji wojskowych zgodnie z zasadami dotyczącymi operacji informacyjnych; zakłócenie, jeśli nie zniszczenie systemów informacyjnych i komunikacyjnych, szeroko zdefiniowanych, obejmujących nawet kulturę wojskową, na której opiera się przeciwnik, aby dowiedzieć się: kim jest, gdzie jest, co może zrobić, kiedy, dlaczego walczy, jakim zagrożeniom przeciwdziałać najpierw itd.; próba poznania wszystkiego na temat przeciwnika, przy jednoczesnym utrudnieniu zdobywania wiedzy o sobie.
5	P. Cirnish, D. Livingstone, D. Clemente, C. Yorke (2010)	Konflikt między państwami, ale może również angażować podmioty niepaństwowe na różne sposoby, w którym zwykle trudno jest kierować precyzyjną i proporcjonalną siłą; cel może być wojskowy, przemysłowy lub cywilny albo może nim być serwer obsługujący wielu różnych klientów, a tylko jeden z nich jest celem zamierzonym.
6	M. Taddeo (2012)	Działania wojenne oparte na pewnych zastosowaniach technologii informacyjno-komunikacyjnych w ramach ofensywnej lub defensywnej strategii militarnej zatwierdzonej przez państwo i mające na celu natychmiastowe zakłócenie lub kontrolowanie zasobów wroga; prowadzone w środowisku informacyjnym, z agentami i celami, zarówno w zakresie fizycznych, jak i nie fizycznych celów; poziom przemocy tych działań może być różny w zależności od okoliczności.
7	C. Billo (2004)	Operacje ofensywne i defensywne jednostek zorganizowanych wzdłuż granic państwowych, wykorzystujących komputery do atakowania innych komputerów lub sieci za pomocą środków elektronicznych.
8	R.A. Clarke (2010)	Działania państwa narodowego polegające na penetracji komputerów lub sieci innego narodu w celu spowodowania szkód lub zakłóceń.

Źródło: M. Siek, *Wojna informacyjna w cyberprzestrzeni*, [w:] Wybrane zagadnienia bezpieczeństwa międzynarodowego, Załoga W. (red.) Wydawnictwo: Wojskowa Akademia Techniczna, Warszawa 2018, s. 141

Za Siekiem należy stwierdzić, że cyberwojna musi nosić znamiona wojny (toczonej dla celów politycznych przez podmioty państwowe – wysoce ustrukturyzowane). Nie można jej utożsamiać z cyberterroryzmem lub cyberprzestępczością, szpiegostwem, działalnością hakerów. W cyberwojnie należy się spodziewać zastosowania na jeszcze większą skalę działań prowadzonych przeciwko zasobom i systemom informacyjnym znajdującym się w cyberprzestrzeni[116]. Głównym kryterium klasyfikacji działań w cyberprzestrzeni i rozstrzyganiu, czy dane działania w cyberprzestrzeni są cyberwojną, cyberwalką, czy inną formą konfliktu jest analiza podmiotu prowadzącego działania oraz jego intencji. Wszystkie działania

[116] Siek M., Wojna informacyjna, wyd. cyt., s. 139

w cyberprzestrzeni noszą znamiona walki, która toczy się jedynie w tym specyficznym środowisku, jakim jest cyberprzestrzeń. Z cyberwojną mamy do czynienia jedynie, gdy podmiot jest państwowy (posiada zdolność deklaracji wojny i ją wypowiedział). W innych przypadkach mówimy o cyberwalce, cyberterroryzmie, cyberaktywiźmie itp.[117].

Wobec narastającej skali wyzwań, zagrożeń i incydentów w cyberprzestrzeni, mających charakter cyberprzemocy, cyberprzestępczości, cyberterroryzmu, cyberkonfliktów, cyberwalki czy cyberwojny przed państwami i ich systemami bezpieczeństwa narodowego i systemami cyberbezpieczeństwa stoją ogromne, ciągłe zmieniające się i rosnące wyzwania i odpowiedzialność.

2.4. Bezpieczeństwo polskiej cyberprzestrzeni

Cyberataki i cyberprzestępczość są obecne w przestrzeni publicznej, politycznej i gospodarczej, odkąd upowszechniła się technologia telekomunikacyjna i będą zachodzić również w przyszłości. Możliwe skutki przeprowadzonych cyberataków na systemy teleinformatyczne mogą być bardzo rozległe i szkodliwe nie tylko dla podmiotów życia gospodarczego, ale i całych gospodarek krajowych. Należy zdawać sobie sprawę, że ogromna ilość zdarzeń nie zostaje nigdy wykryta, a zdarzenia wykryte często są nieujawniane z obawy przed negatywnymi konsekwencjami takiego ujawnienia.

Niezwykle istotne jest prowadzenie stałego monitoringu zdarzeń, analiz podatności i zabezpieczania systemów teleinformatycznych dla zapewnienia bezpieczeństwa cyberprzestrzeni. Regulacje ustawy o krajowym systemie cyberbezpieczeństwa[118] ustanowiły wyspecjalizowane, dedykowane do monitorowania bezpieczeństwa cyberprzestrzeni i adekwatnego reagowania na zdarzenia i incydenty jednostki CSIRT (ang. Computer Security Incident Responce Team). Wcześniej w Polsce funkcjonowały jednostki typu CERT (ang. Computer Emergency Responce Team), prowadzone przez NASK i ABW, które zmieniły status na CSIRT w związku z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa, powołującym takie organy do istnienia. Dodatkowo został powołany CSIRT sektora militarnego. Powstałe jednostki, to: CSIRT NASK (CERT Polska) - prowadzony przez NASK-PIB (Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy), CSIRT GOV - prowadzony przez Agencję Bezpieczeństwa Wewnętrznego, w której kręgu

[117] tamże, s. 143
[118] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

zainteresowań są podmioty administracji rządowej i jednostki centralne oraz operatorzy infrastruktury krytycznej oraz CSIRT MON – prowadzony przez Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), dedykowaną jednostkę w strukturach Wojska Polskiego. Jednostki CSIRT GOV i CSIRT NASK/CERT Polska corocznie opracowują raporty ze swojej działalności oraz prezentują stan bezpieczeństwa cyberprzestrzeni RP.

2.4.1. Zapewnienie cyberbezpieczeństwa przez CERT Polska – CSIRT NASK

Jednostka CERT Polska (CSIRT NASK) publikuje corocznie raporty na temat stanu polskiego cyberbezpieczeństwa i informacje dotyczące obsłużonych przez nią incydentów bezpieczeństwa – „*Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*". Przedstawiane w raportach dane od wielu lat wykazują sukcesywny wzrost liczby incydentów. Zgodnie z danymi opublikowanymi w raportach z ostatnich lat CERT Polska w roku 2021 zarejestrował 116 071 zgłoszeń, spośród których wytypowano 29 483 incydenty, w roku 2020 obsłużył 34 555 zgłoszeń, które po przeanalizowaniu i pogrupowaniu wyodrębniły 10 420 incydentów, w roku 2019 – 22 343 zgłoszenia, z czego 6484 stanowiło incydenty, a w roku 2018 – 19 439 zgłoszeń, spośród których zarejestrowano 3739 incydentów. CERT Polska odnotował w roku 2021 wzrost liczby obsłużonych incydentów na poziomie 182% w porównaniu do roku poprzedniego, w roku 2020 odnotował wzrost liczby obsłużonych incydentów na poziomie 60,7% w porównaniu do roku 2019 i wzrost liczby obsłużonych incydentów w roku 2019 na poziomie 73% w porównaniu do 2018 r.[119]. Szczegółowe informacje o zgłoszeniach i zidentyfikowanych przez CERT Polska incydentach w latach 2015-2021 zostały przedstawione w tabeli 6 i na rysunku 2 poniżej.

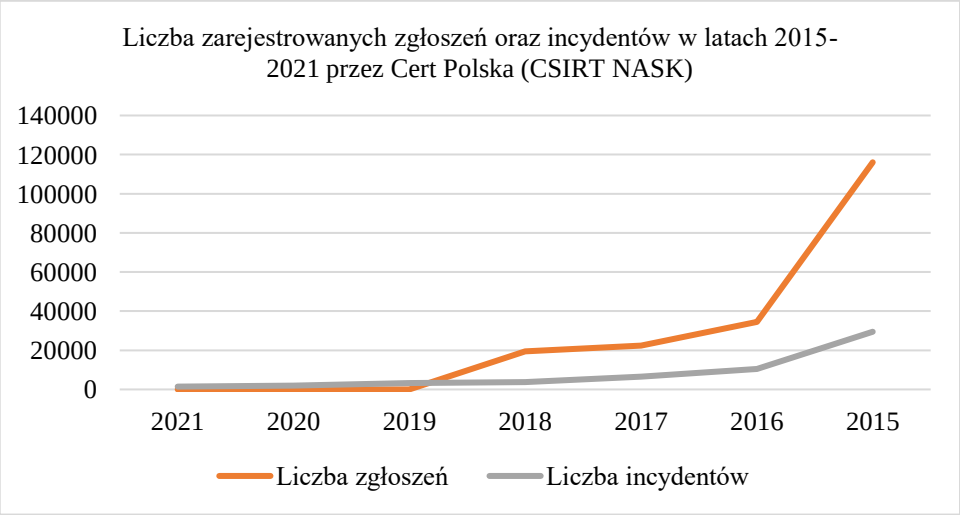
Tabela 6. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2021 przez Cert Polska (CSIRT NASK)

Zgłoszenia / Rok	2021	2020	2019	2018	2017	2016	2015
Liczba zgłoszeń	116.071	34.555	22.343	19.439			
Liczba incydentów	29.483	10.420	6.484	3.739	3.182	1.926	1.456

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB, 2022, s. 20, 2021, s. 24, 2020, s. 12, 2019, s. 10

[119] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 20, 2021, s. 24, 2020, s. 12, 2019, s. 10

Rys. 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2021 przez Cert Polska (CSIRT NASK)



Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB, 2022, s. 20, 2021, s. 24, 2020, s. 12, 2019, s. 10

CERT Polska prowadzi działalność związaną z monitorowaniem i zapewnieniem bezpieczeństwa polskiej cyberprzestrzeni od połowy lat 90-tych. Na przestrzeni tych lat liczba incydentów bezpieczeństwa stale wzrasta i wykazuje znacznie zwiększoną dynamikę wzrostu w ostatnich 5 latach. Ilość, skalę i dynamikę wzrostu ilości incydentów obsłużonych przez zespół CERT Polska w latach 1996 – 2021 zawierają tabela 7 i rysunek 3.

Tabela 7. Liczba incydentów obsłużonych ręcznie przez CERT Polska na przestrzeni lat 1996 - 2021

Rok	Liczba incydentów	Rok	Liczba incydentów	Rok	Liczba incydentów
		2013	1.219	2004	1.222
2021	29.483	2012	1.082	2003	1.196
2020	10.420	2011	605	2002	1.013
2019	6.484	2010	674	2001	741
2018	3.739	2009	1.292	2000	126
2017	3.182	2008	1.796	1999	105
2016	1.926	2007	2.108	1998	100
2015	1.456	2006	2.427	1997	75
2014	1.282	2005	2.516	1996	50

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 20, 2021, s. 24, 2020, s. 12, 2019, s. 10

Rys. 3. Liczba incydentów obsłużonych ręcznie przez CERT Polska na przestrzeni lat 1996 – 2021

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 20, 2021, s. 24, 2020, s. 12, 2019, s. 10

Ataki cybernetyczne i incydenty kierowane są w stronę konkretnych podmiotów instytucjonalnych i gospodarczych, reprezentujących zdefiniowane sektory. CERT Polska od roku 2018 prowadzi raportowanie w zakresie sektorów gospodarki, które były obiektami ataków. W roku 2019 została ustanowiona nowa kategoryzacja sektorów gospodarki, mająca na celu dokładne wskazanie kierunków i celów ataków cybernetycznych. Zdefiniowany wykaz sektorów, dla których prowadzone są analizy i raportowanie nie pokrywa się wprost z sektorami i systemami bezpieczeństwa ustanowionymi w ramach regulacji zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, niemniej pozwala na zidentyfikowanie intensywności działań cyberprzestępczych nakierowanych na obszary wskazane w regulacjach.

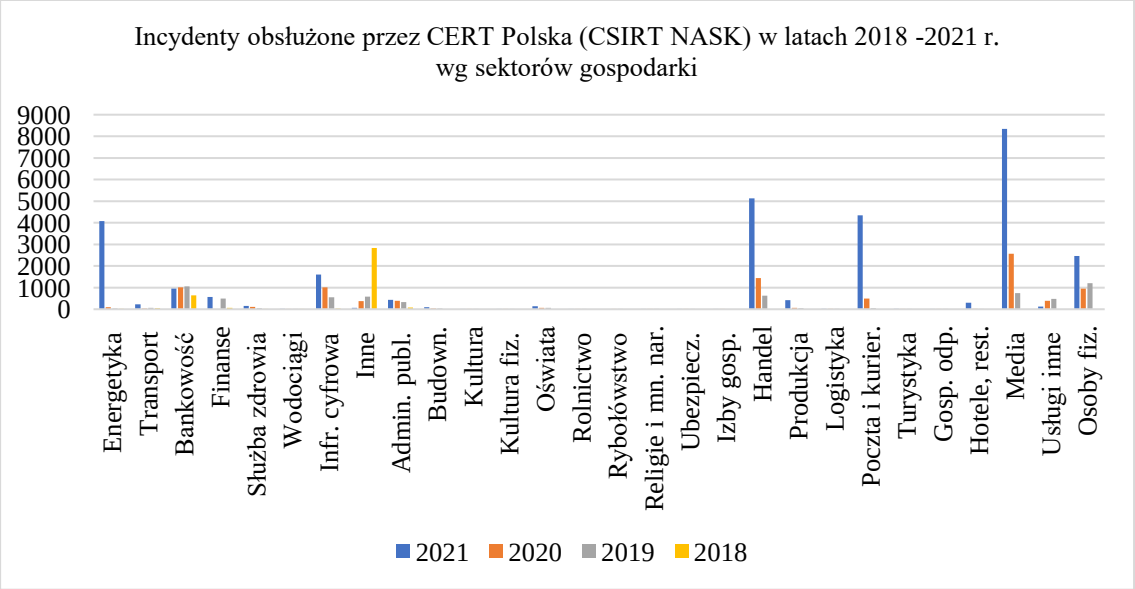
Szczegółowy wykaz incydentów zidentyfikowanych w sektorach gospodarki w latach 2018-2021 przez CERT Polska został przedstawiony w tabeli 8 i na rysunku 4.

Tabela 8. Incydenty obsłużone przez CERT Polska (CSIRT NASK) w latach 2018 - 2021 r. wg sektorów gospodarki

	2021		2020		2019		2018	
Sektor gospodarki	**Liczba incyd.**	**%**	**Liczba incyd.**	**%**	**Liczba incyd.**	**%**	**Liczba incyd.**	%
Energetyka	4.084	13,85	101	0,97	28	0,4	20	0,53
Transport	220	0,75	29	0,28	61	0,9	51	1,36
Bankowość	947	3,21	1.008	9,67	1.057	16,3	643	17,2
Finanse/ Infrastruktura rynków finansowych	563	1,91	1.283	12,31	500	7,7	62	1,66
Służba zdrowia	150	0,51	112	1,07	53	0,8	13	0,35
Wodociągi	18	0,06	9	0,09	5	0,08	2	0,05
Infrastruktura cyfrowa	1.606	5,45	1.016	9,75	550	8,5	29	0,78
Inne	68	0,28	379	3,64	578	9	2.834	75,8
Administracja publiczna	429	1,46	388	3,72	336	5,2	85	2,27
Budown. i gosp. nieruch.	89	0,30	29	0,28	31	0,5	-	-
Kultura i ochr. dziedz. narod.	11	0,04	7	0,07	9	0,1	-	-
Kultura fizyczna	2	0,01	9	0,09	4	0,06	-	-
Oświata i wychowanie	142	0,48	71	0,68	62	1	-	-
Rolnictwo	2	0,01	4	0,04	3	0.05	-	-
Rybołówstwo	0	0,0	1	0,01	2	0,03	-	-
Wyznania rel. i mniejsz. narod.	6	0,02	8	0,08	3	0,05	-	-
Działalność ubezpiecz.	3	0,01	2	0,2	5	0,08	-	-
Izby gosp. i handlowe	4	0,01	3	0,03	0	0,0	-	-
Handel hurt. i detal.	5.125	17,38	1.437	13,79	624	9,6	-	-
Produkcja	421	1,43	57	0,55	46	0,7	-	-
Logistyka i dystrybucja	18	0,06	27	0,26	19	0,3	-	-
Poczta i usługi kurier.	4.338	14,71	500	4,8	49	0,8	-	-
Turystyka	15	0,05	9	0,09	8	0,1	-	-
Gospodarka odpadami	6	0,02	1	0,01	2	0,03	-	-
Hotele, restauracje, catering	295	1,0	19	0,18	9	0,1	-	-
Media	8.339	28,28	2.568	24,64	748	11,5	-	-
Usługi inne	118	0,4	384	3,69	480	7,4	-	-
Osoby fizyczne	2.464	8,36	959	9,20	1.212	18,7	-	-
Razem	**29.483**	**100**	**10.420**	**100**	**6.484**	**100**	**3.739**	**100**

Źródło: opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2022, s. 22, 2021, s. 26, 2020, s. 14, 2019, s. 13

Rys. 4. Incydenty obsłużone przez CERT Polska (CSIRT NASK) w latach 2018 -2021 r. wg sektorów gospodarki



Źródło: opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2022, s. 22, 2021, s. 26, 2020, s. 14, 2019, s. 13

W roku 2021 najczęściej atakowane były sektory – media, handel hurtowy i detaliczny, poczta i usługi kurierskie oraz energetyka. CERT Polska zarejestrował łącznie 8339 incydentów, które wystąpiły w sektorze media, co stanowi 28,28% wszystkich zarejestrowanych incydentów. Sektor ten obejmuje między innymi media społecznościowe, prasę czy telewizję. Wśród wszystkich incydentów zaklasyfikowanych w sektorze media, znaczna część - 91,73%, to incydenty typu phishing. Kolejnym sektorem pod względem ilości zarejestrowanych incydentów był sektor handlu hurtowego i detalicznego, gdzie zarejestrowano 5125 incydentów, co daje 17,38% wszystkich incydentów. Sektor ten obejmuje między innymi serwisy aukcyjne oraz sklepy internetowe. Podobnie jak w sektorze media, w tym przypadku również incydenty typu phishing stanowiły najznaczniejszą grupę – 89,17%. Trzecim sektorem z najliczniejszą pulą incydentów był sektor poczta i usługi kurierskie, w którym zarejestrowano 4338 incydentów cyberbezpieczeństwa, co stanowi 14,71% wszystkich incydentów, gdzie 84,14% z nich również dotyczą phishingu. Ten sektor obejmuje między innymi firmy spedycyjne czy operatorów poczty elektronicznej. Kolejnym najczęściej atakowanym sektorem była energetyka, gdzie zanotowano 4084 incydenty, co stanowi 13,85% wszystkich zdarzeń. W roku 2020 incydenty najliczniej występowały w sektorach media, handel hurtowy i detaliczny oraz finanse. CERT Polska zarejestrował łącznie

2568 incydentów, które wystąpiły w sektorze media, co stanowiło 24,64% wszystkich incydentów. Kolejnym sektorem pod względem ilości zarejestrowanych incydentów był sektor handel hurtowy i detaliczny, w którym zarejestrowano łącznie 1437 incydentów, co stanowiło 13,79% zarejestrowanych incydentów. Następny sektor to finanse z liczbą 1283 incydentów i 12,31% udziałem w puli incydentów. Incydenty zaklasyfikowane do tego sektora wystąpiły między innymi w serwisach szybkich płatności internetowych[120].

CSIRT NASK w ramach realizacji zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa w roku 2021 obsłużył 36 incydentów, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie ma istotny skutek zakłócający świadczenie usługi kluczowej, gdzie 31 incydentów poważnych z sektora bankowego, 3 z sektora energii oraz 2 z sektora ochrony zdrowia. Zarejestrowano o 4 incydenty poważne więcej niż w roku 2020. W 2021 r. CSIRT NASK obsłużył 512 incydentów dotyczących podmiotów publicznych. To wzrost o 11% względem roku ubiegłego. Najczęstsze zarejestrowane incydenty zaklasyfikowane jako incydenty w podmiocie publicznym należały do sektorów administracja publiczna – 288 przypadków, oświata i wychowanie – 81 incydentów oraz infrastruktura cyfrowa – 43 incydenty[121]. CSIRT NASK w roku 2020 obsłużył 32 incydenty, które zaklasyfikowano jako poważne, spośród których 27 incydentów dotyczyło sektora bankowego, 4 sektora ochrony zdrowia oraz 1 sektora energii. Ponadto CSIRT NASK obsłużył 1 incydent istotny, czyli taki, którego wystąpienie ma wpływ na świadczenie usługi cyfrowej. W 2020 r. CSIRT NASK obsłużył 461 incydentów dotyczących podmiotów publicznych, co stanowi ok. 4,4% wszystkich zarejestrowanych incydentów. Zgłoszenia z tego sektora najczęściej były klasyfikowane jako szkodliwe oprogramowanie lub obraźliwe i nielegalne treści, w tym spam, jak też ataki phishingowe, mające na celu przejęcie danych uwierzytelniających do poczty elektronicznej. W 2020 r. CERT Polska zarejestrował o 23 incydenty poważne więcej względem roku 2019. Ponad połowa incydentów z sektora bankowego dotyczyła różnego rodzaju awarii, czego efektem była niedostępność usługi[122].

Ataki realizowane są poprzez zastosowanie odpowiednich, dedykowanych danemu typowi ataku technik. Wywoływane poprzez ataki incydenty można rozróżnić ze względu

[120] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 20, 2020, s. 24, 25
[121] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 21
[122] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2021, s. 25

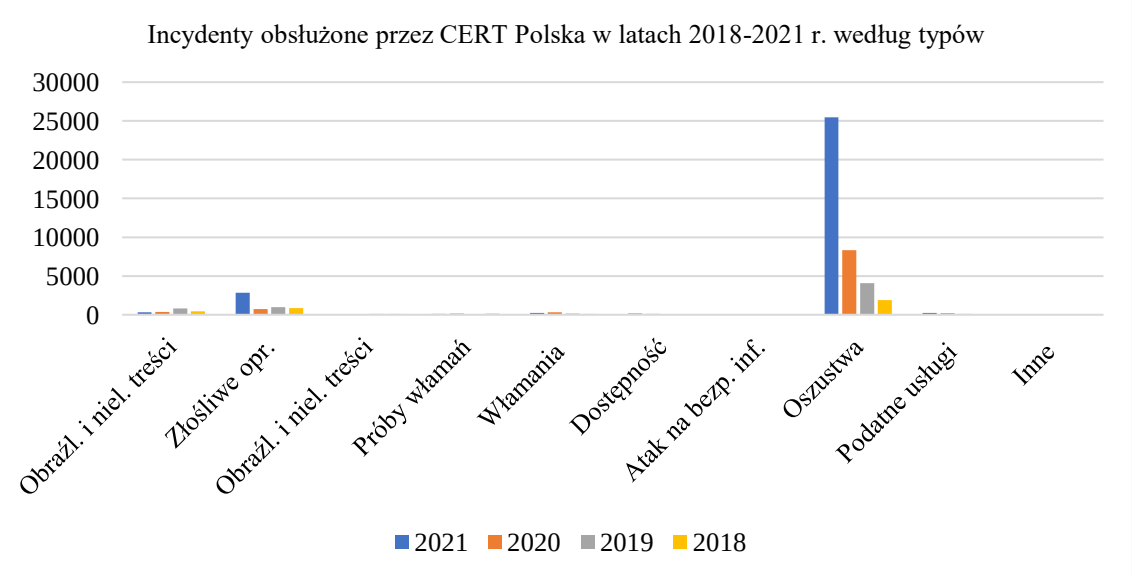
na ich typ. Dane dotyczące zestawienia typów incydentów występujących w polskiej cyberprzestrzeni obsłużonych przez CERT Polska w latach 2018-2021 r. zawierają tabela 9 i rysunek 5.

Tabela 9. Incydenty obsłużone przez CERT Polska w latach 2018-2021 r. według typów

Typ incydentu	2021		2020		2019		2018	
	Liczba incyd.	%	Liczba incyd.	%	Liczba incyd.	%	Liczba incyd.	%
Obraźliwe i nielegalne treści	311	1,05	371	3,56	812	12,5	431	11,53
Złośliwe oprogramowanie	2.847	9,66	746	7,16	969	14,9	862	23,05
Gromadzenie informacji	27	0,09	60	0,58	95	1,5	101	2,70
Próby włamań	127	0,43	174	1,67	77	1,2	153	4,09
Włamania	247	0,84	317	3,04	160	2,5	125	3,34
Dostępność zasobów	148	0,50	121	1,16	57	0,9	49	1,31
Atak na bezpiecz. informacji	55	0,19	68	0,65	41	0,6	46	1,23
Oszustwa komputerowe	25.472	86,40	8.310	79,75	4086	63,0	1878	50,23
Podatne usługi	216	0,73	211	2,02	102	1,6	69	1,85
Inne	33	0,11	42	0,4	85	1,3	25	0,67
Razem	**29.483**	**100**	**10.420**	**100**	**6.484**	**100**	**3.739**	**100**

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2022, s. 23, 24, 2021, s. 26, 27, 2020, s. 15, 2019, s. 11, 12

Rys. 5. Incydenty obsłużone przez CERT Polska w latach 2018-2021 r. według typów



Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2022, s. 23, 24, 2021, s. 26, 27, 2020, s. 15, 2019, s. 11, 12

Najczęstszym typem incydentów w roku 2021 były oszustwa komputerowe z liczbą 25 472 incydenty, co stanowiło aż 86,40% wszystkich zarejestrowanych incydentów. W ramach tego typu najpopularniejszy był phishing – stanowiący aż 76,57 proc. wszystkich obsłużonych incydentów. Zarejestrowano 22 575 incydentów tego typu, co stanowiło wzrost do roku poprzedniego o 196%. Drugim najliczniejszym typem incydentów było szkodliwe oprogramowanie. Zarejestrowano 2847 przypadków, co stanowiło 9,66% wszystkich obsłużonych incydentów. Liczba ta w porównaniu do roku ubiegłego wzrosła o 281%. Trzecim najliczniejszym typem incydentu były obraźliwe i nielegalne treści, w tym spam. Zrejestrowano 311 przypadków, stanowiących 1,05%. Tak niewielki udział tego typu incydentu wynika z faktu, iż do jednego incydentu często przypisuje się wiele zgłoszeń - za 311 incydentów odpowiadało aż 21 522 zgłoszeń[123].

W roku 2020 CERT Polska odnotował wzrost liczby obsłużonych incydentów na poziomie 60,7 proc. w porównaniu do roku 2019. Najczęstszym typem incydentu były oszustwa komputerowe, których zarejestrowano 8 310, co stanowiło 79,75% wszystkich incydentów. Wśród oszustw najpopularniejszym typem incydentu był phishing — odnotowano 7 622 incydentów - 73,15% wszystkich obsłużonych incydentów. Liczba incydentów zaklasyfikowanych jako phishing w porównaniu do roku 2019 wzrosła aż o 116%. Na drugim miejscu pod względem liczby zarejestrowanych incydentów znalazło się szkodliwe oprogramowanie — zarejestrowano 746 incydentów, co stanowiło 7,16%. Trzecie miejsce w rankingu liczby zarejestrowanych incydentów w roku 2020 przypada kategorii obraźliwych i nielegalnych treści, których odnotowano 371 przypadków, co stanowiło 3,56%. W tej kategorii najpopularniejszy był spam – 336 przypadków i 3,22% wszystkich incydentów[124].

W roku 2019 najczęściej występującym typem ataku był phishing, który stanowił ok. 54,2% wszystkich incydentów. Na drugim miejscu pod względem liczby zarejestrowanych incydentów znalazły się zgłoszenia dotyczące złośliwego oprogramowania – ok. 14,9%. Incydenty z kategorii “obraźliwe i nielegalne treści”, w tym spam, stanowiły ok. 12,1% wszystkich zarejestrowanych incydentów. Zdecydowanie najpopularniejszym typem incydentu obsługiwanym przez CERT Polska w 2019 r. był phishing, stanowiący ponad połowę wszystkich przypadków. W porównaniu do roku wcześniejszego udział incydentów phis-

[123] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2022, s. 20

[124] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2021, s. 24, 25

hingowych wzrósł o ok. 10 punktów procentowych. Stosunek zgłoszeń dotyczących złośliwego oprogramowania do ogółu zarejestrowanych incydentów zmalał o ok. 9 punktów procentowych w porównaniu do ubiegłego roku – z ok. 24% do ok. 15% – chociaż incydentów odnotowano więcej. W 2019 r. obserwowano wiele kampanii, które w sposób masowy atakowały polskich użytkowników. Biorąc pod uwagę liczbę incydentów obsłużonych w 2019 r. na trzecim miejscu znalazły się zgłoszenia nielegalnych i obraźliwych treści o charakterze spamu. W porównaniu do 2018 r. odnotowano w tej kategorii wzrost zarejestrowanych incydentów na poziomie ok. 88%[125].

W roku 2018 najbardziej popularne wśród przestępców były fałszywe sklepy internetowe, gdzie w odniesieniu do 2017 r. odnotowano prawie 3-krotny wzrost tego typu działalności. Następnym rodzajem szkodliwej działalności jest spam, który w 2018 r. w porównaniu z 2017 rokiem podwoiły swoją liczbę. Miało miejsce wiele incydentów z próbami włamań do systemów, urządzeń i aplikacji. Część z tych ataków została przeprowadzona na słabo zabezpieczone urządzenia Internetu Rzeczy (ang. IoT, Internet of Things), które często posiadają niezmienianą, standardową konfigurację producenta z domyślnym hasłem dostępowym. Przedstawione przez CERT Polska zestawienie incydentów bezpieczeństwa wg typów pokazuje, że w 2018 r. najliczniej występowały: oszustwa komputerowe – 50,23%, złośliwe oprogramowanie – 23%, obraźliwe i nielegalne treści – 11,53%. Łącznie te 3 typy stanowiły 85% wszystkich incydentów[126].

2.4.2. Zapewnienie cyberbezpieczeństwa przez CSIRT GOV

Zespół CSIRT GOV (ABW) publikuje coroczny raport – „*Raport o stanie bezpieczeństwa cyberprzestrzeni RP*”. Zgodnie z danymi przedstawionymi w raportach z ostatnich lat w roku 2021 Zespół CSIRT GOV odnotował 762 175 zgłoszeń o potencjalnym wystąpieniu incydentów cyberbezpieczeństwa, z czego jako incydenty zakwalifikowano 26 899 przypadków, w roku 2020 odnotował 246107 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych, z czego jako incydenty zakwalifikowano 23 309 przypadków, wobec 226 914 zgłoszeń i 12 405 incydentów w roku 2019, 31 865 zgłoszeń i 6236 incydentów

[125] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2020, s. 13
[126] *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, NASK-PIB 2019, s. 10, 11

w roku 2018 i 28 281 zgłoszeń i 5819 incydentów w roku 2017[127]. Z analizy przedstawionych danych wynika, że liczba zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych i liczba zidentyfikowanych incydentów są dynamicznie rosnące. Dane na temat incydentów bezpieczeństwa obsłużonych przez specjalistów CSIRT GOV w ostatnich latach przedstawione zostały w tabeli 10 i na rysunku 6.

Tabela 10. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2021 przez CSIRT GOV

Zgłoszenia / Rok	2021	2020	2019	2018	2017	2016	2015
Liczba zgłoszeń	762.175	246.107	226.914	31.865	28.281	19.954	16.123
Liczba incydentów	26.899	23.309	12.405	6.236	5.819	9.288	8.914

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 9, 2021, s. 9, 2020, s. 8, 9, 2019, s. 11

Rys. 6. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2021 przez CSIRT GOV

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 9, 2021, s. 9, 2020, s. 8, 9, 2019, s. 11

Incydenty zidentyfikowane przez CSIRT GOV są różnego typu i charakteru, i są klasyfikowane zgodnie z przyjętą klasyfikacją. W roku 2019 została zmieniona klasyfikacja incydentów, co jest odzwierciedlone w zbiorczych danych o incydentach za ostanie lata.

[127] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 9, 2021, s. 9, 2020, s. 8, 9, 2019, s. 11

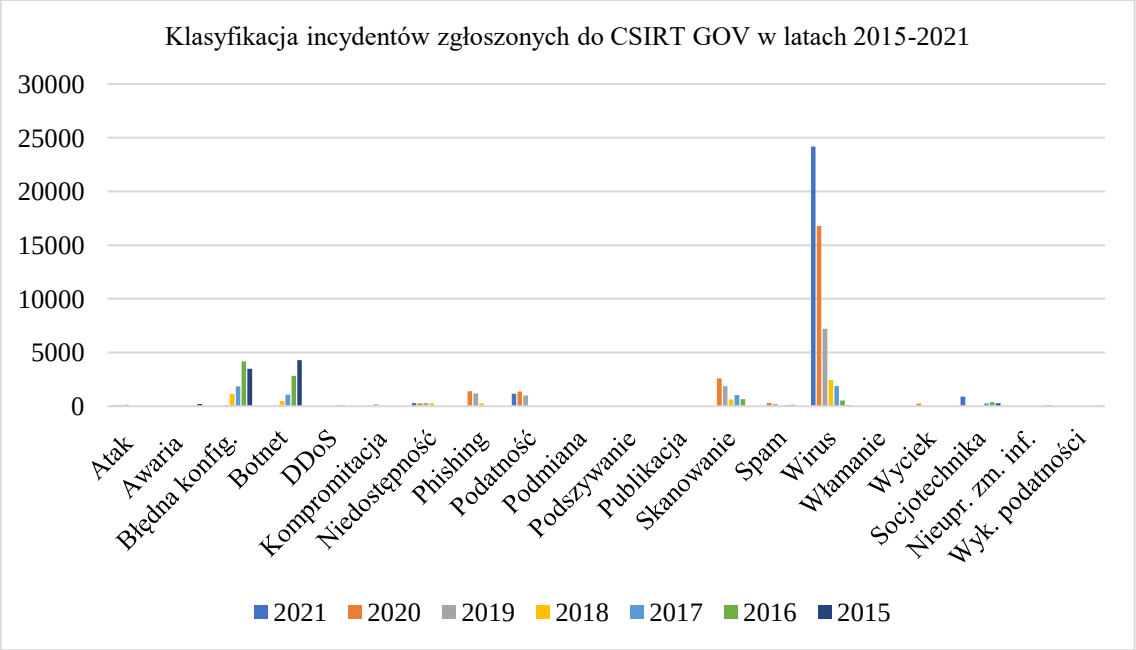
Dane dotyczące klasyfikacji incydentów komputerowych zidentyfikowanych w latach 2015-2020 przedstawiono w tabeli 11 i na rysunku 7.

Tabela 11. Klasyfikacja incydentów zgłoszonych do CSIRT GOV w latach 2015-2021

Incydent	2021	2020	2019	2018	2017	2016	2015
Atak	74	96	141				
Awaria			1				219
Błędna konfiguracja		69	119	1.138	1.847	4.158	3.491
Botnet	16	36	37	488	1.082	2.836	4.284
DDoS			9		98	76	
Kompromitacja		66	188				
Niedostępność	310	254	290	275			
Phishing		1.396	1.178	276			
Podatność	1.148	1.366	1.016				
Podmiana		13	8				
Podszywanie		72	50				
Publikacja		11	3				
Skanowanie		2.604	1.878	636	1.030	661	
Spam		311	210		119	137	
Wirus	24.171	16.777	7.219	2.448	1.868	540	84
Włamanie		8	44				
Wyciek		230	14				
Inżynieria społeczna Socjotechnika	904				254	382	257
Nieuprawniona zmiana informacji							74
Wykorzystanie podatności							72

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 14, 2021, s. 12; 2020, s. 11; 2019, s. 13

Rys. 7. Klasyfikacja incydentów zgłoszonych do CSIRT GOV w latach 2015-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 14, 2021, s. 12; 2020, s. 11; 2019, s. 13

W roku 2021 najwięcej incydentów sklasyfikowano jako wirus, podatność oraz socjotechnika. W ramach kategorii wirus zidentyfikowano 24 171 incydentów. Wiąże się to z alarmami pochodzącymi z systemu wczesnego ostrzegania o zagrożeniach pochodzących z sieci Internet ARAKIS GOV. Przedmiotowe alarmy mogą świadczyć o infekcji stacji roboczych, jak również serwerów w instytucjach administracji państwowej lub u operatorów infrastruktury krytycznej. Wzrastająca liczba incydentów zawartych w tej kategorii spowodowana jest aktualizowaną bazą IoC (ang. Indicators of Compromise) o najnowsze wskaźniki kompromitacji. Baza ta wzbogacana jest o IoC pochodzące zarówno z własnych ustaleń, jak również źródeł zewnętrznych o znanej reputacji. Na ilość incydentów typu wirus wpływ ma także rozwój systemu ARAKIS GOV obejmujący nowe instancje w instytucjach. Druga najliczniejsza kategoria to podatność, w ramach której zidentyfikowano 1 148 incydentów w zasobach IT rozumianych jako słabość systemu teleinformatycznego, błędy konfiguracyjne oraz brak odpowiedniej polityki bezpieczeństwa, związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych rozwiązań teleinformatycznych. Trzecią najliczniejszą kategorią jest socjotechnika obejmująca 904 incydenty. Zagrożenia te dotyczą kampanii phishingowych, podszywania się oraz ataków z zakresu inżynierii społecznej przeciwko użytkownikom systemów teleinformatycznych, które mają na celu wyłudzenie poufnych infor-

macji, zainfekowanie komputera złośliwym oprogramowaniem, bądź nakłonienie użytkownika do określonych działań. W tej kategorii najwięcej incydentów dotyczyło podszywania się pod witryny internetowe wykorzystujące wizerunek podmiotu, często mających na celu wyłudzenie środków finansowych bądź danych logowania. Następną kategorią jest niedostępność (310 zarejestrowanych incydentów). Tę kategorię obejmują zdarzenia dotyczące niedostępności witryn internetowych, awarii technicznych oraz prac technicznych. W kategorii publikacja zarejestrowano 158 incydentów obejmujących zgłoszenia dotyczące wycieków, publikacji w sieci wykradzionych informacji, dezinformacji, zniesławienia czy naruszenia praw autorskich. Kolejna kategoria skanowanie objęła 118 incydentów dotyczących rekonesansu infrastruktury teleinformatycznej administracji rządowej oraz infrastruktury krytycznej. W kategorii atak zgłoszone zostały 74 incydenty związane z wszelkiego rodzaju przeprowadzanymi atakami na systemy teleinformatyczne np. DDoS, DoS, przełamanie zabezpieczeń. W ramach ostatniej kategorii botnet zarejestrowano w sumie 16 incydentów, czyli zagrożeń dotyczących identyfikacji komputerów należących do sieci przejętych komputerów[128].

W roku 2020, podobnie jak i w 2019, najwięcej incydentów zostało sklasyfikowanych wśród trzech następujących kategorii: wirus, skanowanie, phishing. Kategoria wirus jako najliczniejsza, stanowiła prawie 72% ogółu wszystkich incydentów. Ilość incydentów w tej kategorii związana jest przede wszystkim ze zwiększeniem się skuteczności identyfikacji oprogramowania złośliwego w oparciu o systemy detekcji, sygnatury oraz przepływy sieciowe. W tym zakresie należy wskazać na powiadomienia systemu ARAKIS 3.0 GOV. Dotyczą one alarmów, które mogą świadczyć o infekcji stacji roboczej w instytucji administracji państwowej lub u operatora infrastruktury krytycznej. Liczba incydentów typu wirus rośnie gwałtownie na przestrzeni ostatnich lat. W stosunku do roku 2019 można zaobserwować wzrost o ponad 132%. W kategorii wirus w 2019 r. zarejestrowano 7 219 incydentów, podczas gdy w 2020 r. odnotowano 16 777 incydentów. Drugą pod względem liczności grupą są incydenty zaklasyfikowane jako skanowanie. Wynikają one także z alarmów ARAKIS 3.0 GOV i dotyczą złośliwego lub podejrzanego ruchu skierowanego na adresację podmiotów podległych CSIRT GOV. W przypadku kategorii skanowanie utrzymuje się wyraźna tendencja wzrostowa, przy czym w 2020 roku tego typu incydentów było prawie 39% więcej niż w roku 2019. W kategorii skanowanie w 2019 r. zarejestrowano 1 878 incyden-

[128] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 14, 15

tów, podczas gdy w 2020 r. odnotowano 2 604 incydentów. Jednym z istotniejszych rodzajów zagrożeń są także kampanie phishingowe. Pomimo tego, że opierają się one na stosowaniu metod socjotechniki, stanowią realne zagrożenie dla bezpieczeństwa systemów teleinformatycznych i mogą również stanowić fazę inicjującą bardziej rozległy atak, pozwalający na uzyskanie dostępu do infrastruktury teleinformatycznej danego podmiotu. Wzrost zarejestrowanych incydentów dotyczących kategorii phishing wynosi prawie 19% w porównaniu z rokiem 2019. W kategorii phishing w 2019 r. zarejestrowano 1 178 incydentów, podczas gdy w 2020 r. odnotowano 1 396 incydentów. Kolejnym zagrożeniem, które godzi w bezpieczeństwo teleinformatyczne, są podatności w zasobach IT rozumiane jako słabość systemu teleinformatycznego, wynikające z błędów konfiguracyjnych lub braku odpowiedniej polityki bezpieczeństwa, związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych rozwiązań teleinformatycznych. Również w tym wypadku można zaobserwować wzrost liczby incydentów w kategorii podatność o ponad 34% w stosunku do roku 2019. W kategorii podatność w 2019 r. zarejestrowano 1 016 incydentów, podczas gdy w 2020 r. odnotowano 1366 incydentów[129].

W roku 2021 zespół CSIRT GOV przyjął bardziej zagregowaną klasyfikację incydentów niż w latach ubiegłych (2020, 2019), stąd trudność w bezpośrednim porównaniu danych i identyfikacji trendów.

CSIRT GOV od roku 2019 publikuje informacje o instytucjach, przeciwko którym zostały skierowane incydenty. Liczba zarejestrowanych incydentów w instytucjach przedstawiona jest w tabeli 12 i na rysunku 8 poniżej.

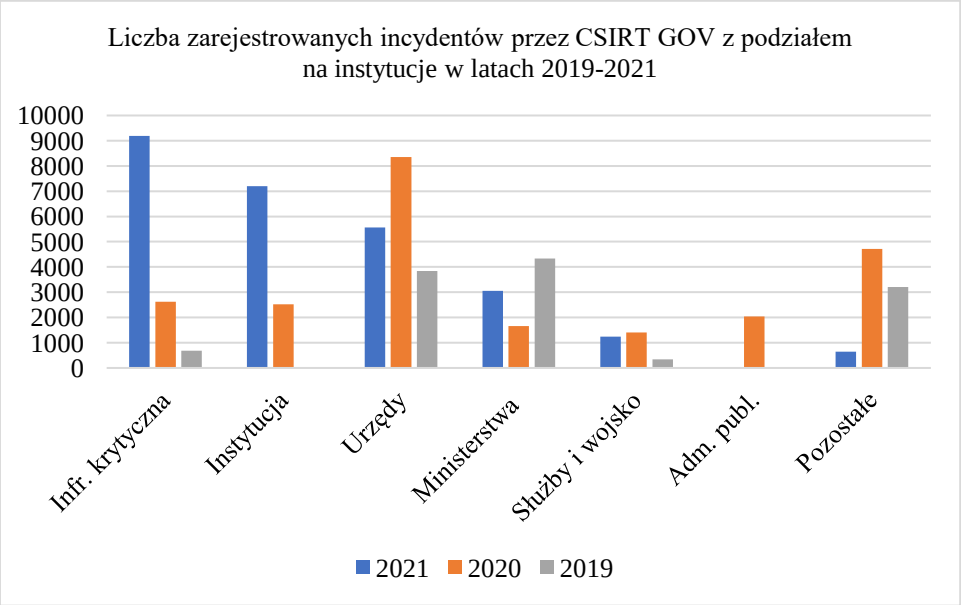
Tabela 12. Liczba zarejestrowanych incydentów przez CSIRT GOV z podziałem na instytucje w latach 2019-2021

Instytucje	2021	2020	2019
Infrastruktura krytyczna	9.196	2.626	685
Instytucja	7.203	2.518	-
Urzędy	5.563	8.356	3.837
Ministerstwa	3.056	1.656	4.336
Służby i wojsko	1.237	1.400	341
Administracja publiczna	-	2.039	-
Pozostałe	644	4.714	3.206
Razem	**26.899**	**23.309**	**12.405**

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 16, 2021, s. 14, 2020, s. 10

[129] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2021, s. 12, 13, 14

Rys. 8. Liczba zarejestrowanych incydentów przez CSIRT GOV z podziałem na instytucje w latach 2019-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 16, 2021, s. 14, 2020, s. 10

Stosowana przez CSIRT GOV klasyfikacja instytucji nie pokrywa się wprost z sektorami i systemami bezpieczeństwa ustanowionymi w ramach regulacji zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, jest znacznie węższa niż przedstawiona w raportowaniu CERT Polska i jednocześnie znacznie węższa niż wykazy sektorów i systemów powołane w regulacjach. Takie ujęcie informacji nie pozwala na zidentyfikowanie intensywności działań cyberprzestępczych nakierowanych na obszary wskazane w regulacjach, niemniej jednak choć w przybliżony, ogólny sposób umożliwia poznanie kierunków działań.

Obserwowana wysoka liczba zgłoszeń jest wynikiem przede wszystkim wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa, tym samym w latach 2019 - 2020 nastąpił zauważalny wzrost liczby zgłoszeń przesyłanych do CSIRT GOV w stosunku do wcześniejszych okresów sprawozdawczych. Jednocześnie czynnikiem oddziaływującym na wskazaną tendencję był wzrost liczby zgłoszeń rejestrowanych przez systemy wykrywania oraz ostrzegania przed zagrożeniami dotyczącymi systemów teleinformatycznych instytucji, podmiotów czy organów państwa znajdujących się w kompetencji Zespołu CSIRT GOV, co było podyktowane skalą cyberzagrożeń obecnych w cyberprzestrzeni RP[130].

[130] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2021, s. 9

W 2021 roku zarejestrowano ponad trzykrotnie więcej zgłoszeń w stosunku do roku poprzedniego, gdzie w sumie zarejestrowano 246 107 zgłoszeń. Wzrost zarejestrowanych zgłoszeń wynika przede wszystkim z liczby alarmów generowanych przez system ARAKIS GOV. System ARAKIS GOV umożliwia identyfikowanie zagrożeń m.in. na podstawie dedykowanych sygnatur bezpieczeństwa. Stałe zasilanie systemu ARAKIS w nowe sygnatury, jak również zwiększająca się liczba zainstalowanych sond w kolejnych przyłączanych systemach teleinformatycznych, skutkują większą detekcją, a co za tym idzie - większą liczbą generowanych zgłoszeń. Spośród ponad 760 tys. zgłoszeń w 2021 roku zarejestrowano 26 899 incydentów. Stanowi to wzrost o około 15% w porównaniu do poprzedniego roku, gdzie zidentyfikowano 23 309 incydentów. Zebrane statystyki wskazują na utrzymującą się tendencję wzrostową zarówno wpływających zgłoszeń, jak również zarejestrowanych incydentów. Wśród stałych czynników mających wpływ na obserwowany poziom cyberzagrożeń jest z jednej strony szerokie wykorzystanie cyberprzestrzeni do utrzymywania ciągłości działania różnego rodzaju usług elektronicznych, zapewnienia ciągłości działania procesów biznesowych, wykorzystania cyberprzestrzeni do komunikacji i działalności statutowej instytucji i podmiotów, z drugiej strony natomiast czynnikiem kształtującym wskazaną tendencję jest postępujący rozwój taktyk i technik wykorzystywanych przez cyberprzestępców starających się wykorzystywać nowe oraz znane już podatności, a także stosujących zaawansowane wektory ataku. Wśród okoliczności, które w 2021 roku nie pozostawały bez wpływu na liczbę incydentów, był także utrzymujący się stan pandemii wirusa SARS-CoV-2, a powiązane z nią motywy wykorzystywane były do przeprowadzania ataków phishingowych. W 2021 roku odnotowano różnego rodzaju incydenty socjotechniczne z wykorzystaniem tematyki szczepień, certyfikatów szczepień, a także testów epidemicznych. Zostały także zidentyfikowane incydenty takie jak ransomware, vishing czy spoofing telefoniczny[131].

W roku 2020 Zespół CSIRT GOV odnotował 246 107 zgłoszeń, które zostały zakwalifikowane jako zdarzenia dotyczące potencjalnego wystąpienia incydentu teleinformatycznego w ramach obszaru kompetencyjnego Zespołu. Obserwowana wysoka ilość zgłoszeń jest wynikiem przede wszystkim wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa, tym samym w latach 2019 - 2020 nastąpił zauważalny wzrost ilości zgłoszeń przesyłanych do CSIRT GOV w stosunku do wcześniejszych okresów sprawozdawczych. Jednocześnie, czynnikiem oddziaływującym na wskazaną tendencję, był

[131] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 9, 10

wzrost ilości zgłoszeń rejestrowanych przez systemy wykrywania oraz ostrzegania przed zagrożeniami dotyczącymi systemów teleinformatycznych instytucji, podmiotów czy organów państwa znajdujących się w kompetencji Zespołu CSIRT GOV, co było podyktowane skalą cyberzagrożeń obecnych w cyberprzestrzeni RP. Liczba zdarzeń, które zostały zarejestrowane w roku 2020 jako faktyczny incydent, wyniosła w sumie 23 309, co stanowi wzrost o około 88% w stosunku do roku 2019, kiedy zidentyfikowano 12405 incydentów przy wzroście liczby zgłoszeń tylko na poziomie około 8%. Liczba incydentów w roku 2019 wzrosła w stosunku do roku 2018 o 99%. W okresie lat 2018-2020 został utrzymany trend wskazujący na podwajanie liczby incydentów w relacji rok do roku[132].

Różnica pomiędzy liczbą zarejestrowanych zgłoszeń a faktyczną liczbą incydentów wynika z faktu, iż część ze zgłoszeń stanowią tzw. false-positive, czyli błędnie wskazujące na wystąpienie zagrożenia. Są to najczęściej przypadki niewłaściwej interpretacji przez zgłaszającego prawidłowego ruchu sieciowego. Kolejną przyczyną powodującą różnice dotyczące przedmiotowych danych są wielokrotne zgłoszenia dotyczące tych samych incydentów. Zależność ta wynika przede wszystkim z alarmów systemu Arakis 3.0 GOV, których liczba we wskazanych okresach wzrosła ze względu na wykryte aktywne skanowanie adresacji sieciowych należących do instytucji administracji państwowej i operatorów infrastruktury krytycznej. Dodatkowym czynnikiem kształtującym wskazaną statystykę był zwiększony poziom detekcji zagrożeń związany z rozwojem możliwości zautomatyzowanych systemów wczesnego ostrzegania - Arakis GOV i N6 - działających w infrastrukturze podmiotów krajowego systemu cyberbezpieczeństwa. Ponadto zgłoszenia pochodzące z systemów automatycznych zostają poddane późniejszej weryfikacji przez Zespół CSIRT GOV, który wskazuje, czy zgłoszenia można zaklasyfikować jako faktyczne incydenty[133].

System Arakis 3.0 GOV to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł. W roku 2021 w sieciach teleinformatycznych podmiotów uczestniczących w projekcie Arakis 3.0 GOV zanotowano łącznie 1 758 708 908 przepływów, co przełożyło się na 3 366 360 wygenerowanych przez system alarmów, w 2020 roku zanotowano łącznie 1 813 243 995 przepływów, co przełożyło się na 1 758 813 wygenerowanych przez system alarmów, a w roku 2019 zanotowano 1 052 675 641 przepływów,

[132] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2021, s. 9, 10
[133] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2021, s. 10, 11, 2020, s. 9

z czego za alarmy uznano 844 951[134]. W ujęciu rok do roku, w okresie 2021-2020 ilość przepływów spadła o 4%, a ilość incydentów wzrosła o 91%, w okresie 2020-2019 r. wzrost liczby przepływów wyniósł 72%, a wzrost liczby zidentyfikowanych alarmów wyniósł 108%, w okresie 2019-2018 r. wzrost liczby przepływów wyniósł 330%, natomiast wzrost liczby zidentyfikowanych alarmów wyniósł 86%. Szczegółowe informacje na temat liczby i procentowego rozkładu przepływów i alarmów systemu Arakis GOV zostały przedstawione w tabeli 13 i na rysunku 9.

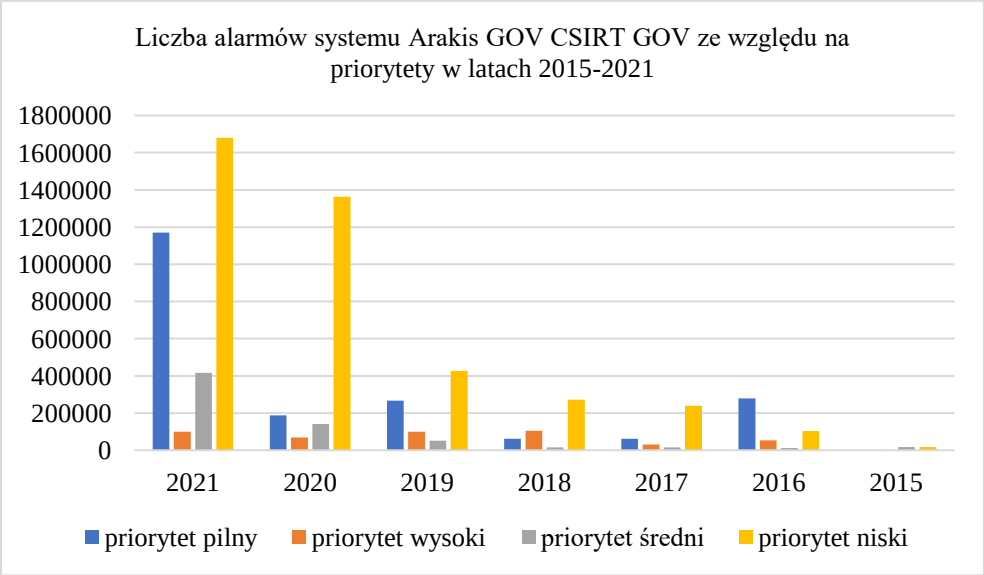
Tabela 13. Liczba i procentowy rozkład przepływów i alarmów systemu Arakis GOV CSIRT GOV ze względu na priorytety w latach 2015-2021

	2021	**2020**	**2019**	**2018**	**2017**	**2016**	**2015**
Przepływy	1.758.708.908	1.813.243.995	1.052.675.641	319.943.424	323.722.095	338.430.181	55.510
Alarmy	3.366.360	1.758.813	844.951	454.207	347.178	446.915	36.815
priorytet pilny	1.170.136 35%	187.149 11%	266.135 31%	62.365 14%	62.292 18%	279.181 62%	Nd.
priorytet wysoki	99.207 3%	67.939 4%	99.612 12%	104.502 23%	30.505 9%	52.766 12%	1.429 4%
priorytet średni	416.987 12%	140.303 8%	51.721 6%	15.412 3%	15.911 4%	12.365 3%	17.548 48%
priorytet niski	1.680.030 50%	1.363.422 77%	427.483 51%	271.928 60%	238.470 69%	102.603 23%	17.838 48%

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017, 2016

[134] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 38, 2021, s. 38

Rys. 9. Liczba alarmów systemu Arakis GOV CSIRT GOV ze względu na priorytety w latach 2015-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017, 2016

Alarmy o priorytecie pilnym wymagają niezwłocznej reakcji na zagrożenie ze strony administratorów z uwagi na duże ryzyko przełamania zabezpieczeń, alarmy o priorytecie wysokim wymagają wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie z uwagi na średnie ryzyko przełamania zabezpieczeń, alarmy o priorytecie średnim, informujące o dobrze znanym zagrożeniu, niosą małe ryzyko przełamania zabezpieczeń i wymagają uwagi, alarmy o priorytecie niskim, informujące o aktualnej sytuacji na styku sieci wewnętrznej z siecią internet, wymagają obserwacji[135].

Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów przedstawionych w tabeli 14 i na rysunku 10 poniżej.

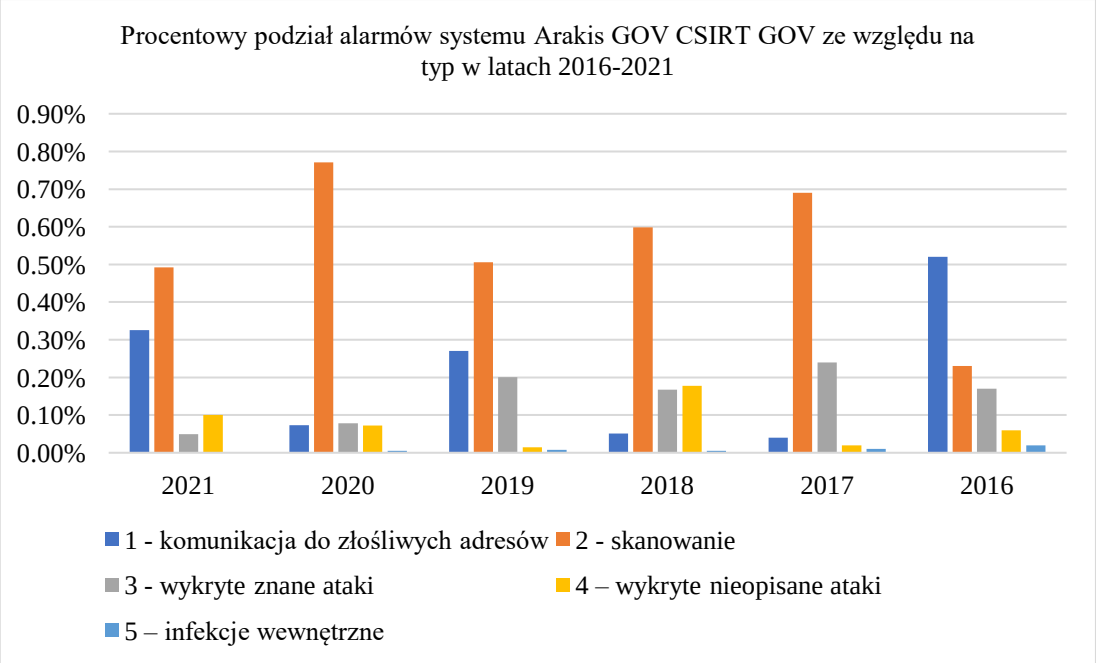
[135] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 38

Tabela 14. Procentowy podział alarmów systemu Arakis GOV CSIRT GOV ze względu na typ w latach 2016-2021

Typ	2021	2020	2019	2018	2017	2016
1 - komunikacja do złośliwych adresów	32,54%	7,34%	27,04%	5,12%	4%	52%
2 – skanowanie	49,26%	77,14%	50,59%	59,88%	69%	23%
3 - wykryte znane ataki	4,94%	7,80%	20,10%	16,74%	24%	17%
4 – wykryte nieopisane ataki	10,04%	7,22%	1,48%	17,75%	2%	6%
5 – infekcje wewnętrzne	0,21%	0,50%	0,79%	0,52%	1%	2%

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Rys. 10. Procentowy podział alarmów systemu Arakis GOV CSIRT GOV ze względu na typ w latach 2016-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Alarmy Systemu ARAKIS GOV typu 1 (komunikacja do złośliwych adresów) wynikają z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe lub mogącymi stanowić zagrożenie. Alarmy typu 2 (skanowania) pozwalają określić kierunki zainteresowań osób przeprowadzających skanowania. Alarmy typu 3 i 4 (wykryte znane ataki, wykryte nieopisane ataki) to alarmy wynikające z wygenerowania znanych lub nieznanych sygnatur szkodliwego oprogramowania lub działania w oparciu o obserwowane komunikacje lub dopasowania do bazy sygnatur. Alarmy typu 5 (infekcje wewnętrzne) są to

infekcje wewnętrzne identyfikowane na podstawie niepożądanej komunikacji z elementami sieci objętymi systemem ARAKIS GOV[136].

Spośród zidentyfikowanych alarmów w roku 2021 największą intensywność miało działanie typu skanowanie portów sieciowych (typ 2) – 49%, podobnie jak latach ubiegłych – 77% w roku 2020, 50% w roku 2019 i 60% w roku 2018. Tego typu aktywność w największym stopniu jest kierowana w stronę takich instytucji jak: urzędy – 26,41% w roku 2021, 31,29% w roku 2020 i 32,81% w roku 2019 – oraz operatorzy infrastruktury krytycznej – 31,81% w roku 2021, 29,04% w roku 2020 i 31,21% w roku 2019. Szczegółowy procentowy rozkład przepływów alarmów typu 2 z podziałem na instytucje przedstawiony jest w tabeli 15 i na rysunku 11.

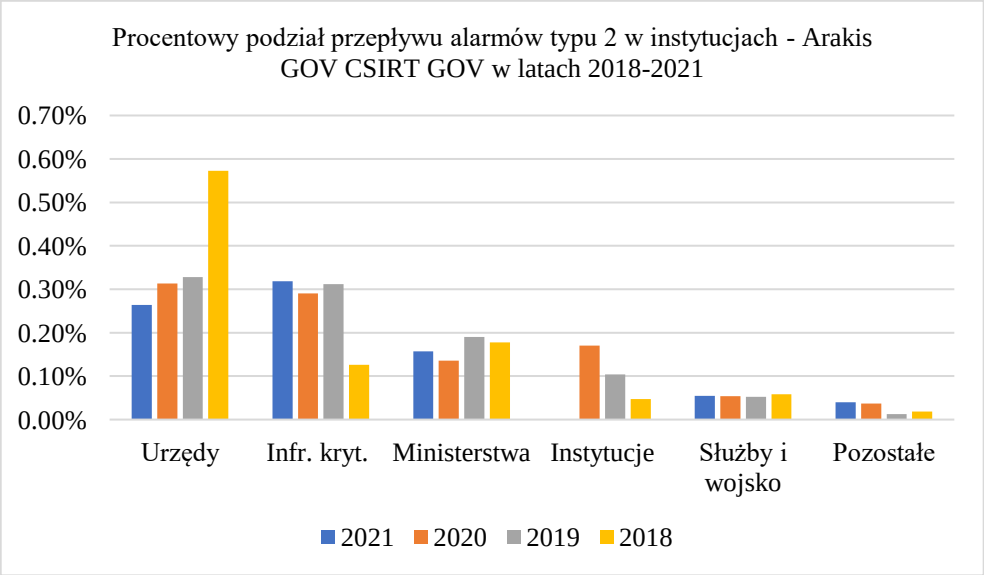
Tabela 15. Procentowy podział przepływu alarmów w instytucjach - Arakis GOV CSIRT GOV w latach 2016-2021

Podmioty	**2021**	**2020**	**2019**	**2018**	**2017**		**2016**	
Typ alarmu	2	2	2	2	1	5	1	5
Urzędy	26,41%	31,29%	32,81%	57,24%	5,74%	42,91%	616.119	5.832.490
Infrastruktura krytyczna	31,81%	29,04%	31,21%	12,59%	92,64%	39,75%	752.710 49%	160832
Ministerstwa	15,72%	13,56%	19,01%	17,74%	0,60%	6,50%	160.890	4.591
Instytucje	16.60%	17,06%	10,42%	4,76%	0,61%	0,98%	-	-
Służby i wojsko	5,44%	5,37%	5,27%	5,83%	0,26%	6,38%	1.124	156.221
Pozostałe	4,02%	3,68%	1,28%	1,84%	0,14%	3,48%	-	-

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

[136] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 39, 40

Rys. 11. Procentowy podział przepływu alarmów typu 2 w instytucjach - Arakis GOV CSIRT GOV w latach 2018-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w roku 2021 należały – Rosja (25%) oraz USA (15%). W roku 2020 do najbardziej aktywnych należały – Rosja (22%), USA (16%) i Polska (12%). W roku 2019 do najaktywniejszych należały - Rosja (28%), Stany Zjednoczone (13%), Niderlandy (12%) oraz Polska (10%). W roku 2018 do najbardziej aktywnych krajów pod względem liczby generowanych przepływów zaliczamy Chiny (22%), Stany Zjednoczone (19%), Rosja (13%) i Polska (12%). Z kolei w roku 2017 najbardziej aktywnymi krajami w generowaniu przepływów były Chiny (35%), Stany Zjednoczone (17%), Polska (15%) i Rosja (7%). Liczba przepływów z poszczególnych krajów, należących do grupy TOP 10, stanowiła w roku 2021 – 76%, w roku 2020 - 73%, a w roku 2019 - 67% wszystkich wygenerowanych przepływów zanotowanych przez system Arakis GOV[137].Wskazanie państw, z których generowane były przepływy w systemach teleinformatycznych polskiej cyberprzestrzeni wraz z rozkładem procentowym w ciągu ostatnich lat zostało przedstawione w tabeli 16 i na rysunku 12.

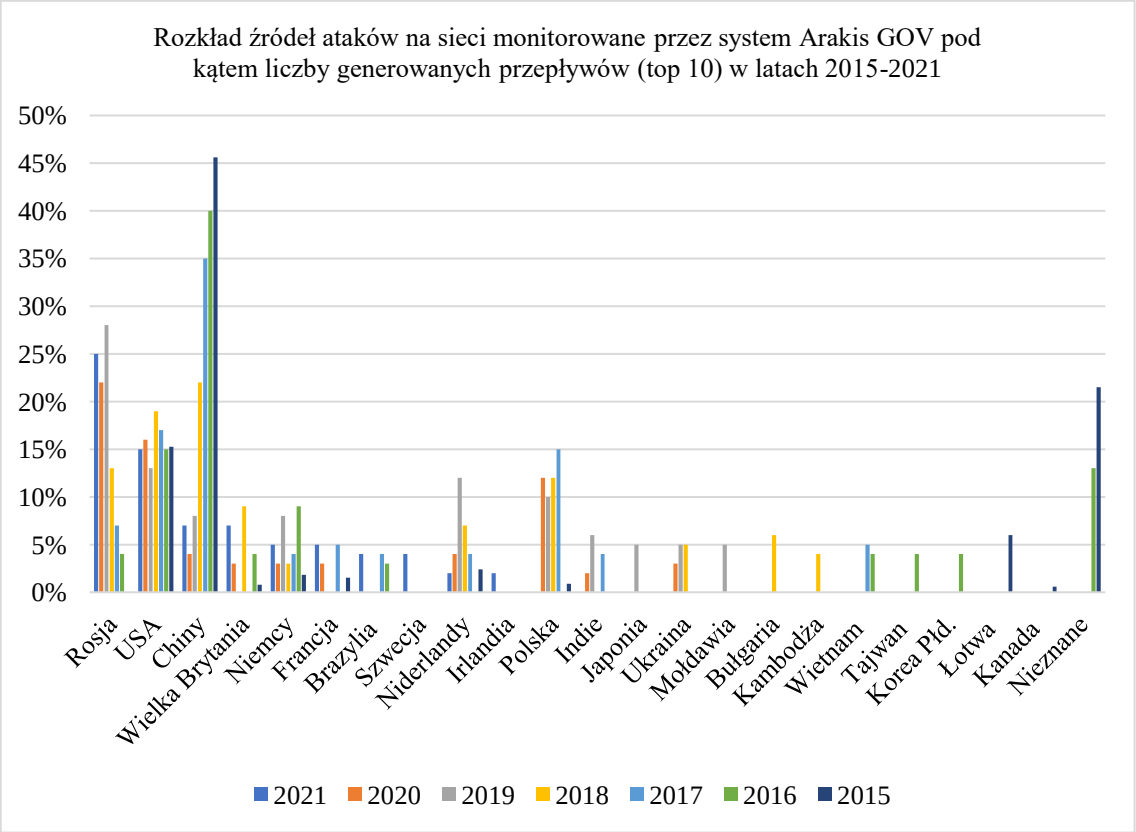
[137] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Tabela 16. Rozkład źródeł ataków na sieci monitorowane przez system Arakis GOV pod kątem liczby generowanych przepływów (top 10) w latach 2015-2021

Kraj	2021	2020	2019	2018	2017	2016	2015
Rosja	25%	22%	28%	13%	7%	4%	-
USA	15%	16%	13%	19%	17%	15%	15,27%
Chiny	7%	4%	8%	22%	35%	40%	45,61%
Wielka Brytania	7%	3%	-	9%	-	4%	0,79%
Niemcy	5%	3%	8%	3%	4%	9%	1,84%
Francja	5%	3%	-	-	5%	-	1,53%
Brazylia	4%	-	-	-	4%	3%	-
Szwecja	4%	-	-	-	-	-	-
Niderlandy	2%	4%	12%	7%	4%	-	2,4%
Irlandia	2%	-	-	-	-	-	-
Polska	-	12%	10%	12%	15%	%	0,9%
Indie	-	2%	6%	-	4%	-	-
Japonia	-	-	5%	-	-	-	-
Ukraina	-	3%	5%	5%	-	-	-
Mołdawia	-	-	5%	-	-	-	-
Bułgaria	-	-	-	6%	-	-	-
Kambodża	-	-	-	4%	-	-	-
Wietnam	-	-	-	-	5%	4%	-
Tajwan	-	-	-	-	-	4%	-
Korea Płd.	-	-	-	-	-	4%	-
Łotwa	-	-	-	-	-	-	5,99%
Kanada	-	-	-	-	-	-	0,59%
Nieznane	-	-	-	-	-	13%	21,50%

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Rys. 12. Rozkład źródeł ataków na sieci monitorowane przez system Arakis GOV pod kątem liczby generowanych przepływów (top 10) w latach 2015-2021



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, 2021, 2020, 2019, 2018, 2017

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w infrastrukturze polskich systemów teleinformatycznych należą niezmiennie Rosja, USA, Chiny i Niemcy, z których ruch jest generowany przez wszystkie lata prowadzenia monitorowania sieci. Wielka Brytania, Francja i Niderlandy są krajami, z których generowane przepływy są wykrywane na nieco niższym poziomie i nie we wszystkich latach. Należy zwrócić uwagę, że w roku 2021 nie odnotowano ukierunkowanych przepływów z infrastruktury ulokowanej w Polce, po raz pierwszy od czasu gromadzenia i raportowania danych na ten temat – od roku 2015, kiedy to w poprzednich latach udział takich przepływów mieścił się w zakresie 10%-15%.

Biorąc pod uwagę specyfikę sieci internet (tzw. brak granic), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu Arakis GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie.

W związku z tym zaprezentowana statystyka odzwierciedla lokalizację złośliwej infrastruktury sieciowej w poszczególnych krajach, zaś duża liczba przepływów z Polski wynika ze specyfiki działania systemu Arakis GOV[138].

Zespół CSIRT GOV, na mocy art. 32a Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz Rozporządzenia Prezesa Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym, corocznie przeprowadza ocenę bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej. W ramach przeprowadzanych ocen bezpieczeństwa prowadzi szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej instytucji[139].

Liczba podatności w systemach teleinformatycznych w instytucjach poddanych ocenie bezpieczeństwa przez CSIRT GOV ze względu na kategorie w latach 2015-2021 została przedstawiona w tabeli 17 i na rysunku 13.

Tabela 17. Zakres oceny bezpieczeństwa systemów teleinformatycznych i liczba incydentów wykrytych przez CSIRT GOV w latach 2015-2021

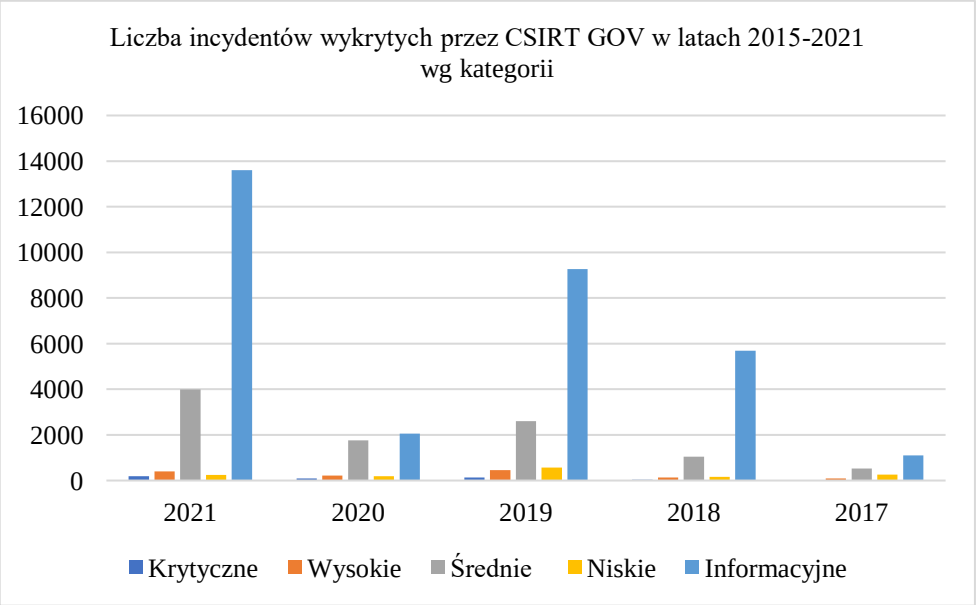
Instytucje i systemy teleinformatyczne	**2021**	**2020**	**2019**	**2018**	**2017**	**2016**	**2015**
• Ilość instytucji	17	14	10	-	-	-	-
• Ilość syst. teleinform.	185	82	35	-	-	-	-
Klasa podatności							
• Krytyczne	185	95	131	38	11	-	3%
• Wysokie	394	223	457	130	88	-	13%
• Średnie	3.993	1.761	2.608	1.051	530	-	Nd.
• Niskie	248	194	571	166	255	-	77%
• Informacyjne	13.607	2.056	9.268	5.690	1.098	-	7%

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP*, CSIRT-GOV ABW, 2022, s. 44, 2021, s. 47, 2020, 2019, 2018, 2017

[138] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 41, 2021, s. 42, 2020, s. 26

[139] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 44, 2021, s. 46, 2020, s. 30

Rys. 13. Liczba incydentów wykrytych przez CSIRT GOV w latach 2015-2021 wg kategorii



Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 44, 2021, s. 47, 2020, 2019, 2018, 2017

W roku 2021 zespól CSIRT GOV przeprowadził ocenę bezpieczeństwa systemów teleinformatycznych w 17 instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał w sumie 149 segmentów sieci i systemów teleinformatycznych oraz 36 domen i subdomen internetowych. W roku 2020 zespól CSIRT GOV przeprowadził ocenę bezpieczeństwa systemów teleinformatycznych w 14 instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał w sumie 82 systemy teleinformatyczne, a w roku 2019 w 10 instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadał w sumie 35 systemów teleinformatycznych. W ramach przeprowadzonych ocen bezpieczeństwa przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej instytucji. Do testów należało pasywne, półpasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, wykorzystywanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej[140]. W wyniku przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV dokonał identyfikacji szeregu podatności od stopnia informacyjnego, aż do błędów należących do kategorii krytycznych.

[140] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 44, 2021, s. 46, 47, 2020, s. 30

W roku 2021 względem roku 2020 liczba podatności krytycznych wzrosła o 95%, podatności wysokich o 77%, średnich o 127%, niskich o 28%, a informacyjnych o 562%, przy jednoczesnych wzroście liczby badanych podmiotów (z 14 do 17) i systemów teleinformatycznych oraz infrastruktury domen internetowych (z 82 do 185). W roku 2020 względem roku 2019 liczba podatności krytycznych spadła o 28%, podatności wysokich o 51%, średnich o 33%, niskich o 66%, a informacyjnych o 78%, przy jednoczesnych wzroście liczby badanych podmiotów (z 10 do 14) i systemów teleinformatycznych (z 35 do 82). Liczba podatności w systemach teleinformatycznych kluczowych podmiotów w kraju znacząco spadła względem roku poprzedniego. Liczba podatności w roku 2019 znacząco wzrosła względem roku 2018.

W ramach prowadzonych ocen bezpieczeństwa Zespół CSIRT GOV corocznie przeprowadza również analizę źródeł otwartych, tzw. OSINT. Czynności te pozwalają na określenie ilości danych zawartych jako metadata w dokumentach publikowanych w ramach publicznych serwerów WWW oraz na portalach społecznościowych, na których pracownicy posiadali aktywne konta. Dane te mogą posłużyć do przeprowadzenia ataków socjotechnicznych na pracowników instytucji[141].

Ataki cybernetyczne są coraz bardziej powszechne i wszechstronne. W ostatnim czasie zwiększyła się ilość działań w kierunku administracji rządowej i samorządowej oraz infrastruktury krytycznej. Zaprezentowane analizy raportów prezentowanych przez jednostki CERT Polska (CSIRT NASK) i CSIRT GOV realizujące zadania dla podmiotów gospodarki i administracji publicznej i rządowej pokazują jednoznacznie, że niezależnie od charakteru ujawnionych incydentów środowisko krajowych systemów teleinformatycznych jest w trybie ciągłym poddawane różnorodnym szkodliwym i przestępczym działaniom oraz atakom ze strony różnych aktorów i wymaga zapewnienia stałej ochrony. Ilość ataków stale, z roku na rok, wzrasta, wywołując stan zwiększającego się zagrożenia. Wynikać to może z kilku powodów, m.in.: ze zwiększonej aktywności wrogich podmiotów (grup hakerskich, państw) oraz zwiększonej ilości systemów teleinformatycznych administracji, dostawców usług kluczowych i operatorów infrastruktury krytycznej włączonych do systemów monitorowania i wczesnego ostrzegania[142].

[141] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2022, s. 52, 2021, s. 53, 2020, s. 34
[142] Mąkosa G., *Bezpieczeństwo cyberprzestrzeni RP*, wyd. cyt., s.94

2.5. Cyberbezpieczeństwo w dokumentach strategicznych bezpieczeństwa narodowego

Cyberbezpieczeństwo jako najnowsza i najbardziej wymagająca składowa bezpieczeństwa narodowego i międzynarodowego jest coraz istotniejszym jego komponentem, a zapewnienie odpowiednio wysokiego poziomu cyberbezpieczeństwa jest kluczowym wyzwaniem. Kwestia zapewnienia bezpieczeństwa informacyjnego czy cyberbezpieczeństwa jest przede wszystkim odpowiedzialnością i domeną państwa.

Strategiczne podejście do bezpieczeństwa, w tym bezpieczeństwa narodowego i cyberbezpieczeństwa, każe uwzględnić aspekty trwania, przetrwania i rozwoju podmiotu państwowego, w tym realizację jego wizji i celów strategicznych w odniesieniu do wyzwań, zagrożeń i szans. Strategia i polityka bezpieczeństwa, w których jasno zostały sformułowane cele strategiczne są podstawą do budowy koncepcji i metod bezpiecznego funkcjonowania podmiotu. Złożony i wielopłaszczyznowy charakter misji, celów i zadań państwa w dziedzinie bezpieczeństwa sprawia, że ich podmiotowym (organizacyjnym) odpowiednikiem powinien być jednolity, kolektywny i uporządkowany zbiór elementów, zdolny do skoordynowanego działania we wszystkich warunkach i okolicznościach funkcjonowania państwa[143]. Najbardziej generalne kształtowanie bezpieczeństwa jest zadaniem strategii i poprzez strategię jest ono realizowane[144]. Posiadanie strategii jest jednym ze środków zapewniania bezpieczeństwa, które to działanie, traktowane jako nadrzędny cel państwa, określa sposób politycznego ujęcia problemu[145]. Strategia jest dokumentem politycznym, w którym dość szczegółowo opisano plany i zamierzenia, jakie poszczególny rząd chce realizować w polityce wewnętrznej i, co do zasady, ma charakter otwarty[146]. Podstawą polityki ochrony przestrzeni cybernetycznej muszą być narodowe strategie, wynikające z uwarunkowań wewnątrzpaństwowych[147]. Polityka i strategia cyberbezpieczeństwa muszą również uwzględniać zmieniające się w czasie uwarunkowania zewnętrzne względem państwa, w tym regionalne i globalne, tak geopolityczne, społeczne i technologiczne.

---

[143] Kitler W., *System bezpieczeństwa*, wyd. cyt., s. 5
[144] Koziej S., *Bezpieczeństwo,* wyd. cyt., s. 21
[145] Zalewski S., *Strategia jako instrument bezpieczeństwa politycznego państwa*, DOCTRINA Studia Społeczno-Polityczne Nr 6, 2009, Akademia Podlaska, Siedlce, 2009, s. 42
[146] Brzostek A., *Organy władzy publicznej w zakresie ochrony cyberbezpieczeństwa w wybranych strategiach cyberbezpieczeństwa*, Przegląd Prawa Konstytucyjnego, ISSN 2082-1212, DOI 10.15804/ppk.2021.01.18, Nr 1 (59)/2021, Warszawa, 2021, s. 288
[147] tamże, s. 289

Kwestie cyberbezpieczeństwa są istotną składową polskich dokumentów strategicznych i operacyjnych bezpieczeństwa narodowego. Właściwe organy RP opracowały i wdrożyły dokumenty poziomu strategicznego i operacyjnego właściwe dla zapewnienia cyberbezpieczeństwa państwa i tworzące jego system cyberbezpieczeństwa. W ramach dokumentów strategicznych bezpieczeństwa Rzeczypospolitej Polskiej, w kontekście zagadnień cyberbezpieczeństwa, należy wymienić i poddać bliższej analizie aktualnie obowiązujące dokumenty strategiczne i operacyjne bezpieczeństwa, w tym w szczególności następujące:

- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[148];
- Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[149];
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[150];
- Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej[151];
- Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[152].

Wymienione dokumenty tworzą system cyberbezpieczeństwa odpowiadający stawianym wymaganiom wobec systemu bezpieczeństwa narodowego w przedmiotowym zakresie cyberbezpieczeństwa. Dokumenty strategiczne odpowiadają też na postawione wymagania teoretyczne dotyczące strategii bezpieczeństwa w systemie bezpieczeństwa narodowego[153].

2.5.1. Strategia Bezpieczeństwa Narodowego RP

Strategia Bezpieczeństwa Narodowego RP, ustanowiona w roku 2020, definiuje współczesne środowisko bezpieczeństwa jako coraz bardziej złożone i niepewne. Rosną interakcje polityczne, militarne, gospodarcze i społeczne w skali krajowej, regionalnej i globalnej. Wywiera to znaczący wpływ zarówno na strategię, jak i główne kierunki transformacji systemu bezpieczeństwa narodowego. Opracowanie i realizacja Strategii Bezpieczeństwa Narodowego RP wynika z potrzeby zapewnienia zdolności państwa do przeciwdziałania za-

[148] Strategia Bezpieczeństwa Narodowego RP, BBN 2020
[149] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Kancelaria Prezydenta/ BBN 2020
[150] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r., MP poz. 1037
[151] Doktryna cyberbezpieczeństwa RP, BBN 2015
[152] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Kancelaria Prezydenta/ BBN 2013
[153] Mąkosa G., *Strategiczne ujęcie cyberbezpieczeństwa*, wyd. cyt, s. 122

grożeniom i sprostania wyzwaniom, wynikającym ze zmieniających się uwarunkowań bezpieczeństwa Polski. Ma również na celu wykorzystanie szans, dzięki którym możliwa będzie poprawa bezpieczeństwa państwa i obywateli, zapewnienie jego dalszego rozwoju oraz wzmacnianie pozycji Rzeczypospolitej Polskiej na arenie międzynarodowej. Strategia określa kompleksową wizję kształtowania bezpieczeństwa narodowego Rzeczypospolitej Polskiej we wszystkich jego wymiarach. Strategia uwzględnia aspekt podmiotowy (wymiar wewnętrzny bezpieczeństwa narodowego oraz środowisko międzynarodowe – stosunki bilateralne, współpracę regionalną, w skali globalnej oraz współpracę na forach organizacji międzynarodowych) oraz przedmiotowy (uwzględnia wszystkie wymiary funkcjonowania systemu bezpieczeństwa narodowego). Strategia formułuje również interesy narodowe oraz cele strategiczne w dziedzinie bezpieczeństwa narodowego, które zostały sformułowane w zgodzie z wartościami narodowymi określonymi w Konstytucji Rzeczypospolitej Polskiej. Strategia wskazuje, że jej zapisy powinny znaleźć rozwinięcie i odzwierciedlenie w krajowych dokumentach strategicznych w dziedzinie bezpieczeństwa narodowego i rozwoju Polski. Strategia Bezpieczeństwa Narodowego określa środowisko bezpieczeństwa, w ramach którego wskazuje na aspekty podejmowanych w otoczeniu wszechstronnych i kompleksowych działań za pomocą środków pozamilitarnych (w tym: cyberataków i dezinformacji) oraz rozwoju zdolności do prowadzenia działań w wielu wymiarach, w tym w cyberprzestrzeni i w przestrzeni kosmicznej. Zwraca uwagę na szybki postęp w dziedzinie technologii cyfrowych, co powoduje konieczność efektywnego wykorzystania najnowszych technologii, co również stwarza nowe możliwości rozwojowe dla Polski, równocześnie generując nieznane wcześniej zagrożenia. Uwaga Strategii jest skierowana na systemy łączności, które są kluczowym elementem zasobów bezpieczeństwa narodowego i gotowości na wypadek sytuacji kryzysowych, a zatem stanowią ważny element krajowej infrastruktury krytycznej. W zakresie systemów łączności kluczowym wyzwaniem jest rozbudowa bezpiecznych i nowoczesnych sieci telekomunikacyjnych, zdolnych obsłużyć coraz większą ilość użytkowników końcowych i systemów. W kontekście rewolucji cyfrowej uwzględnia szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej ze względu na stwarzanie możliwości dezinformacji i manipulacji informacją[154].

Struktura dokumentu Strategii jest zbudowana w oparciu o zdefiniowane filary bezpieczeństwa narodowego. Ich realizacja odbywa się poprzez osiąganie wynikających z nich

[154] Strategia Bezpieczeństwa Narodowego RP, wyd. cyt., s. 5, 6, 7

celów strategicznych, wymagających zaplanowania i wdrożenia określonych zadań oraz posiadania i wykorzystania odpowiednich sił, środków oraz zdolności. Obejmują one, niżej wymienione, kluczowe przygotowania i działania strategiczne. Kwestie cyberbezpieczeństwa państwa zostały ulokowane w ramach filaru I - Bezpieczeństwo państwa i obywateli, realizującego interes narodowy: strzeżenie niepodległości, nienaruszalności terytorialnej, suwerenności oraz zapewnienie bezpieczeństwa państwa i obywateli. W ramach filaru I zostały zdefiniowane działania strategiczne, wśród których są również te odnoszące się i adresujące kwestie cyberbezpieczeństwa. Działanie strategiczne „Odporność państwa i obrona powszechna" w ramach celu „Podniesienie odporności państwa na zagrożenia, poprzez tworzenie systemu obrony powszechnej, opartego na wysiłku całego narodu oraz budowanie zrozumienia dla rozwoju odporności i zdolności obronnych Rzeczypospolitej Polskiej" realizuje zadanie 2.10 „Rozwijać zdolności państwa w zakresie zapobiegania i reagowania na zagrożenia o charakterze terrorystycznym oraz zwalczania przestępczości zorganizowanej, z uwzględnieniem działalności przestępczej w cyberprzestrzeni". Działanie strategiczne „Siły zbrojne rzeczypospolitej polskiej" w ramach celu „Wzmocnienie zdolności operacyjnych Sił Zbrojnych Rzeczypospolitej Polskiej do odstraszania i obrony przed zagrożeniami bezpieczeństwa, ze szczególnym uwzględnieniem podniesienia poziomu mobilności i modernizacji technicznej" realizuje zadanie 3.10 „Uzyskać zdolności operacyjne do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, rozwijać wojska obrony cyberprzestrzeni oraz zbudować zdolności do prowadzenia działań w przestrzeni kosmicznej, jak również do działań informacyjnych". Działanie strategiczne „Cyberbezpieczeństwo" w ramach celu „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji" realizuje zestaw działań adresujących kwestie cyberbezpieczeństwa. Zadania w ramach ww. działania strategicznego i celu to[155]:

1. Zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia;
2. Wzmacniać defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa;

[155] Strategia Bezpieczeństwa Narodowego RP, wyd. cyt., s. 20

3. Uzyskać zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
4. Rozwijać krajowe zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa;
5. Rozwijać kompetencje, wiedzę oraz świadomość zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa;
6. Wzmacniać i rozbudowywać potencjał państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego.

Podjęta i przedstawiona przez autora problematyka jest właściwa dla zdefiniowanego w Strategii Bezpieczeństwa Narodowego celu podniesienia poziomu odporności na cyberzagrożenia oraz zwiększenia poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Problematyka rozprawy adresuje działanie strategiczne „Cyberbezpieczeństwo" w zakresie zadania 1. Zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia, poprzez opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych oraz w zakresie zadania 2. Wzmacniać defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa, poprzez realizację wszystkich hipotez i celów szczegółowych rozprawy.

Powyższy, aktualny dokument Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej jest poprzedzony dokumentem Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z roku 2014. Poprzednia Strategia w sposób całościowy ujmowała zagadnienia bezpieczeństwa narodowego oraz wskazywała optymalne sposoby wykorzystania wszystkich zasobów pozostających w dyspozycji państwa w sferze obronnej, ochronnej, społecznej i gospodarczej na potrzeby bezpieczeństwa. Wskazywała, że kluczową sprawą jest ich właściwa integracja w systemie bezpieczeństwa narodowego. Poprzednia Strategia

wskazywała, że Rzeczpospolita Polska zapewnia bezpieczeństwo państwa i obywateli poprzez stwarzanie warunków do realizacji interesów narodowych i osiągania celów strategicznych, a z układu interesów wynikają odpowiadające im cele strategiczne w dziedzinie bezpieczeństwa, w tym zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni. Bezpieczne funkcjonowanie systemu teleinformatycznego Rzeczypospolitej Polskiej jest warunkiem niezakłóconego działania całego państwa. Poprzednia Strategia definiowała podejście, że zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni RP, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa, powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Do najważniejszych zadań przygotowawczych w obszarze cyberbezpieczeństwa miało należeć wdrożenie i rozwijanie systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym, a także określenie zasad prowadzenia aktywnej obrony oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP, kompatybilnego z systemami państw sojuszniczych. Jako istotne wskazane było stworzenie narodowego ośrodka koordynacji wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymianę informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa. Za ważne wskazano nabycie pełnych kompetencji do rozpoznawania, zapobiegania i zwalczania cyberzagrożeń oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni[156].

2.5.2. Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP

Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej do 2022[157] jest kolejnym dokumentem rozpatrywanym w odniesieniu do cyberbezpieczeństwa. Strategia ta za cel główny stawia wzmocnienie efektywności i spójności systemu bezpieczeństwa narodowego, który powinien być zdolny do identyfikacji i eliminacji źródeł, przejawów oraz skutków zagrożeń bezpieczeństwa narodowego, co również adresuje kwestie związane z cyberbezpieczeństwem. Realizacji celu głównego służą zdefiniowane cele

[156] Mąkosa G., *Krajowy system cyberbezpieczeństwa RP*, wyd. cyt., s. 238
[157] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej do 2022, BBN

operacyjne, stanowiące rozwinięcie celu głównego w dziedzinach posiadających kluczowe znaczenie dla bezpieczeństwa narodowego a adresowane do organów administracji publicznej. Podmiotem Strategii jest całe państwo, w tym organy administracji publicznej oraz społeczeństwo obywatelskie.

Szczególne zadania podmiotów odpowiedzialnych za wdrożenie i monitorowanie realizacji strategii oraz jej ocenę, związane z realizacją strategii w obszarze cyberbezpieczeństwa zostały przedstawione poniżej dla wybranych podmiotów, tj. ministrów właściwych do spraw administracji publicznej, informatyzacji, łączności, Szefa ABW, Dyrektora RCB. Ministrowie właściwi do spraw administracji publicznej, informatyzacji, łączności są odpowiedzialni za wdrożenie systemu łączności na potrzeby administracji publicznej, systemu kierowania bezpieczeństwem narodowym, bezpieczeństwem i porządkiem publicznym oraz ratownictwa, doskonalenie zdolności do wsparcia działań Sił Zbrojnych RP i wojsk sojuszniczych w okresie zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny, opracowanie Polityki ochrony cyberprzestrzeni oraz rozwijanie Systemu Reagowania na Incydenty Komputerowe. Szef ABW ma określoną odpowiedzialność w zakresie poprawy zdolności rozpoznania i ochrony przed zagrożeniami bezpieczeństwa państwa, doskonalenia zasad i mechanizmów współpracy z właściwymi podmiotami na rzecz zapewnienia bezpieczeństwa cybernetycznego, rozwijania Systemu Reagowania na Incydenty Komputerowe, realizacji przedsięwzięć związanych z tworzeniem Rządowego Programu Rezerw Strategicznych. Dyrektor RCB jest odpowiedzialny za doskonalenie działań podmiotów i struktur organizacyjnych właściwych do spraw zarządzania kryzysowego i reagowania obronnego do funkcjonowania w okresie pokoju, kryzysu i w czasie wojny, zapewnienie spójności procesów i dokumentów planowania obronnego i zarządzania kryzysowego, realizację przedsięwzięć w ramach planowania cywilnego, wdrożenie i aktualizację, we współpracy z właściwymi ministrami i innymi podmiotami - Narodowego Programu Ochrony Infrastruktury Krytycznej, Krajowego Planu Zarządzania Kryzysowego oraz Raportu o zagrożeniach bezpieczeństwa narodowego, wdrażanie przedsięwzięć i procedur systemu zarządzania kryzysowego, współpracę z organami i podmiotami krajowymi i międzynarodowymi na rzecz zapewnienia bezpieczeństwa cybernetycznego oraz realizację przedsięwzięć w ramach planowania cywilnego, w tym w czasie podwyższania gotowości obronnej państwa i okresie po wprowadzeniu stanów nadzwyczajnych[158].

[158] tamże, s. 89

Strategia wskazuje, że dokumentami wdrożeniowymi jej zapisów w zakresie cyberbezpieczeństwa są Narodowy Program Ochrony Infrastruktury Krytycznej i Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej[159].

2.5.3. Strategia Cyberbezpieczeństwa RP

Strategia cyberbezpieczeństwa RP jest dokumentem najbardziej bezpośrednio i kompleksowo adresującym problematykę cyberbezpieczeństwa, poświęconym wprost tym zagadnieniom. Strategia Cyberbezpieczeństwa RP na lata 2019–2024, ustanowiona w roku 2019 przez Prezydenta RP, we wstępie definiuje przesłanki do działań zwiększających cyberbezpieczeństwo. Zwrócono szczególną uwagę na[160]:

- zależność rozwoju społeczno-gospodarczego od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym;
- wpływ dynamicznego rozwoju systemów informacyjnych na rozwój gospodarki narodowej, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych oraz na kształtowanie relacji społecznych i wpływ na zachowania grup społecznych, a także oddziaływania w sferze politycznej;
- wpływ znaczących zakłóceń funkcjonowania cyberprzestrzeni, na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe;
- wyzwanie, jakim jest ochrona systemów informacyjnych oraz przetwarzanych w nich informacji dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów informacyjnych, organów władzy publicznej, organów odpowiedzialnych za bezpieczeństwo narodowe, a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej.

Strategia Cyberbezpieczeństwa definiuje kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej. W ramach takiego ujęcia Strategia stwierdza, że jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na

[159] Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej (2013) została zastąpiona w 2017 r. dokumentem Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022, a ten dokument został zastąpiony w 2022 r. Strategią Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2022-2024.
[160] Strategia Cyberbezpieczeństwa, wyd. cyt., s. 5

celu podniesienie poziomu cyberbezpieczeństwa RP. Zamierzeniem Strategii Cyberbezpieczeństwa jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na cyberzagrożenia, a także zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń. Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) i szpiegowskim w cyberprzestrzeni. Strategia Cyberbezpieczeństwa ma być spójna z prowadzonymi działaniami dotyczącymi systemów teleinformatycznych operatorów infrastruktury krytycznej oraz uwzględniać potrzeby zapewnienia zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych[161].

W ramach swojego zakresu Strategia Cyberbezpieczeństwa definiuje cele i priorytety w zakresie cyberbezpieczeństwa, podmioty zaangażowane w jej wdrażanie i realizację, środki służące realizacji celów, środki w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym, podejście do oceny ryzyka, działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych oraz badawczo-rozwojowych w zakresie cyberbezpieczeństwa[162].

Strategia Cyberbezpieczeństwa ma oddziaływać w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli. Strategia Cyberbezpieczeństwa określa wizję, cel główny i cele szczegółowe. Wizja zdefiniowana w Strategii Cyberbezpieczeństwa określa pomyślny rozwój Rzeczypospolitej Polskiej, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym aktywność społeczna oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa, są związane ze sprawnym i bezpiecznym działaniem systemów informacyjnych i środków komunikacji elektronicznej. W ramach działań zaplanowanych w Strategii Cyberbezpieczeństwa rząd ma systematycznie wzmacniać i rozwijać krajowy system cyberbezpieczeństwa. Działania uwzględniają systemowe

[161] Mąkosa G., *Strategiczne ujęcie cyberbezpieczeństwa*, wyd. cyt., s. 128,
[162] Strategia Cyberbezpieczeństwa, wyd. cyt., s. 7

rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych oraz prowadzenie badań naukowych tak, aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze oprogramowania, urządzeń i usług cyfrowych. Działania rządu będą podejmowane z poszanowaniem praw i obywateli oraz przez budowę zaufania między poszczególnymi sektorami rynkowymi a administracją publiczną. Celem głównym Strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

W ramach celów szczegółowych zdefiniowano 5 celów, z których każdy zawiera zadania prowadzące do realizacji przyjętych celów[163]:

1. Cel szczegółowy 1 – Rozwój krajowego systemu cyberbezpieczeństwa:
   1.1. Wdrożenie i ocena funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa;
   1.2. Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa;
   1.3. Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym;
   1.4. Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej;
   1.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym;
   1.6. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym.
2. Cel szczegółowy 2 – Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty:
   2.1. Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń;
   2.2. Bezpieczeństwo łańcucha dostaw;
   2.3. Testy i audyty cyberbezpieczeństwa;

[163] tamże, s. 8

3. Cel szczegółowy 3 – Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa:
   3.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
   3.2. Nastawienie na rozwój współpracy między sektorem publicznym i prywatnym;
   3.3. Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa;
   3.4. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
4. Cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa:
   4.1. Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej;
   4.2. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli;
   4.3. Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni;
5. Cel szczegółowy 5 – Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa:
   5.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym;
   5.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym.

Strategia Cyberbezpieczeństwa RP została poddana procesowi przeglądu i aktualizacji na przełomie lat 2021/22 i zapewne zostanie zaktualizowana w roku 2022. Racjonalnym i pożądanym byłoby dopasowanie i zsynchronizowanie zapisów Strategii Cyberbezpieczeństwa i Strategii Bezpieczeństwa Narodowego oraz Doktryny Cyberbezpieczeństwa.

Problematyka podjęta przez autora jest właściwa dla zdefiniowanego w Strategii Cyberbezpieczeństwa celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa zadania 1.2. Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa poprzez realizację wszystkich hipotez i celów szczegółowych rozprawy. Natomiast poprzez realizację celów opracowania koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych rozprawa adresuje zadanie 1.4. Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury kry-

tycznej sformułowanych celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz cel szczegółowy 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Dokumentem poprzedzającym Strategię Cyberbezpieczeństwa RP na lata 2019–2024 jest dokument Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022 (KRPC, Krajowe Ramy). Jest to dokument, który wpisywał się w kontynuację działań, podejmowanych w przeszłości przez administrację rządową, mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP, w tym przyjętą przez rząd w 2013 roku Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, którą zastąpił. Krajowe Ramy Polityki Cyberbezpieczeństwa RP to dokument strategii w zakresie cyberbezpieczeństwa państwa, został opracowany przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego. Zamierzeniem KRPC RP było określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane w KRPC kierunki strategiczne miały również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. Krajowe Ramy Polityki Cyberbezpieczeństwa były spójne z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej, wykorzystujących systemy teleinformatyczne oraz uwzględniały potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej Polskiej. Celem głównym, postawionym przez KRPC było zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych. Cel główny rozłożony jest na 4 cele szczegółowe, a te z kolei na cele niższego rzędu[164]. Cele szczegółowe Krajowych Ram Polityki Cyberbezpieczeństwa RP, to[165]:

[164] Mąkosa G., *Krajowy system cyberbezpieczeństwa RP*, wyd. cyt., s. 233, 234
[165] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022

1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa;
2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom;
3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni;
4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

2.5.4. Doktryna Cyberbezpieczeństwa RP

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej powołana w roku 2015 określa warunki do zespolenia i strategicznego ukierunkowania wysiłków na rzecz budowania zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Przede wszystkim określa cel strategiczny, który ma zostać osiągnięty przez implementację zadań o charakterze operacyjnym i przygotowawczym w dziedzinie cyberbezpieczeństwa. Ponadto zawiera ocenę zagrożeń, ryzyk i szans w dynamicznie rozwijającym się środowisku cyberbezpieczeństwa, a także wskazuje najważniejsze czynności operacyjne jakie mają być podjęte w sektorze publicznym, prywatnym i obywatelskim oraz wskazuje czynności przygotowawcze mające na celu doskonalenie, rozwój i transformację systemu cyberbezpieczeństwa, z uwzględnieniem podsystemu kierowania oraz publicznych i prywatnych ogniw wykonawczych[166].

Doktryna cyberbezpieczeństwa RP jest dokumentem realizującym strategiczny cel w obszarze cyberbezpieczeństwa RP, sformułowany w Strategii Bezpieczeństwa Narodowego RP, jakim jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia. Dokument określa sposób osiągnięcia wyznaczonego celu strategicznego

[166] Oleksiewicz I., *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne rzeczypospolitej polskiej*, Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie, nr 33 (2019), Częstochowa, 2019, s. 148

przez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Główne cele operacyjne to[167]:

1. ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans;
2. zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans;
3. obrona i ochrona własnych systemów i zgromadzonych w nich zasobów;
4. zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne);
5. po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

Doktryna Cyberbezpieczeństwa RP wskazuje, że do osiągnięcia powyższych celów operacyjnych potrzebne jest, w wymiarze preparacyjnym, zbudowanie, utrzymywanie i systematyczne doskonalenie (rozwój) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo systemu cyberbezpieczeństwa RP obejmującego[168]:

1. podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie cyberbezpieczeństwa;
2. podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych.

Zgodnie z przyjętą Doktryną Cyberbezpieczeństwa zapewnienie bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej powinno być realizowane w kilku płaszczyznach: przez sektor publiczny, sektor komercyjny, obywatelski oraz w wymiarze transsektorowym[169]. Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym. Do jednych z głównych zadań sektora publicznego w wymiarze krajowym należą rozpoznawanie realnych i potencjalnych źródeł zagrożeń, ciągła analiza

[167] Doktryna cyberbezpieczeństwa, wyd. cyt., s. 9
[168] tamże, s. 9
[169] Oleksiewicz I., *Bezpieczeństwo informacyjne*, wyd. cyt., s. 148

ryzyka w odniesieniu do ważnych obiektów infrastruktury krytycznej, działania w dziedzinie kryptografii i kryptoanalizy, bieżący monitoring newralgicznych punktów systemu bezpieczeństwa, audyt środków i mechanizmów cyberbezpieczeństwa, wdrażanie scenariuszy postępowania w razie cyberataków, opracowywanie i aktualizacja planów reagowania kryzysowego oraz operacyjnych planów funkcjonowania w czasie zagrożenia i wojny, prowadzenie aktywnej cyberobrony oraz utrzymanie gotowości do cyberwojny, ochrona i obrona systemów teleinformatycznych i zasobów danych, wspieranie kluczowych podmiotów sektora prywatnego, przeciwdziałanie i zwalczanie cyberprzestępczości, a także bieżące działania informacyjne i edukacyjne skierowane do społeczeństwa w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz informowanie o zidentyfikowanych zagrożeniach. Główne jego zadnia na poziomie międzynarodowym, to wymiana informacji o podatnościach, zagrożeniach i incydentach, udział w reagowaniu na zagrożenia w cyberprzestrzeni, wymiana doświadczeń i dobrych praktyk, a także oddziaływanie na transnarodowe struktury sektora prywatnego. Doktryna wskazuje także główne zadania sektora prywatnego, do których należą współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, prowadzenie audytu środków i mechanizmów cyberbezpieczeństwa, wymiana informacji dotyczących zagrożeń dla cyberbezpieczeństwa oraz o podatnościach, zagrożeniach i incydentach. Jako główne zadania transsektorowe Doktryna wskazuje koordynację współpracy podmiotów sektora prywatnego i publicznego oraz tworzenie mechanizmów wymiany informacji, a także standardów i dobrych praktyk w obszarze cyberbezpieczeństwa[170].

Cel Doktryny Cyberbezpieczeństwa zapewnienia adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych jest adresowany poprzez realizacją celu rozprawy opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych. Zdefiniowane w Doktrynie zagadnienia i zadania dotyczące zbudowania, utrzymywania i systematycznego doskonalenia (rozwoju) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo systemu cyberbezpieczeństwa RP składającego się z podsystemu kierowania i podsystemów operacyjnych i wsparcia adresowane są

[170] Doktryna cyberbezpieczeństwa, wyd. cyt., s. 14-16

w rozprawie poprzez opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym i koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.

Doktryna Cyberbezpieczeństwa RP jest dokumentem adresującym cele cyberbezpieczeństwa zdefiniowane w Strategii Bezpieczeństwa Narodowego z roku 2014, wymaga więc aktualizacji. Aktualnie obowiązująca Strategia Bezpieczeństwa Narodowego (2020) inaczej definiuje wartości interesy i cele, w tym dotyczące cyberbezpieczeństwa. Synchronizacja zaktualizowanych dokumentów może zapewnić efekt systemowego i strategicznego podejścia do zarządzania cyberbezpieczeństwem[171].

2.5.5. Biała Księga Bezpieczeństwa Narodowego RP

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej ustanowiona przez prezydenta RP w roku 2013 określa strategiczne zadania w zakresie cyberbezpieczeństwa, które obejmują: przeciwdziałanie zagrożeniom w cyberprzestrzeni, ochronę systemów informacyjnych państwa, rozwój współpracy i koordynację działań ochronnych z podmiotami sektora prywatnego, szczególnie w sferze dostępu do informacji o dokonywanych atakach i ich rodzajach, prowadzenie działań o charakterze prewencyjnym i profilaktycznym w zakresie ochrony obywateli przed zagrożeniami płynącymi z cyberprzestrzeni, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców, prowadzenie ofensywnej i defensywnej walki informacyjnej w cyberprzestrzeni, a także koordynację działań z innymi podmiotami systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej[172].

System bezpieczeństwa narodowego RP jest zbudowany w oparciu o dokumenty strategiczne i akty prawne go definiujące. Polska cyberprzestrzeń i jej bezpieczeństwo powinna mieć oparcie w stosownych, dobrze opracowanych regulacjach prawnych oraz dokumentach strategicznych bezpieczeństwa państwa i wynikających z nich rozwiązań strukturalnych, systemowych, organizacyjnych i technicznych. Rozwiązania dokumentów strategicznych powinny konstytuować holistyczny, zintegrowany system cyberbezpieczeństwa państwa będący integralną częścią systemu bezpieczeństwa narodowego.

[171] Mąkosa G., *Strategiczne ujęcie cyberbezpieczeństwa*, wyd. cyt., s.127
[172] Biała Księga Bezpieczeństwa Narodowego, wyd. cyt., s. 172

2.6. Cyberbezpieczeństwo w regulacjach prawnych

Kwestie cyberbezpieczeństwa państwa jako aspektu bezpieczeństwa narodowego, mającego coraz większy wpływ oraz coraz większy stopień skomplikowania technologicznego i dynamicznych zmian, stanowią istotne wyzwanie nie tylko na poziomie poszczególnych pojedynczych krajów, ale także na poziomie związków państw, jak np. Unia Europejska.

Unia Europejska jako podmiot polityczny, tworzy regulacje prawne – dyrektywy i rozporządzenia – obowiązujące jej członków, również w zakresie cyberbezpieczeństwa i ochrony danych. Spośród regulacji unijnych warto wskazać na te bezpośrednio adresujące poruszane kwestie, tj.:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, (Dyrektywa NIS);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Akt o cyberbezpieczeństwie);
- Strategia Cyberbezpieczeństwa UE (budowanie odporności UE na ataki cybernetyczne, kształtowanie skutecznej unijnej prewencji cybernetycznej, wzmocnienie współpracy międzynarodowej w dziedzinie bezpieczeństwa cybernetycznego);
- Strategia bezpieczeństwa UE na lata 2020-2025 (EU Security Union Strategy) - adresująca również kwestie cyberbezpieczeństwa.

Polska będąc niezależnym państwowym podmiotem politycznym tworzy, w ramach swojego systemu prawnego, rozwiązania strategiczne i prawne (legislacyjne), w tym również implementujące regulacje Unii Europejskiej. W ramach polskiego porządku prawnego i zarządzania strategicznego bezpieczeństwem narodowych zostały ustanowione stosowne regulacje prawne adresujące przedmiotową problematykę cyberbezpieczeństwa i bezpieczeństwa systemów teleinformatycznych, tj.:

- ustawa o krajowym systemie cyberbezpieczeństwa[173] wraz z towarzyszącymi rozporządzeniami wykonawczymi, stanowiące krajowy system cyberbezpieczeństwa[174], implementujące Dyrektywę NIS do polskiego porządku prawnego;
- ustawa o zarządzaniu kryzysowym[175] wraz z towarzyszącymi rozporządzeniami wykonawczymi i dokumentami operacyjnymi, stanowiące system zarządzania kryzysowego;
- ustawa o informatyzacji podmiotów realizujących zadania publiczne[176] wraz z towarzyszącymi rozporządzeniami wykonawczymi i dokumentami operacyjnymi, stanowiące system informatyzacji podmiotów publicznych.

Dokumenty te wyznaczają strategiczną perspektywę, punkty odniesienia i ramy cyberbezpieczeństwa, a także cele i zadania do osiągnięcia odpowiedniego jego poziomu. Regulacje prawne wskazane powyżej definiują zagadnienia cyberbezpieczeństwa, podmioty zaangażowane oraz ich odpowiedzialność, przedmiot zainteresowania danej regulacji oraz aspekty organizacyjne funkcjonowania systemu cyberbezpieczeństwa[177]. W/w regulacje prawne definiują również wymagania wobec podmiotów nimi objętych dotyczące wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa[178]. Charakterystyka regulacji prawnych dotyczących cyberbezpieczeństwa przedstawiona jest w tabeli 18 poniżej.

[173] Ustawa o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560 z późn. zmianami (Dz.U. 2022 poz. 655)
[174] Autor zastosował określenia: system zarządzania kryzysowego, krajowy system cyberbezpieczeństwa, system informatyzacji podmiotów publicznych w publikacjach: *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych* (2020), *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne* (2020), *Organizacja systemu cyberbezpieczeństwa RP* (2020)
[175] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 Nr 89 poz. 590 z późn. zmianami (Dz.U. 2021 poz. 159)
[176] Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565 z późn. zmianami (Dz. U. 2020 r. poz. 346, 568, 695 i 1517)
[177] Mąkosa G., *Cyberbezpieczeństwo,* wyd. cyt., s. 109
[178] Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, w: Studia Bezpieczeństwa Narodowego, 2020, 17(1), WAT, Warszawa 2020, s. 139

Tabela 18. Charakterystyka regulacji prawnych dotyczących cyberbezpieczeństwa

Domena, podmiot, przedmiot regulacji	Nazwa regulacji i dokumentów towarzyszących
Zarządzanie kryzysowe Podmiot – operatorzy infrastruktury krytycznej Przedmiot – infrastruktura krytyczna, usługi kluczowe IK	• Ustawa o zarządzaniu kryzysowym, • Rozp. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej • Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) • Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje
Krajowy system cyberbezpieczeństwa Podmiot – operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty realizujące zadania publiczne Przedmiot – infrastruktura teleinformatyczna, usługi kluczowe, usługi cyfrowe	• Ustawa o krajowym systemie cyberbezpieczeństwa • Rozp. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo • Rozp. w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych
Informatyzacja podmiotów publicznych Podmiot – podmioty realizujące zadania publiczne Przedmiot – systemy teleinformatyczne, rejestry publiczne	• Ustawa o informatyzacji podmiotów realizujących zadania publiczne, • Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Źródło: Mąkosa G., *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 109 na podstawie: 1. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, 2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, 3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565.

Wskazane powyżej regulacje prawne odnoszą się w pewnym zakresie, każda w innym, do kwestii cyberbezpieczeństwa w aspektach zorganizowania zarządzania i struktur na poziomie krajowym i operacyjnym, zakresu objętych nimi systemów, sektorów i typów podmiotów czy zapewnienia bezpieczeństwa systemów teleinformatycznych. Objęte regulacjami sektory i usługi mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej[179], realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[180], są realizowane w celu ochrony interesu publicznego[181]. Domeną oddziaływania cyberbezpieczeństwa jest cyberprzestrzeń i składające

[179] adresowane przez Ustawę o krajowym systemie cyberbezpieczeństwa, wyd. cyt.
[180] adresowane przez Ustawę o zarządzaniu kryzysowym, wyd. cyt.
[181] adresowane przez Ustawę o informatyzacji, wyd. cyt.

się na nią zasoby informacyjne i systemy teleinformatyczne, realizujące usługi cyfrowe społeczeństwa informacyjnego, wspomagające działalność administracji i podmiotów realizujących zadania publiczne oraz stanowiące publiczną i prywatną teleinformatyczną infrastrukturę krytyczną, infrastrukturę teleinformatyczną wspomagającą funkcjonowanie pozostałych systemów infrastruktury krytycznej, czyli tzw. usług kluczowych. Zagadnienie cyberbezpieczeństwa, czyli bezpieczeństwa systemów teleinformatycznych istotnych ze względu na bezpieczeństwo państwa, można rozpatrywać z trzech perspektyw wynikających z kontekstu nadanego przez regulacje prawne – w ujęciu zarządzania kryzysowego, traktującego te systemy, jako krytyczną infrastrukturę teleinformatyczną, w ujęciu krajowego systemu cyberbezpieczeństwa, traktującego te systemy, jako infrastrukturę usług kluczowych i usług cyfrowych oraz w ujęciu systemu informatyzacji podmiotów realizujących zadania publiczne, traktującego te systemy, jako infrastrukturę usług publicznych. Istotną w tym układzie perspektyw jest kwestia relacji między systemami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów realizujących zadania publiczne w zakresie struktury zarządzania i rozwiązań organizacyjnych zapewnienia bezpieczeństwa kluczowych dla bezpieczeństwa państwa systemów teleinformatycznych i cyberbezpieczeństwa, rozwiązań zarządzania bezpieczeństwem organizowanych i realizowanych na poziomie krajowym, systemów i sektorów oraz typów podmiotów systemów zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz struktur zarządzania i reagowania na incydenty i sytuacje kryzysowe zawartych w systemach zarządzania bezpieczeństwem. Bezpieczeństwo systemów teleinformatycznych usług krytycznych, kluczowych i cyfrowych zależne jest od rozwiązań ochrony ich infrastruktury teleinformatycznej oraz od systemów zarządzania bezpieczeństwem wdrożonych przez podmioty będące operatorami infrastruktury krytycznej, operatorami usług kluczowych i dostawcami usług cyfrowych oraz podmiotami realizującymi zadania publiczne[182].

2.6.1. Krajowy system cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa[183] (Ustawa KSC) wraz z towarzyszącymi rozporządzeniami - Rozporządzeniem w sprawie warunków organizacyjnych

[182] Mąkosa G., *Organizacja systemu cyberbezpieczeństwa RP*, [w:] P. Lizakowski (red.), Świat bez równowagi bezpieczeństwa. Studium wybranych problemów, Wydawnictwo FNCE, Poznań 2021, s. 181
[183] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt.

i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[184], Rozporządzeniem w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych[185] i Rozporządzeniem w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[186] wraz innymi powiązanymi rozporządzeniami stanowią dokumenty formalne, ustanawiające i definiujące krajowy system cyberbezpieczeństwa.

Ustawa o krajowym systemie cyberbezpieczeństwa wraz ze wspomnianymi rozporządzeniami towarzyszącymi są dokumentami o charakterze sprawczym, które m.in. regulują kwestie organizacyjne, decyzyjne i nadzorcze, co do działań podmiotów i ich odpowiedzialności, czego bardzo brakowało w dotychczasowych dokumentach strategicznych. Ustawa o krajowym systemie cyberbezpieczeństwa ma na celu wdrożenie uregulowań prawnych umożliwiających implementację unijnej dyrektywy NIS[187]. Ustawa KSC określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów Ustawy oraz zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. W Ustawie KSC zdefiniowane zostały typy incydentów (incydent, incydent krytyczny, incydent poważny, incydent istotny, incydent w podmiocie publicznym) mających wpływ na cyberbezpieczeństwo państwa. Cyberbezpieczeństwo zostało zdefiniowane jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Przedmiotem zainteresowania krajowego systemu cyberbezpieczeństwa są zdefiniowane w Ustawie KSC usługi kluczowe i usługi cyfrowe. Usługa kluczowa to usługa, która ma

[184] Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. 2018 poz. 1780

[185] Rozporządzenie w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, Dz. U. 2018 poz. 2080

[186] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz. U. poz. 1806

[187] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych, w załączniku nr 1 do Ustawy KSC. Usługa cyfrowa to usługa świadczona drogą elektroniczną, tj. - internetowa platforma handlowa, usługa przetwarzania w chmurze, wyszukiwarka internetowa, wymienione w załączniku nr 2 do Ustawy KSC. Ustawa KSC określa podmioty i typy podmiotów, należące do różnych sektorów, objęte krajowym systemem cyberbezpieczeństwa oraz typy podmiotów, do których zapisów ustawy się nie stosuje. Zdefiniowane zostały nowe typy podmiotów operujące w krajowym systemie cyberbezpieczeństwa – operator usługi kluczowej, dostawca usługi cyfrowej, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa (Pojedynczy Punkt Kontaktowy) oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (Pełnomocnik) i Kolegium do Spraw Cyberbezpieczeństwa (Kolegium). W ustawie KSC ustanowiono procesy obsługi i zarządzania incydentami cyberbezpieczeństwa, zarówno na poziomie podmiotów objętych regulacjami, jak i na poziomie krajowym i międzynarodowym – europejskim oraz struktury organizacyjne, relacje i procesy krajowego systemu cyberbezpieczeństwa, wskazując role, zadania i odpowiedzialność poszczególnych ww. podmiotów i organów[188].

Operatorem usługi kluczowej (OUK) jest podmiot, który świadczy usługę kluczową, świadczenie tej usługi zależy od systemów informacyjnych, a incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora, spełniający wymogi przynależności do sektora i podsektora oraz rodzaju podmiotu, określone w załączniku do Ustawy KSC, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Operator usługi kluczowej jest zobowiązany do wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniającego[189]:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy;

[188] Ustawa o krajowym systemie cyberbezpieczeństwa , wyd. cyt., art. 2, 3, 4, 5, 8, 17, 18
[189] tamże, art. 5, 8

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Operator usługi kluczowej ma obowiązek opracowania, stosowania, aktualizowania i nadzorowania dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Zgodnie z zapisami przywołanego powyżej rozporządzenia, dokumentację stanowi dokumentacja normatywna i dokumentacja operacyjna, która merytorycznie powinna się opierać m.in. na międzynarodowych i polskich normach PN-ISO/IEC ISO 27001 i PN-ISO ISO 22301. Operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej – operatorem infrastruktury krytycznej - który posiada zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania dokumentacji cyberbezpieczeństwa. Operator usługi kluczowej w zakresie obsługi i zarządzania incydentami cyberbezpieczeństwa jest zobowiązany zapewniać obsługę i klasyfikację takich incydentów, zgłaszać incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz współdziałać nim podczas obsługi incydentu poważnego i incydentu krytycznego. Operator jest także zobowiązany usuwać podatności systemu informacyjnego i informować o tym organ właściwy do spraw cyberbezpieczeństwa. Operator usługi kluczowej w celu realizacji zadań w zakresie zapewnienia cyberbezpieczeństwa oraz obsługi i zarządzania incydentami musi powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. Wewnętrzne struktury i zewnętrzne podmioty są zobowiązane spełniać wymagania określone w przywołanym powyżej rozporządzeniu, dotyczące warunków organizacyjnych i technicznych ich działalności oraz zobowiązujące do dysponowania prawem

do wyłącznego korzystania z pomieszczeń, które wyposażone są w adekwatne zabezpieczenia techniczne[190].

Dostawcą usługi cyfrowej (DUC) jest podmiot - osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców. Dostawca usługi cyfrowej zobowiązany jest do podejmowania środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi. Dostawca usługi cyfrowej jest zobowiązany do podejmowania właściwych i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te mają zapewniać cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniać[191]:

1) bezpieczeństwo systemów informacyjnych i obiektów;
2) postępowanie w przypadku obsługi incydentu;
3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;
4) monitorowanie, audyt i testowanie;
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi.

Dostawca usługi cyfrowej w zakresie obsługi i zarządzania incydentami cyberbezpieczeństwa jest zobowiązany zapewniać obsługę i klasyfikację incydentów, zgłaszać incydenty istotne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz współdziałać nim podczas obsługi incydentu istotnego i incydentu krytycznego, przekazywać operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora oraz usuwać podatności systemu informacyjnego[192].

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego w zakresie obsługi i zarządzania incydentami cyberbezpieczeństwa jest zobowiązany zarządzać incydentami, zgłaszać incydenty do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz współdziałać nim podczas obsługi incydentu w podmiocie publicznym

[190] tamże, art. 10, 11, 14
[191] tamże, art. 17
[192] tamże, art. 18

i incydentu krytycznego, zapewniać osobom, na rzecz których realizowane są zadania publiczne dostęp do wiedzy o zagrożeniach cyberbezpieczeństwa i sposobach zabezpieczania się przed nimi[193].

Rozwiązania organizacyjne systemu cyberbezpieczeństwa zdefiniowane w przepisach prawnych krajowego systemu cyberbezpieczeństwa (Ustawy KSC i wskazanych rozporządzeń), właściwe dla zakresu problemów badawczych niniejszej dysertacji zostaną przybliżone kontekstowo w kolejnych, dedykowanych poszczególnym problemom badawczym rozprawy jej rozdziałach: trzecim w odniesieniu do organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym, czwartym – odnośnie zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, piątym – dotyczącym kwestii doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i szóstym – adresującym kwestie wymaganych norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa państwa.

2.6.2. System zarządzania kryzysowego

Ustawa o zarządzaniu kryzysowym[194] (Ustawa ZK) wraz z Rozporządzeniem w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[195] oraz Narodowym Programem Ochrony Infrastruktury Krytycznej[196] (NPOIK) wraz z Załącznikiem 1 do NPOIK – Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje[197] stanowią dokumenty formalne ustanawiające i definiujące system zarządzania kryzysowego.

Ustawa o zarządzaniu kryzysowym ustanawia proces zarządzania kryzysowego, będący elementem kierowania bezpieczeństwem narodowych, który polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu

[193] tamże, art. 22
[194] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 Nr 89 poz. 590, z późn. zmianami (Dz.U. 2021 poz. 159)
[195] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. 2010 Nr 83 poz. 541
[196] Opracowany w 2015 r. i aktualizowany co ok. 2 lata przez Rządowe Centrum Bezpieczeństwa. Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej
[197] Opracowany i aktualizowany wraz z Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)

ich skutków i odtwarzaniu zasobów i infrastruktury krytycznej. Ustawa ZK ustanawia infrastrukturę krytyczną, którą stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje 11 wskazanych systemów. Ustawa ZK definiuje sytuację kryzysową jako sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków, a także definiuje pojęcie i zakres ochrony infrastruktury krytycznej, co należy rozumieć jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. Ustawa ZK ustanawia proces planowania cywilnego, którym jest całokształt przedsięwzięć organizacyjnych mających na celu przygotowanie administracji publicznej i Sił Zbrojnych RP do zarządzania kryzysowego. Planowanie cywilne jest realizowane w ramach cyklu planowania, tzn. okresowego realizowania etapów: analizowania, programowania, opracowywania planu lub programu, jego wdrażania, testowania i uruchamiania[198]. Zadania z zakresu planowania cywilnego obejmują przygotowanie planów zarządzania kryzysowego, przygotowanie struktur uruchamianych w sytuacjach kryzysowych, przygotowanie i utrzymywanie zasobów niezbędnych do wykonania zadań ujętych w planie zarządzania kryzysowego, utrzymywanie baz danych niezbędnych w procesie zarządzania kryzysowego, przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzanymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wykonania wynika z odrębnych przepisów.

Ustawa ZK ustanawia tworzenie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego (KPZK) oraz wojewódzkich, powiatowych i gminnych planów zarządzania kryzysowego (plany zarządzania kryzysowego). W skład planów zarządzania kryzysowego wchodzą plan główny, zespół przedsięwzięć na wypadek sytuacji kryzysowych i załączniki

[198] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 2, 3

funkcjonalne planu głównego. Ustawa ZK powołuje również, na mocy rozporządzenia, ustanowienie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Zadania z zakresu ochrony infrastruktury krytycznej obejmują[199]:

1) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
2) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
3) odtwarzanie infrastruktury krytycznej;
4) współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Ustawa ZK nakłada na właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej (operatorów infrastruktury krytycznej, OIK) obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia. Operatorzy infrastruktury krytycznej są zobowiązani do opracowania planów ochrony infrastruktury krytycznej, a ci będący jednocześnie operatorami usług kluczowych (OUK, w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa), uwzględniają w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych[200].

Przywołane Rozporządzenie w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Rozp. NPOIK) określa sposób realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej - operatorami infrastruktury krytycznej - oraz innymi organami i służbami publicznymi[201].

[199] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 5, 5b, 6
[200] tamże, art. 6,
[201] Rozporządzenie w sprawie NPOIK, wyd. cyt., par. 1

Przywołany powyżej Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) obejmuje infrastrukturę krytyczną (IK) umieszczoną w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. Nadrzędnym celem ochrony IK jest utrzymanie ciągłości świadczenia usług kluczowych dla państwa i nie może być ona traktowana jako wyłączna domena któregokolwiek z uczestników NPOIK. Operatorzy infrastruktury krytycznej mają najlepszą wiedzę i warunki do ograniczenia zagrożeń dla IK, zmniejszania jej podatności na te zagrożenia oraz wyboru najodpowiedniejszych strategii minimalizacji skutków tych zagrożeń, dlatego to im powierzony został obowiązek ochrony obiektów, urządzeń, instalacji i usług infrastruktury krytycznej. W związku z powyższym zobowiązani są oni do przygotowania i wdrażania, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia, wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej, niezwłoczne przekazywanie Szefowi Agencji Bezpieczeństwa Wewnętrznego, informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej oraz współpracy w tworzeniu i realizacji NPOIK[202].

NPOIK definiuje ochronę infrastruktury krytycznej jako proces zapewnienia jej bezpieczeństwa uwzględniający dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie, obejmujący znaczną liczbę obszarów zadaniowych i kompetencji, angażujący wiele zainteresowanych stron oraz obejmujący wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej. System ochrony IK powinien mieć zastosowanie do wszystkich typów zidentyfikowanych zagrożeń, tak naturalnych, jak i intencjonalnych oraz technicznych, a także być przygotowany do możliwie szybkiego przywrócenia funkcji realizowanych przez daną IK. Ponadto powinna cechować go kompleksowość i elastyczność oraz łatwość zastosowania i zrozumienia przez odpowiedzialnych za ochronę IK[203].

Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez zmniejszenie prawdopodobieństwa wystąpienia zagrożenia, zmniejszanie podatności lub minimalizowanie skutków wystąpienia zagrożenia. Na działania na rzecz zapewnienia bezpieczeństwa IK składają się[204]:

[202] NPOIK, wyd. cyt., s. 8, 15, 16
[203] tamże, s. 27
[204] tamże, s. 30

1) zapewnienie bezpieczeństwa fizycznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
6) plany ciągłości działania i odtwarzania – rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

W kręgu zainteresowania rozprawy są zagadnienia zapewnienia bezpieczeństwa teleinformatycznego infrastruktury krytycznej, stanowiącego aspekt cyberbezpieczeństwa państwa. Przywołany powyżej NPOIK Załącznik 1 - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej dobre praktyki i rekomendacje, definiuje zapewnienie bezpieczeństwa teleinformatycznego jako zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne, włączając w to akty szeroko rozumianej cyberprzestępczości i cyberterroryzmu a także przypadkowych (niecelowych) działań użytkowników. Dokument wskazuje standardy bezpieczeństwa teleinformatycznego możliwe do zastosowania przez operatorów infrastruktury krytycznej do ochrony systemów teleinformatycznych stanowiących i wspierających ich IK, takie jak: ISO/IEC 27002, IEC 62443/ISA 62443, NIST 800-82, NERC-CIP, TIA 942, ISO/IEC 24762 oraz standardy bezpieczeństwa opracowywane przez

ENISA[205]. Dokument wskazuje, że najistotniejszymi elementami zapewnienie bezpieczeństwa teleinformatycznego IK są współpraca sektorowa, plany awaryjne i ciągłości działania, bezpieczeństwo oprogramowania, kontrola dostępu, ochrona stacji roboczych, bezpieczeństwo sieci bezprzewodowych, monitoring zagrożeń i reakcja na incydenty[206].

Rozwiązania organizacyjne systemu cyberbezpieczeństwa zdefiniowane w przepisach prawnych systemu zarządzania kryzysowego (Ustawy ZK, wskazanych rozporządzeń i NPOIK), właściwe dla zakresu problemów badawczych niniejszej dysertacji zostaną przybliżone kontekstowo w kolejnych, dedykowanych poszczególnym problemom badawczym rozprawy jej rozdziałach: trzecim w odniesieniu do organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym, czwartym – w zakresie zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, piątym – odnośnie kwestii doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i szóstym – dotyczącym kwestii doboru wymaganych norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

2.6.3. System informatyzacji podmiotów publicznych

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[207] (Ustawa IPP) wraz z Rozporządzeniem w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[208] (Rozporządzenie KRI) stanowią dokumenty formalne ustanawiające i definiujące system informatyzacji podmiotów publicznych.

Ustawa IPP nie jest dokumentem bezpośrednio adresującym kwestie bezpieczeństwa państwa czy bezpieczeństwa teleinformatycznego, odnosi się jednak do kwestii informatyzacji podmiotów publicznych i definiuje wymagania bezpieczeństwa ich systemów telein-

[205] ENISA (ang. – European Agency for Network and Information Security) Europejska Agencja Bezpieczeństwa Sieci i Informacji, zajmująca się kwestiami bezpieczeństwa teleinformatycznego.
[206] NPOIK Załącznik 1, Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej dobre praktyki i rekomendacje, s. 67, 74, 75, 76
[207] Ustawa z dnia 17 lutego 2005 r. informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565 z późn. zmianami (Dz. U. z 2020 r. poz. 346, 568, 695 i 1517)
[208] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526 z późn. zmianami (Dz.U. 2017 poz. 2247) (Rozporządzenie KRI)

formatycznych. Ustawa IPP obejmuje m.in. kwestie ustalania i wdrażania minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi oraz Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji, wśród których są zagadnienia bezpieczeństwa tych systemów i przetwarzanych w nich danych w celu ochrony interesu publicznego, w tym zachowania przez Państwo możliwości swobody wyboru technologii w procesach informatyzacji realizacji zadań publicznych. Ustawa IPP wskazuje podmioty publiczne, do których ma zastosowanie oraz podmioty, do których jej zapisów się nie stosuje. Ustawa IPP zobowiązuje podmioty publiczne do używania do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność i bezpieczeństwo systemów na zasadach określonych w Krajowych Ramach Interoperacyjności (Rozporządzeniu KRI)[209].

Przywołane Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zobowiązuje podmioty realizujące zadania publiczne m.in. do stosowania rozwiązań z zakresu interoperacyjności na poziomie organizacyjnym, semantycznym i technologiczny. Interoperacyjność na poziomie technologicznym osiągana może być przez stosowanie określonych minimalnych wymagań dla systemów teleinformatycznych oraz stosowanie dedykowanych regulacji, a w przypadku ich braku uwzględnienia postanowień odpowiednich Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe. Rozporządzenie KRI wymaga, aby systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne były projektowane, wdrażane oraz eksploatowane z uwzględnieniem aspektów jakościowych - funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i ma odbywać się w oparciu o udokumentowane procedury. Powyższe wymagania uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, moni-

[209] Ustawa o informatyzacji, wyd. cyt., art. 13

torowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2. Rozporządzenie KRI stawia wymaganie, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Wymagania uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji zostanie opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem oraz PN-ISO/IEC 24762[210] – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania[211].

Rozwiązania organizacyjne systemu cyberbezpieczeństwa zdefiniowane w przepisach prawnych systemu informatyzacji podmiotów publicznych (Ustawy IPP, Rozporządzenia KRI), właściwe dla zakresu problemów badawczych niniejszej dysertacji zostaną przybliżone kontekstowo w kolejnych, dedykowanych poszczególnym problemom badawczym rozprawy jej rozdziałach: piątym – odnośnie kwestii doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i szóstym – dotyczącym kwestii doboru wymaganych norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

Regulacje prawne, a szczególnie regulacje systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych oraz dotyczące innych obszarów i dziedzin, nie poruszanych w rozprawie, kształtują polski system cyberbezpieczeństwa, definiując procesy zarządzania, nadając mu strukturę, relacje i odpowiedzialność. Ważnym jest, aby rozwiązania zdefiniowane w regulacjach prawnych były ze sobą spójne i powiązane, stanowiły jednorodny, zintegrowany system bezpieczeństwa i cyberbezpieczeństwa państwa.

[210] Norma wycofana, ale jej obowiązywanie w ramach przepisów Rozporządzenia KRI zostało utrzymane, gov.pl, iso.org [dostęp 30.10.2022]
[211] Rozporządzenie KRI, wyd. cyt., art. 5, 15, 20

2.7. Normy, standardy i metodyki bezpieczeństwa teleinformatycznego

Zapewnienie i zarządzanie bezpieczeństwem teleinformatycznym, czy też cyberbezpieczeństwem jest jedną z kluczowych i krytycznych zarazem kwestii dla podmiotów wszelkiego typu, zarówno publicznych, przemysłowych czy usługowych, dużych czy małych, będących operatorami infrastruktury krytycznej, operatorami usług krytycznych, dostawcami usług cyfrowych, prywatnych czy publicznych. To zagadnienie dotyczy każdego podmiotu w związku z zależnością ich działalności i realizowanych usług od systemów teleinformatycznych.

Rozwiązania bezpieczeństwa teleinformatycznego należy rozpatrywać w ujęciu szerszym niż tylko zabezpieczenia systemu teleinformatycznego i przetwarzanych w nim danych. Bezpieczeństwo informacji definiowane jest jako zachowanie poufności, integralności i dostępności informacji, a także takich aspektów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zapewnienie bezpieczeństwa informacji jest zależne od zapewnienia bezpieczeństwa systemu teleinformatycznego, uwzględniającego te same atrybuty bezpieczeństwa. Istotnym aspektem bezpieczeństwa jest zapewnienie jego ciągłości. Ciągłość bezpieczeństwa informacji (teleinformatycznego) to procesy i procedury zapewniające ciągłość bezpieczeństwa informacji (teleinformatycznego)[212].

Niektóre podmioty, ważne dla bezpieczeństwa sfery publiczno-społeczno-gospodarczej, są zobowiązane do wdrożenia rozwiązań bezpieczeństwa teleinformatycznego dedykowanymi przepisami prawa (co zostało wykazane w podrozdziale 2.6.) inne decydują się na podjęcie działań w tym zakresie z własnej inicjatywy i dla własnej ochrony. Niezależnie od motywacji, realizacja rozwiązań bezpieczeństwa teleinformatycznego jest dużym wyzwaniem dla każdego zainteresowanego podmiotu. Ogromną pomocą i niekwestionowanym wsparciem mogą być wszelkiego typu normy, metodyki i standardy zarządzania bezpieczeństwem teleinformatycznym i związanymi z tym zagadnieniami, oferujące metodyczne i systemowe podejście do tego zagadnienia. Warto zwrócić uwagę na rozwiązania ogólnoorganizacyjne, dedykowane podmiotom jako całym organizacjom lub ich zorganizowanym częściom, jak również na rozwiązania dedykowane organizacjom informatycznym, czy działom informatycznym i rozwiązania dedykowane stricte systemom teleinformatycznym, które w dobie znaczącej i dynamicznie postępującej informatyzacji działalności i uzależnienia or-

[212] PN-ISO/IEC-27000:2017 Technologia informacyjna – Techniki zabezpieczeń – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia

ganizacji od systemów teleinformatycznych mają szczególnie istotne znaczenie. Identyfikacja i rozpoznanie norm, metodyk i standardów dotyczących zarządzania bezpieczeństwem teleinformatycznym, stanowi ogromną, bazową wartość informacyjną w projektowaniu i wdrażaniu rozwiązań zarządzania bezpieczeństwem teleinformatycznym.

Przegląd metodyk, norm i standardów dotyczących zarządzania bezpieczeństwem teleinformatycznym zostanie przeprowadzony w odniesieniu do zagadnień:

- bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych oraz realizacji procesów związanych z zarządzaniem bezpieczeństwem teleinformatycznym;
- ciągłości działania systemów teleinformatycznych, usług zależnych od tych systemów, usług realizowanych przez te systemy, procesów związanych z zarządzaniem operacyjnym systemami teleinformatycznymi;
- dostępności usług systemów teleinformatycznych i realizacją procesów związanych z zarządzaniem operacyjnym systemami teleinformatycznymi.

2.7.1. Normy ISO bezpieczeństwa teleinformatycznego

Szczególną uwagę należy zwrócić na normy ISO, adresujące kwestie bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji, które dedykowane są do opracowywania i wdrażania systemów zarządzania bezpieczeństwem teleinformatycznym oraz implementowania rozwiązań zapewniających bezpieczeństwo teleinformatyczne. Normy te przynależą do grupy norm ISO 270xx. Zidentyfikowane normy obejmują zagadnienia zarządzania bezpieczeństwem informacji i systemów teleinformatycznych, ładu bezpieczeństwa informacji, ciągłości działania systemów teleinformatycznych, cyberbezpieczeństwa, bezpieczeństwa sieci, bezpieczeństwa aplikacji, zarządzania incydentami bezpieczeństwa, bezpieczeństwa składowanych danych, zarządzania ryzykiem bezpieczeństwa informacji. Zidentyfikowane normy bezpieczeństwa informacji i teleinformatycznego to m.in.:

1. ISO/IEC 27000 Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia,
2. ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji - Wymagania,
3. ISO/IEC 27002 Praktyczne zasady zabezpieczenia informacji,
4. ISO/IEC 27004 Information security management – Measurement,
5. ISO/IEC 27005 Information security risk management,
6. ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 – Requirements,

7. ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications,
8. ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002,
9. ISO/IEC 27014 Governance of information security,
10. ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services,
11. ISO/IEC 27018 Code of practice for protection of personally identifiable information (IIP) in public clouds acting as IPP processors,
12. ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry,
13. ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002,
14. ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity,
15. ISO/IEC 27032:2012 Guidelines for cybersecurity,
16. ISO/IEC 27033 Network security,
17. ISO/IEC 27034 Application security,
18. ISO/IEC 27035 Information security incident management,
19. ISO/IEC 27036 Information security in relations with suppliers,
20. PN-EN ISO/IEC 27037 Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych,
21. ISO/IEC 27040 Storage security.

Grupa norm z serii ISO 270xx jest znacznie szersza, obejmująca również normy adresujące specjalistyczne aspekty bezpieczeństwa teleinformatycznego, niemniej ich lista nie będzie już rozwijana w rozprawie. Omówione po krótce zostaną wybrane normy z wyżej wyszczególnionych.

ISO/IEC 27000 zawiera przegląd systemów zarządzania bezpieczeństwem informacji (SZBI). Zawiera również terminy i definicje powszechnie stosowane w rodzinie standardów SZBI. Dokument dotyczy wszystkich typów i rozmiarów organizacji (np. przedsiębiorstw handlowych, agencji rządowych, organizacji non-profit)[213].

[213] PN-ISO/IEC 27000 Technologia informacyjna – Techniki zabezpieczeń – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia

ISO/IEC 27001 określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji, z uwzględnieniem uwarunkowań, w których działa organizacja. Podano również dostosowane do potrzeb organizacji wymagania, dotyczące szacowania i postępowania z ryzykami w bezpieczeństwie informacji. System zarządzania bezpieczeństwem informacji zapewnia zachowanie poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem i dostarcza zainteresowanym stronom zaufania, że ryzyka są odpowiednio zarządzane. Wymagania mają charakter ogólny i są przeznaczone do stosowania w organizacji każdego rodzaju, wielkości czy charakteru[214].

ISO/IEC 27002 zawiera wytyczne dotyczące standardów bezpieczeństwa informacji organizacji i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrażania i zarządzania kontrolami (zabezpieczeniami) z uwzględnieniem środowiska (-ów) bezpieczeństwa informacji organizacji. Jest przeznaczona do użytku przez organizacje, które zamierzają wybrać zabezpieczenia w ramach procesu wdrażania Systemu Zarządzania Bezpieczeństwem Informacji opartego na ISO/IEC 27001 albo wdrożyć powszechnie akceptowane zabezpieczenia bezpieczeństwa informacji lub opracować własne wytyczne dotyczące zarządzania bezpieczeństwem informacji. Norma jest również przeznaczona do stosowania w ramach rozwoju branżowych i specyficznych dla organizacji wytycznych dotyczących zarządzania bezpieczeństwem informacji, z uwzględnieniem środowiska ryzyka, w którym występują specyficzne ryzyka w bezpieczeństwie informacji[215].

ISO/IEC 27005 zawiera wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji, rozwija ogólne koncepcje określone w ISO/IEC 27001. Opracowano ją w celu wsparcia satysfakcjonującego wdrożenia podejścia do bezpieczeństwa opartego na zarządzaniu ryzykiem. Dla zrozumienia normy ISO/IEC 27005 istotna jest znajomość koncepcji, modeli, procesów i terminologii podanych w ISO/IEC 27001 oraz ISO/IEC 27002. Norma ISO 27005 ma zastosowanie do wszystkich typów organizacji (np. przedsiębiorstw, instytucji rządowych, organizacji non-profit), które zamierzają zarządzać ryzykami, mogącymi spowodować naruszenie bezpieczeństwa informacji w tych organizacjach[216].

ISO/IEC 27010 zawiera wytyczne dotyczące wdrażania zarządzania bezpieczeństwem informacji w środowisku społeczeństwa informacyjnego i wymiany informacji, roz-

[214] PN-ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji - Wymagania
[215] PN-ISO/IEC 27002 Praktyczne zasady zabezpieczenia informacji
[216] ISO/IEC 27005 Information security risk management

szerzone względem wskazówek podanych w rodzinie norm ISO / IEC 27000. Norma ta zapewnia zabezpieczenia i wskazówki dotyczące w szczególności inicjowania, wdrażania, utrzymywania i poprawy bezpieczeństwa informacji w komunikacji między organizacjami i między sektorami. Zawiera wytyczne i ogólne zasady dotyczące sposobu spełnienia określonych wymagań przy użyciu ustalonych komunikatów i innych metod technicznych. Norma ma zastosowanie do wszystkich form wymiany i udostępniania poufnych informacji, zarówno publicznych, jak i prywatnych, na szczeblu krajowym i międzynarodowym, w tej samej branży lub sektorze rynku lub między sektorami. W szczególności może mieć zastosowanie do wymiany informacji i dzielenia się nimi w związku z dostarczaniem, utrzymaniem i ochroną krytycznej infrastruktury organizacji lub państwa narodowego. Została zaprojektowana, aby wspierać tworzenie zaufania podczas wymiany i udostępniania poufnych informacji, tym samym wspierając międzynarodowy rozwój społeczeństwa informacyjnego i wymiany informacji[217].

ISO/IEC 27011 ma na celu określenie wytycznych wspierających wdrażanie kontroli (zabezpieczeń) bezpieczeństwa informacji w organizacjach telekomunikacyjnych, umożliwia organizacjom telekomunikacyjnym spełnienie podstawowych wymagań w zakresie zarządzania bezpieczeństwem informacji, takich jak poufność, integralność, dostępność i wszelkich innych istotnych zabezpieczeń[218].

ISO/IEC 27014 zawiera koncepcje i wskazówki dotyczące zasad i procesów zarządzania bezpieczeństwem informacji, dzięki którym organizacje mogą oceniać, kierować i monitorować zarządzanie bezpieczeństwem informacji. Niniejsza norma międzynarodowa ma zastosowanie do wszystkich typów i rozmiarów organizacji[219].

ISO/IEC 27017 zawiera wytyczne dotyczące kontroli (zabezpieczeń) bezpieczeństwa informacji mających zastosowanie do świadczenia i korzystania z usług w chmurze, zapewniając dodatkowe wytyczne dotyczące wdrażania odpowiednich kontroli określonych w ISO/IEC 27002 oraz dodatkowe kontrole wraz z wytycznymi dotyczącymi wdrażania, które odnoszą się konkretnie do usług w chmurze. Norma zapewnia zabezpieczenia i wskazówki dotyczące wdrażania bezpieczeństwa, zarówno dla dostawców, jak i klientów usług w chmurze[220].

---

[217] ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications
[218] ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
[219] ISO/IEC 27014 Governance of information security
[220] ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018 ustanawia powszechnie uznawane cele stosowania zabezpieczeń, zabezpieczenia oraz wytyczne do wdrażania środków ochrony danych identyfikujących osobę (ang. PII - Personally Identifiable Information), zgodnie z pryncypiami zdefiniowanymi w normie ISO/IEC 29100, dla środowiska przetwarzania w chmurze. Wytyczne zawarte w normie zostały zaprezentowane w układzie normy ISO/IEC 27002, przy uwzględnieniu wymagań regulacyjnych odnoszących się do ochrony danych identyfikujących osobę, które mogą mieć zastosowanie w kontekście środowisk ryzyka związanego z bezpieczeństwem informacji u dostawcy usługi chmury publicznej. Norma ma zastosowanie dla organizacji wszystkich typów i wielkości, w tym podmiotów publicznych i prywatnych, jednostek administracji państwowej oraz organizacji typu non-profit, które świadczą na rzecz innych organizacji usługi przetwarzania informacji w formie przetwarzania w chmurze, zgodnie z zawartą umową na świadczenie usług. Wytyczne normy mogą mieć również odniesienie do organizacji działających jako administratorzy danych osobowych, jednakże mogą oni podlegać dodatkowym przepisom, regulacjom i obowiązkom związanym z ochroną danych osobowych, które nie mają zastosowania do postanowień normy[221].

ISO/IEC 27019 zawiera wytyczne oparte na normie ISO/IEC 27002 stosowane do systemów sterowania procesami wykorzystywanymi przez przemysł energetyczny do kontrolowania i monitorowania produkcji, wytwarzania, przesyłu, przechowywania i dystrybucji energii elektrycznej, gazu, oleju i ciepła oraz do kontroli powiązanych procesów wspierających. Norma zawiera również wymóg dostosowania oceny ryzyka i procesów przetwarzania opisanych w normie ISO/IEC 27001 do szczegółowych wytycznych sektora energetycznego[222].

ISO/IEC 27031 opisuje koncepcje i zasady gotowości informacji i technologii informacyjno-komunikacyjnych (TIK, ang. ICT) do ciągłości biznesowej oraz zapewnia ramy metod i procesów do identyfikacji i określenia wszystkich aspektów (takich jak kryteria wydajności, projekt i wdrożenie) dla poprawy gotowości ICT organizacji do zapewnienia ciągłości biznesowej. Dotyczy każdej organizacji (prywatnej, rządowej i pozarządowej, niezależnie od wielkości) rozwijającej gotowość jej systemów teleinformatycznych do ciągłości działalności i wymagającej, aby jej usługi i infrastruktura teleinformatyczna były gotowe do wspierania operacji biznesowych w przypadku pojawienia się zdarzenia i incydentu oraz

[221] ISO/IEC 27018 Code of practice for protection of personally identifiable information (IIP) in public clouds acting as IPP processors
[222] ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

związanych z nimi zakłóceń, które mogą mieć wpływ na ciągłość (w tym bezpieczeństwo) krytycznych funkcji biznesowych. Zakres normy obejmuje wszystkie zdarzenia i incydenty (w tym związane z bezpieczeństwem), które mogą mieć wpływ na infrastrukturę i systemy teleinformatyczne. Obejmuje i rozszerza praktyki zarządzania incydentami bezpieczeństwa informacji oraz planowania usług w zakresie gotowości ICT[223].

ISO/IEC 27032 zawiera wskazówki dotyczące poprawy stanu bezpieczeństwa cybernetycznego, wyciągania unikalnych aspektów tej działalności i jej zależności od innych domen bezpieczeństwa, w szczególności: bezpieczeństwa informacji, bezpieczeństwa sieci, bezpieczeństwa internetowego i bezpieczeństwo krytycznej infrastruktury informatycznej. Obejmuje podstawowe zasady bezpieczeństwa dla interesariuszy w cyberprzestrzeni. Norma zapewnia przegląd cyberbezpieczeństwa, wyjaśnienie związku między cyberbezpieczeństwem a innymi rodzajami bezpieczeństwa, definicję interesariuszy i opis ich ról w cyberbezpieczeństwie, wskazówki dotyczące rozwiązywania wspólnych problemów związanych z bezpieczeństwem cybernetycznym oraz ramy umożliwiające interesariuszom współpracę w rozwiązywaniu problemów związanych z bezpieczeństwem cybernetycznym[224].

ISO/IEC 27033 jest rodziną norm adresujących kwestie bezpieczeństwa sieci. Na rodzinę norm 27033 składa się sześć części: część 1: Przegląd i pojęcia, część 2: Wytyczne dotyczące projektowania i wdrażania bezpieczeństwa sieci, część 3: Referencyjne scenariusze sieciowe - Zagrożenia, techniki projektowania i kwestie kontroli, część 4: Zabezpieczanie komunikacji między sieciami przy użyciu bram bezpieczeństwa - Zagrożenia, techniki projektowania i kwestie kontroli, część 5: Zabezpieczanie wirtualnych sieci prywatnych - Zagrożenia, techniki projektowania i kwestie kontroli, część 6: Zabezpieczanie dostępu do bezprzewodowej sieci IP[225]. ISO/IEC 27033-1 zawiera przegląd bezpieczeństwa sieci i powiązanych definicji. Definiuje i opisuje pojęcia związane z bezpieczeństwem sieci i zapewnia wskazówki dotyczące zarządzania. Bezpieczeństwo sieci dotyczy bezpieczeństwa urządzeń, bezpieczeństwa działań związanych z zarządzaniem urządzeniami, aplikacjami, usługami i użytkownikami końcowymi, a także bezpieczeństwa informacji przesyłanych przez łącza komunikacyjne[226]. ISO/IEC 27033-2 zawiera wytyczne dla organizacji dotyczące planowania, projektowania, wdrażania i dokumentowania bezpieczeństwa sieci[227]. ISO/IEC 27033-3 opisuje zagrożenia, techniki projektowania i problemy

[223] ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity
[224] ISO/IEC 27032:2012 Guidelines for cybersecurity
[225] ISO/IEC 27033-1 Network security, Overview and concepts
[226] ISO / IEC 27033-1 Overview and concepts
[227] ISO / IEC 27033-2 Guidelines for the design and implementation of network security

związane z kontrolą sieci dotyczącą scenariuszy odniesienia. Dla każdego scenariusza zawiera szczegółowe wskazówki dotyczące zagrożeń bezpieczeństwa i technik projektowania zabezpieczeń oraz mechanizmów kontrolnych wymaganych do ograniczenia związanego z tym ryzyka[228]. ISO/IEC 27033-4 zawiera wskazówki dotyczące zabezpieczania komunikacji między sieciami przy użyciu bram bezpieczeństwa (zapora ogniowa, zapora sieciowa aplikacji, system ochrony przed intruzami itp.)[229]. ISO/IEC 27033-5 zawiera wytyczne dotyczące wyboru, wdrażania i monitorowania technicznych kontroli niezbędnych do zapewnienia bezpieczeństwa sieci przy użyciu połączeń wirtualnej sieci prywatnej (VPN) do łączenia sieci i łączenia zdalnych użytkowników z sieciami[230]. ISO/IEC 27033-6 opisuje zagrożenia, wymagania bezpieczeństwa, kontrolę bezpieczeństwa i techniki projektowania związane z sieciami bezprzewodowymi. Zawiera wytyczne dotyczące wyboru, wdrażania i monitorowania kontroli technicznych niezbędnych do zapewnienia bezpiecznej komunikacji przy użyciu sieci bezprzewodowych[231].

ISO/IEC 27034 jest rodziną norm adresujących kwestie bezpieczeństwa aplikacji. Na rodzinę norm 27034 składa się siedem części: część 1: Przegląd i pojęcia, część 2: Ramy normatywne organizacji, część 3: Proces zarządzania bezpieczeństwem aplikacji, część 4: Sprawdzanie bezpieczeństwa aplikacji, część 5: Protokoły i struktura danych kontroli bezpieczeństwa aplikacji, część 6: Studia przypadków, część 7: Ramy prognozowania pewności[232]. ISO/IEC 27034-1 przedstawia przegląd bezpieczeństwa aplikacji. Wprowadza definicje, koncepcje, zasady i procesy związane z bezpieczeństwem aplikacji. Zawiera wskazówki, które mają pomóc organizacjom w integracji zabezpieczeń w procesach wykorzystywanych do zarządzania ich aplikacjami. Norma ma zastosowanie do opracowanych aplikacji wewnętrznych, aplikacji nabytych od stron trzecich i tam, gdzie rozwój lub działanie aplikacji jest zlecane na zewnątrz[233]. ISO/IEC 27034-2 zawiera szczegółowy opis ram normatywnych organizacji i zawiera wytyczne dla organizacji dotyczące ich wdrożenia[234]. ISO/IEC 27034-3 zawiera szczegółowy opis i wskazówki dotyczące wdrażania procesu zarządzania bezpieczeństwem aplikacji[235]. ISO/IEC 27034-5 nakreśla i wyjaśnia minimalny zestaw podstawowych atrybutów kontroli bezpieczeństwa aplikacji (ASC) i wyszczególnia

[228] ISO/IEC 27033-3 Reference network scenarios — Threats, design techniques and control issues
[229] ISO/IEC 27033-4 Securing communications between networks using security gateways — Risks, design techniques and control issues
[230] ISO/IEC 27033-5 Securing virtual private networks — Risks, design techniques and control issues
[231] ISO/IEC 27033-6 Securing access to IP wireless network
[232] ISO/IEC 27034-1 Application security Overview and concepts
[233] ISO/IEC 27034-1 Overview and concepts
[234] ISO/IEC 27034-2 Organization normative Framework
[235] ISO/IEC 27034-3 Application security management process

działania i role modelu referencyjnego cyklu życia bezpieczeństwa aplikacji[236]. ISO/IEC 27034-6 podaje przykłady użycia ASC dla określonych zastosowań[237]. ISO/IEC 27034-7 opisuje minimalne wymagania, gdy wymagane działania określone przez kontrolę bezpieczeństwa aplikacji (ASC) są zastępowane przez uzasadnienie przewidywanego bezpieczeństwa aplikacji (PASR). ASC zmapowane do PASR określają oczekiwany poziom zaufania dla kolejnej aplikacji[238].

ISO/IEC 27035 jest rodziną norm adresujących kwestie zarządzania incydentami bezpieczeństwa. Na rodzinę norm 27035 składa się trzy części: część 1: Zasady zarządzania incydentami, część 2: Wytyczne dotyczące planowania i przygotowania do reakcji na incydenty, część 3: Wytyczne dotyczące operacji reagowania na incydenty[239]. ISO/IEC 27035-1 przedstawia podstawowe pojęcia i fazy zarządzania incydentami bezpieczeństwa informacji i łączy te koncepcje z zasadami w ustrukturyzowanym podejściu do wykrywania, raportowania, oceny i reagowania na incydenty oraz stosowania zdobytych doświadczeń[240]. ISO/IEC 27035-2 zawiera wytyczne dotyczące planowania i przygotowania do reakcji na incydenty. Wytyczne opierają się na fazie „Planuj i przygotuj" oraz fazie „Wnioski" w modelu „Fazy zarządzania incydentem bezpieczeństwa informacji" przedstawionym w ISO/IEC 27035-1[241]. ISO/IEC 27035-3 zawiera wytyczne reagowania na incydenty bezpieczeństwa informacji w operacjach związanych z bezpieczeństwem teleinformatycznym, w tym wykrywaniu incydentów związanych z bezpieczeństwem informacji, zgłaszaniu, selekcji, analizie, reagowaniu, powstrzymywaniu, eliminowaniu, odzyskiwaniu i wyciąganiu wniosków[242].

ISO/IEC 27036 jest rodziną norm adresujących kwestie bezpieczeństwa informacji w relacjach z dostawcami. Na rodzinę norm 27036 składa się cztery części: część 1: Przegląd i koncepcje, część 2: Wymagania, część 3: Wytyczne dotyczące bezpieczeństwa łańcucha dostaw technologii informacyjnych i komunikacyjnych, część 4: Wytyczne dotyczące bezpieczeństwa usług w chmurze[243]. ISO/IEC 27036-1 jest wprowadzającą częścią rodziny norm, zawiera przegląd wytycznych i koncepcje mające pomóc organizacjom w zabezpie-

[236] ISO/IEC 27034-5 Protocols and application security control data structure
[237] ISO/IEC 27034-6 Usecases
[238] ISO/IEC 27034-7 Certainty forecasting framework
[239] ISO/IEC 27035-1 Information security incident management, Principles of incident management
[240] ISO/IEC 27035-1 Principles of incident management
[241] ISO/IEC 27035-2 Guidelines to plan and prepare for incident response
[242] ISO/IEC 27035-3 Guidelines for ICT incident response operations
[243] ISO/IEC 27036-1 Information security in relations with suppliers, Overview and concepts

czeniu ich systemów informacyjnych i teleinformatycznych w kontekście relacji z dostawcami. Norma dotyczy perspektyw zarówno nabywców, jak i dostawców[244]. ISO/IEC 27036-2 określa podstawowe wymogi bezpieczeństwa informacji dotyczące definiowania, wdrażania, obsługi, monitorowania, przeglądu, utrzymywania i ulepszania relacji dostawców i nabywców. Wymagania te obejmują wszelkie zamówienia i dostawy produktów i usług, takie jak produkcja lub montaż, zamówienia procesów biznesowych, komponenty oprogramowania i sprzętu, nabywanie procesów wiedzy i usługi w chmurze. Wymagania te można stosować do wszystkich organizacji, bez względu na ich rodzaj, wielkość i charakter[245]. ISO/IEC 27036-3 zapewnia nabywcom produktów i usług oraz dostawcom w łańcuchu dostaw technologii informacyjnych i komunikacyjnych (TIK) wskazówki dotyczące zarządzania zagrożeniami bezpieczeństwa informacji powodowanymi przez fizycznie rozproszone i wielowarstwowe łańcuchy dostaw, reagowania na zagrożenia wynikające z globalnego łańcucha dostaw, integracji procesów i praktyk bezpieczeństwa informacji z procesami cyklu życia systemu i oprogramowania[246]. ISO/IEC 27036-4 zapewnia klientom usług w chmurze i dostawcom usług w chmurze wskazówki dotyczące uzyskania wglądu w zagrożenia bezpieczeństwa informacji związane z korzystaniem z usług w chmurze i skutecznego zarządzanie tymi zagrożeniami oraz reagowania na ryzyka specyficzne dla nabycia lub świadczenia usług w chmurze, które mogą mieć wpływ na bezpieczeństwo informacji w organizacjach korzystających z tych usług[247].

ISO/IEC 27037 Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych zawiera wytyczne do specyficznych działań w ramach postępowania z cyfrowymi śladami dowodowymi. Do tych działań należą: identyfikacja, gromadzenie, pozyskiwanie i utrwalanie cyfrowych śladów dowodowych, które mogą mieć wartość dowodową. Norma zawiera wskazówki dla osób fizycznych w odniesieniu do typowych sytuacji spotykanych w całym procesie postępowania z cyfrowymi śladami dowodowymi i pomaga organizacjom w ich procedurach dyscyplinarnych i w ułatwianiu wymiany potencjalnych cyfrowych śladów dowodowych pomiędzy różnymi systemami prawnymi[248].

ISO/IEC 27040 zawiera przegląd koncepcji bezpieczeństwa pamięci masowej i związanych z nimi definicji. Zawiera wskazówki dotyczące zagrożeń, projektowania

[244] ISO/IEC 27036-1 Overview and concepts
[245] ISO/IEC 27036-2 Requirements
[246] ISO/IEC 27036-3 Information and Communication Technology Supply Chain Security Guidelines
[247] ISO/IEC 27036-4 Cloud service security guidelines
[248] PN-EN ISO/IEC 27037 Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych

i aspektów kontroli związanych z typowymi scenariuszami przechowywania i obszarami technologii pamięci masowej. Ponadto zawiera odniesienia do innych międzynarodowych norm i raportów technicznych, które dotyczą istniejących praktyk i technik, które można zastosować do bezpieczeństwa pamięci masowej. Norma zawiera szczegółowe wskazówki techniczne dotyczące sposobu, w jaki organizacje mogą zdefiniować odpowiedni poziom ograniczania ryzyka poprzez zastosowanie sprawdzonego i spójnego podejścia do planowania, projektowania, dokumentacji i wdrażania bezpieczeństwa przechowywania danych[249].

2.7.2. Normy i metodyki zarządzania usługami i procesami systemów teleinformatycznych

Wśród norm, metodyk i standardów dotyczących zarządzania organizacją informatyczną (podmiot lub komórka organizacyjna) oraz usługami i procesami systemów teleinformatycznych można wyróżnić normę międzynarodową ISO i metodykę zarządczą:

- ISO 20000 – Technika informatyczna – Zarządzanie usługami - Wymagania dotyczące systemu zarządzania usługami (System zarządzania usługami IT);
- ITIL - Zarządzanie usługami IT.

Norma ISO 20000 odnosi się do zarządzania jakością, a właściwie poziomem usług, który powszechnie odczytywany jest jako dostępność usług IT. Atrybut dostępności usług - systemów IT i przetwarzanych w nich danych – jest traktowany jako jeden z aspektów ciągłości działania i bezpieczeństwa. Norma ISO 20000-1 została przygotowana w celu określenia wymagań dotyczących ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia systemu zarządzania usługami (SZU (ang. Service Management System, SMS)). System zarządzania usługami obsługuje zarządzanie cyklem życia usługi, w tym planowanie, projektowanie, przenoszenie, dostarczanie i ulepszanie usług, które spełniają uzgodnione wymagania i zapewniają wartość dla klientów, użytkowników i organizacji dostarczającej usługi. Wdrożenie SZU jest decyzją strategiczną dla organizacji i zależy od celów organizacji, organu zarządzającego, innych stron zaangażowanych w cykl życia usługi oraz potrzeby skutecznych i odpornych usług. Wdrożenie i działanie SZU zapewnia ciągłą widoczność, nadzór usług i ciągłe doskonalenie, co prowadzi do większej skuteczności i wydajności. Norma ISO/IEC 20000 Information technology — Service management jest rodziną norm

[249] PN-EN ISO/IEC 27040: 2016-12 Bezpieczeństwo pamięci masowych

składającą się z dwunastu części: część 1: Wymagania dotyczące systemu zarządzania usługami, część 2: Wytyczne dotyczące stosowania systemów zarządzania usługami, część 3: Wytyczne dotyczące definicji zakresu i stosowalności normy ISO/IEC 20000-1, część 4: Model referencyjny procesu, część 5: Przykładowy plan wdrożenia normy ISO/IEC 20000-1, część 6: Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania usługami, część 8: Wytyczne dotyczące stosowania systemów zarządzania usługami dla mniejszych organizacji, część 9: Wytyczne dotyczące zastosowania normy ISO/IEC 20000 1 w chmurze, część 10: Pojęcia i terminologia, część 11: Wytyczne dotyczące relacji między ISO/IEC20000 1:2011 a ramami zarządzania usługami ITIL, część 12: Wytyczne dotyczące relacji pomiędzy ISO/IEC 20000–1:2011 a ramami zarządzania usługami: CMMI-SVC®2)[250]. Pozostałe części normy, inne niż 20000-1, nie będą omawiane w niniejszej rozprawie.

ITIL jest metodyką zarządzania usługami informatycznymi w ujęciu jakościowym, w którym należy zwrócić uwagę na aspekt dostępności systemów IT i ich usług, jako aspektu bezpieczeństwa i ciągłości działania. ITIL w ujęciu zakresowym jest pokrewny normie ISO 20000, definiującej system zarządzania usługami IT. ITIL dostarcza wytycznych i najlepszych praktyk zarządczych. ITIL 4 (najnowsza wersja metodyki) dostosowuje większość istniejących praktyk ITSM (Information Technology Service Management) do szerszego kontekstu bazującego na doświadczeniu klienta (ang. Customer experience), strumieniu wartości (ang. Value streams) oraz cyfrowej transformacji (ang. Digital transformation), wykorzystując w tym doświadczenia Lean, Agile oraz DevOps. ITIL 4 wskazuje organizacjom wytyczne pozwalające sprostać obecnym wyzwaniom zarządzania usługami i wykorzystać w tym celu potencjał nowych technologii informatycznych. Został zaprojektowany, żeby zapewnić elastyczny, skoordynowany, zintegrowany oraz skuteczny system nadzoru oraz zarządzania usługami IT. System zarządzania usługami ITIL 4 składa się z pięciu podstawowych elementów: łańcuch wartości usług ITIL, 7 zasad przewodnich ITIL, 34 praktyki ITIL, zarządzanie, ciągłe doskonalenie. ITIL 4 wykorzystuje 34 praktyki zarządzania, które są podzielone na trzy obszary: ogólne praktyki zarządzania, praktyki zarządzania usługami i praktyki zarządzania technicznego[251].

[250] ISO/IEC 20000-1:2018 - Information technology - Service management - Part 1: Service management system requirements, s. vii
[251] https://www.axelos.com/best-practice-solutions/itil [dostęp 20.05.2021]

2.7.3. Normy NIST i metodyki cyberbezpieczeństwa

Wśród norm i metodyk i standardów dotyczących zarządzania bezpieczeństwem informacji, systemów teleinformatycznych i cyberbezpieczeństwem, poza normami ISO, warto zwrócić uwagę i wyróżnić amerykańskie normy NIST[252] i brytyjską metodykę zarządczą:

- Resilia;
- NIST.

Resilia jest metodyką zarządczą obszaru cyberbezpieczeństwa. Ma pomóc organizacjom komercyjnym i publicznym w zapobieganiu, wykrywaniu i korygowaniu wpływu cyberataków na informacje potrzebne do prowadzenia działalności. W modelu Resilii aktywną cyberodporność osiąga się dzięki ludziom, procesom i technologii[253]. Resilia została zaprojektowana w celu uzupełnienia istniejących standardów i ram cyberodporności, takich jak ISO 27001, poprzez dostarczenie wskazówek dotyczących tego, w jaki sposób ich kontrole (zabezpieczenia) mogą być odpowiednio wybierane, wdrażane i zarządzane. Resilia obejmuje 29 podkategorii opartych na pięciu etapach cyberodporności: strategia dotycząca odporności cybernetycznej, projektowanie odporności cybernetycznej, przejście na cyberodporność, operacje dotyczące odporności cybernetycznej, ciągłe doskonalenie odporności cybernetycznej[254]. Resilia jest oparta na 4 elementach: 1. zarządzaj i chroń, 2. zidentyfikuj i wykryj, 3. odpowiedz i odzyskaj, 4. zarządzaj i zapewniaj. Etap zarządzaj i chroń - obejmuje identyfikowanie, ocenę i zarządzanie ryzykiem związanym z siecią i systemami informatycznymi, w tym w całym łańcuchu dostaw, ochronę informacji i systemów przed cyberatakami, awariami systemów i nieautoryzowanym dostępem. Etap zidentyfikuj i wykryj - zwiera ciągłe monitorowanie sieci i systemów informatycznych w celu wykrywania anomalii i potencjalnych incydentów cyberbezpieczeństwa zanim spowodują one jakiekolwiek znaczące szkody. Etap odpowiedz i odzyskaj – obejmuje wdrożenie programu zarządzania reagowaniem na incydenty i środków zapewniających ciągłość biznesową - kontynuację działalności i jak najszybszy i efektywny powrót do normalnej pracy. Etap zarządzaj i zapewniaj – to upewnienie się, że program jest nadzorowany od góry organizacji i wbudowany

[252] NIST – National Institute of Standards and Technology (Narodowy Instytut Norm i Techniki), amerykańska agencja federalna pełniąca funkcję analogiczną do Głównego Urzędu Miar
[253] https://www.axelos.com/resilia [dostęp 20.05.2021]
[254] https://www.itgovernanceusa.com/resilia [dostęp 20.05.2021]

w normalny biznes. Z biegiem czasu system powinien coraz bardziej dopasowywać się do zmieniających się celów biznesowych[255].

NIST (National Institute of Standards and Technology) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informatycznych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami. NIST stale współpracuje z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów. Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem. Biorąc pod uwagę wszystkie powyższe aspekty, opracowania NIST można traktować jako godne zaufania i rekomendowane do ich stosowania przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania[256].

Normy NIST z zakresu cyberbezpieczeństwa to m.in.[257]:

1. FIPS PUB 199 Standardy Kategoryzacji Bezpieczeństwa,
2. FIPS PUB 200 Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych,
3. NIST SP 800-18 rev. 1 Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych,

[255] tamże
[256] Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0), KPRM, 2021, s. 5
[257] https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber [dostęp 20.09.2022]

4. NIST SP 800-30 rev. 1 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne,
5. NIST SP 800-37, Rev. 2 Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu,
6. NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View (March 2011) Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego,
7. NIST SP 800-46 rev. 2 Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD),
8. NIST SP 800-53, Rev. 5 Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji,
9. NIST SP 800-53B Zabezpieczenia bazowe systemów informatycznych oraz organizacji,
10. NIST SP 800-60 vol. 1, Rev. 1, vol. 2, Rev. 1 Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego,
11. NSC 800-61, Rev. 2 Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego,
12. NIST SP 800-207Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania".

Na podstawie standardów amerykańskiego National Institute of Science and Technology (NIST) zostały opracowane polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) oraz przyporządkowane obowiązującym w polskim systemie prawnym normom stosowanym w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych. NSC to przewodniki metodyczne, które mają ułatwić budowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w administracji federalnej USA[258].

Wyżej wymienione normy NIST nie będą omawiane szczegółowo w tym podrozdziale. Zostały one zaprezentowane w ramach omówienia Narodowych Standardów Cyberbezpieczeństwa (NSC), które wprost implementują normy NIST, w kolejnym podrozdziale rozprawy.

[258] tamże

2.7.4. Narodowe Standardy Cyberbezpieczeństwa

Narodowe Standardy Cyberbezpieczeństwa (NSC) to polskie dokumenty standaryzacyjne w zakresie cyberbezpieczeństwa, zostały opracowane w KPRM w 2021 r. i przyjęte przez Pełnomocnika Rządu ds. Cyberbezpieczenstwa. NSC zostały opracowane na bazie norm NIST i są ich bezpośrednim odpowiednikiem, tłumaczeniem i adaptacją do statusu formalnych dokumentów rządowych przeznaczonych do stosowania przez operatorów usług kluczowych krajowego systemu cyberbezpieczeństwa i administracje publiczną.

Narodowe Standardy Cyberbezpieczeństwa (NSC) to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. NSC zostały opracowane na podstawie standardów amerykańskiego National Institute of Science and Technology (NIST) oraz przyporządkowane obowiązującym w polskim systemie prawnym normom stosowanym w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych. Na standardy składają się następujące opracowania[259]:

1. Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0),
2. Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0),
3. Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0),
4. Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne (NSC 800-30 wer. 1.0),
5. Poradnik Planowania Awaryjnego (NSC 800-34 wer. 1.0),
6. Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0),
7. Zarządzanie ryzykiem bezpieczeństwa informacji (NSC 800-39 wer. 1.0),
8. Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0),
9. Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0),
10. Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0),

[259] tamże

11. Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0),
12. Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0),
13. Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część II (NSC 800-60 cz. 2 wer. 1.0),
14. Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer.1.0),
15. Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0),
16. Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (NSC 7298 wer. 1.0),
17. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych.

Dokument Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0) ma zastosowanie do wszelkich informacji, które organizacja uzna za informacje wrażliwe, wymagających ochrony przed nieupoważnionym dostępem oraz wszelkich systemów informatycznych przetwarzających informacje jawne na szczeblu państwowym, samorządowym i przez przedsiębiorców będących operatorami usług kluczowych lub operatorami infrastruktury krytycznej. Osoby odpowiedzialne w każdej jednostce organizacyjnej są zobowiązane do wykorzystywania kategoryzacji bezpieczeństwa opisanych w publikacji NSC 199 zawsze, gdy występuje wymóg zapewnienia takiej kategoryzacji informacji lub systemów informatycznych. Dopuszczalne jest opracowanie i wykorzystywanie dodatkowych oznaczeń bezpieczeństwa według uznania właściciela systemu teleinformatycznego. Instytucje państwowe, a także organizacje sektora prywatnego, obejmujące infrastrukturę krytyczną Rzeczpospolitej Polskiej, mogą rozważyć stosowanie tych standardów. Dokument Standardy kategoryzacji bezpieczeństwa opracowany został na podstawie specjalnej publikacji NIST FIPS PUB 199[260].

Dokument Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0) określa opracowane standardy w zakresie: kategoryzacji bezpieczeństwa informacji i systemów informatycznych w oparciu

[260] Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0), KPRM, 2021, s. 7, 10

o cele zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w zależności od zakresu poziomów ryzyka oraz minimalnych wymagań bezpieczeństwa dla informacji i systemów informatycznych w każdej z tych kategorii. Niniejszy standard dotyczy specyfikacji minimalnych wymagań bezpieczeństwa informacji i systemów informatycznych w sektorze publicznym. Określa minimalne wymagania bezpieczeństwa systemów informatycznych w siedemnastu obszarach związanych z bezpieczeństwem. Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w niniejszym dokumencie poprzez stosowanie środków bezpieczeństwa zgodnie ze standardem NSC 800-53. Dokument Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych został opracowany na podstawie specjalnej publikacji NIST FIPS PUB 200[261].

Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0) zawiera wytyczne dla podmiotów publicznych dotyczące opracowywania planów bezpieczeństwa systemu dla publicznych systemów informatycznych. Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych został opracowany na podstawie specjalnej publikacji NIST SP 800-18 rev. 1[262].

Dokument Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne (NSC 800-30 wer. 1.0) ma na celu dostarczenie wskazówek dotyczących przeprowadzania szacowania ryzyka systemów informatycznych podmiotów realizujących zadania publiczne, które zostały rozszerzone w dokumencie NSC 800-39. Szacowanie ryzyka, przeprowadzane na wszystkich trzech poziomach w hierarchii zarządzania ryzykiem, stanowi część ogólnego procesu zarządzania ryzykiem, dostarczając kierownikom wyższego szczebla informacji niezbędnych do określenia odpowiednich kierunków działań w odpowiedzi na zidentyfikowane ryzyka. W szczególności niniejszy dokument zawiera wskazówki dotyczące przeprowadzania każdego z etapów procesu szacowania ryzyka (tj. przygotowania do szacowania, przeprowadzenia szacowania, przekazania wyników szacowania oraz utrzymania szacowania) oraz sposobu, w jaki szacowanie ryzyka i inne procesy zarządzania ryzykiem w podmiocie uzupełniają się i wzajemnie się wspomagają. Publikacja NSC 800-30 zawiera również wytyczne dla organizacji dotyczące identyfikacji konkretnych czynników ryzyka, które należy na bieżąco monitorować

[261] Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0), KPRM, 2021, s. 7, 9
[262] Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0), KPRM, 2021, s. 7, 12

tak, aby podmioty mogły określić, czy ryzyko wzrosło do niedopuszczalnego poziomu (tj. czy przekroczyło poziom tolerancji ryzyka organizacyjnego) i aby można było podjąć różne działania w celu jego obniżenia. Wytyczne zawarte w niniejszej publikacji powinny mieć zastosowanie do wszystkich systemów informatycznych podmiotów realizujących zadania publiczne innych niż systemy podlegające regulacji wynikających z ustawy o ochronie informacji niejawnych. Dokument Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne opracowany został na podstawie specjalnej publikacji NIST SP 800-30 rev. 1[263].

Dokument Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0) kładzie nacisk na zarządzanie ryzykiem poprzez promowanie rozwoju zdolności w zakresie bezpieczeństwa i ochrony prywatności w systemach informatycznych w całym cyklu życia systemu (ang. System development life cycle – SDLC) poprzez utrzymywanie na bieżąco świadomości sytuacyjnej w zakresie bezpieczeństwa i ochrony prywatności tych systemów dzięki ciągłym procesom monitorowania oraz poprzez dostarczanie informacji liderom wyższego szczebla i kadrze kierowniczej w celu ułatwienia podejmowania decyzji dotyczących akceptacji ryzyka dla operacji organizacyjnych i aktywów, osób fizycznych, innych organizacji i państwa, wynikającego z użytkowania i funkcjonowania ich systemów. Dokument opisuje ramy zarządzania ryzykiem (Risk management framework, RMF) i zawiera wytyczne dotyczące zarządzania ryzykiem w zakresie bezpieczeństwa i prywatności oraz stosowania RMF w systemach informatycznych i organizacjach. Ma on na celu pomóc organizacjom w zarządzaniu ryzykiem związanym z bezpieczeństwem i ochroną prywatności oraz w spełnieniu wymogów przepisów ustawowych, wykonawczych i polityki. Zakres niniejszej publikacji odnosi się do systemów informatycznych podmiotów realizujących zadania publiczne, które gromadzą, przetwarzają, przechowują, wykorzystują, dzielą się, rozpowszechniają lub dysponują informacjami, niezależnie od tego, czy są to informacje w formie cyfrowej, czy innej niż cyfrowa. Zasoby informacyjne obejmują informacje i związane z nimi zasoby, takie jak personel, sprzęt, fundusze i technologie informatyczne. Dokument ten został opracowany na podstawie specjalnej publikacji NIST SP 800-37, rev. 2[264].

[263] Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne (NSC 800-30 wer. 1.0), KPRM, 2021, s. 7, 13

[264] Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0), KPRM, 2021, s. 7, 13-15

Dokument Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego (NSC 800-39 wer. 1.0) jest sztandarowym dokumentem z serii opracowanych rekomendacji dotyczących bezpieczeństwa informacji. Celem publikacji NSC 800-39 jest dostarczenie wytycznych do ustanowienia zintegrowanego, obejmującego całą organizację programu zarządzania ryzykiem w zakresie bezpieczeństwa informacji w działalności organizacji (tj. misji, funkcji, wizerunku i reputacji), aktywów organizacji, osób, innych organizacji i państwa. NSC 800-39 zapewnia uporządkowane, elastyczne podejście do zarządzania ryzykiem, które jest celowo szeroko zakrojone, a szczegółowe informacje dotyczące szacowania, reagowania i bieżącego monitorowania ryzyka są zawarte w innych wspierających narodowych standardach cyberbezpieczeństwa (NSC). Rekomendacje zawarte w publikacji nie mają na celu zastąpienia lub podważenia innych działań, programów, procesów lub podejść związanych z ryzykiem, które organizacje wdrożyły lub zamierzają wdrożyć w odniesieniu do obszarów zarządzania ryzykiem objętych innymi przepisami, dyrektywami, politykami, inicjatywami programowymi lub wymaganiami misji/biznesu. Opisane tu wskazówki dotyczące zarządzania ryzykiem mają charakter uzupełniający i powinny być stosowane jako część kompleksowego programu zarządzania ryzykiem w przedsiębiorstwie (ang. Enterprise Risk Management - ERM). Rekomendacje zawarte w dokumencie mają zastosowanie do wszystkich systemów informatycznych innych niż systemy określone, jako systemy bezpieczeństwa narodowego. Zostały opracowane z technicznego punktu widzenia w celu uzupełnienia podobnych zaleceń odnoszących się do systemów bezpieczeństwa narodowego i mogą być stosowane w takich systemach za zgodą odpowiednich organów państwowych sprawujących funkcje władcze nad takimi systemami. Zachęca się organy administracji państwowej, samorządowej i lokalnej, a także organizacje sektora prywatnego do rozważenia zastosowania tych rekomendacji, w zależności od potrzeb. Dokument Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego opracowany został na podstawie specjalnej publikacji NIST SP 800-39[265].

Dokument Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0) ma na celu pomoc organizacjom w ograniczeniu ryzyka związanego z technologiami korporacyjnymi wykorzystywanymi do telepracy, takimi jak serwery zdalnego dostępu, urządzenia klienckie do telepracy (w tym urządzenia typu "przynieś własne urządzenie" [BYOD] oraz urządzenia klienckie kontrahentów, partnerów biznesowych i dostawców,

[265] Zarządzanie ryzykiem bezpieczeństwa informacji (NSC 800-39 wer. 1.0), KPRM, 2021, s. 7, 14-15

znane również jako urządzenia kontrolowane przez strony trzecie) oraz komunikacja zdalnego dostępu. Dokument ten podkreśla znaczenie zabezpieczania wrażliwych informacji przechowywanych na urządzeniach do telepracy i przesyłanych poprzez zdalny dostęp w sieciach zewnętrznych. Zawiera dotyczące tworzenia polityk związanych z telepracą oraz wyboru, wdrożenia i utrzymania niezbędnych zabezpieczeń serwerów i klientów zdalnego dostępu. Dokument Przewodnik po telepracy w podmiocie publicznym został opracowany na podstawie specjalnej publikacji NIST SP 800-46 rev. 2[266].

Dokument Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0) zawiera katalog środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji, mających na celu ochronę operacji organizacyjnych i aktywów, osób, innych organizacji i państwa przed zróżnicowanym zestawem zagrożeń i ryzyka, w tym wrogimi atakami, błędami ludzkimi, klęskami żywiołowymi, awariami strukturalnymi, podmiotami obcego wywiadu oraz zagrożeniami dla prywatności. Zabezpieczenia są elastyczne i możliwe do dostosowania, a ich wdrożenie stanowi część procesu zarządzania ryzykiem w całej organizacji. Zabezpieczenia spełniają zróżnicowane wymagania wynikające z misji i potrzeb biznesowych, prawa, rozporządzeń wykonawczych, dyrektyw, regulacji, polityk, standardów i wytycznych. Skonsolidowany katalog zabezpieczeń odnosi się do bezpieczeństwa i ochrony prywatności z perspektywy funkcjonalności (tj. siły funkcji i mechanizmów zapewnianych przez zabezpieczenia) oraz z perspektywy wiarygodności (tj. miary zaufania do bezpieczeństwa lub możliwości ochrony prywatności zapewnianych przez środki bezpieczeństwa). Uwzględnianie funkcjonalności i wiarygodności zabezpieczeń przyczynia się do zapewnienia, że technologie i systemy informatyczne, które opierają się na tych produktach, są wystarczająco godne zaufania. Dokument Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji opracowany został na podstawie specjalnej publikacji NIST SP 800-53, rev. 5[267].

Dokument Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0) przedstawia zestaw zabezpieczeń bazowych (ang. control baselines) w zakresie bezpieczeństwa i ochrony prywatności. Istnieją trzy poziomy bazowe środków bezpieczeństwa (jeden dla każdego poziomu wpływu na system - niski wpływ, umiarkowany wpływ i wysoki wpływ), a także poziom bazowy zabezpieczeń prywatności, który jest stosowany do systemów niezależnie od poziomu wpływu na system. Poza poziomami

[266] Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0), KPRM, 2021, s. 5, 14
[267] Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0), KPRM, 2021, s. 7, 8

bazowymi zabezpieczeń, niniejsza publikacja zawiera wskazówki dostosowawcze i zestaw założeń roboczych, które pomagają w prowadzeniu i informowaniu o procesie wyboru zabezpieczeń. Zawarte są także wskazówki dotyczące rozwoju nakładek zabezpieczających ułatwiających dostosowanie poziomu bazowych środków bezpieczeństwa do potrzeb konkretnych społeczności, technologii i środowiska działania. Publikacja Zabezpieczenia bazowe systemów informatycznych oraz organizacji została opracowana na podstawie specjalnej publikacji NIST SP 800-53B[268].

Dokument Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0) zawiera tabele mapowania, które dostarczają organizacjom ogólnych wskazówek dotyczących zabezpieczeń NSC 800-53 wer. 21 w odniesieniu do normy PN-ISO/IEC 27001:2013, Technika informatyczna – Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania. Norma PN-ISO/IEC 27001 może być stosowana we wszystkich typach organizacji i określa wymagania dotyczące ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądów, utrzymywania i doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji (ang. Information Security Management System - ISMS) w kontekście ryzyka biznesowego. Publikacja NIST 800-39 zawierająca wytyczne dotyczące zarządzania ryzykiem na poziomie organizacyjnym, poziomie misji/procesu biznesowego oraz na poziomie systemu informacyjnego, jest zgodna z normą PN-ISO/IEC 27001 i dostarcza dodatkowych szczegółów wdrożeniowych dla podmiotów publicznych i ich kontrahentów[269].

Dokumenty Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0) i część II (NSC 800-60 cz. 2 wer. 1.0) służą zapewnieniu odpowiedniego poziomu bezpieczeństwa informacji w systemach informatycznych podmiotów publicznych zgodnie z oszacowanym poziomem ryzyka. Stanowią przewodnik metodyczny pozwalający na określenie poziomu wpływu potencjalnego incydentu na bezpieczeństwo informacji oraz na dostępność systemu informatycznego, w którym te informacje są przetwarzane. Wytyczne mają na celu ułatwienie przypisania odpowiedniego poziomu bezpieczeństwa informacji zgodnie z po-

[268] Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0), KPRM, 2021, s. 7, 8
[269] Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0), KPRM, 2021, s. 2

ziomami wpływu zakłóceń / incydentów, które mogą wynikać z nieuprawnionego ujawnienia, modyfikacji lub wykorzystania systemu informatycznego lub informacji. Wytyczne te zakładają, że użytkownik zapoznał się ze standardami kategoryzacji bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych przedstawionymi w publikacji NSC 199. Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I i część II, opracowane zostały na podstawie specjalnej publikacji NIST SP 800-60 vol. 1, rev. 1 i vol. 2, rev. 1[270].

Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer.1.0) ma na celu pomóc organizacjom w ograniczaniu ryzyka związanego z incydentami związanymi z bezpieczeństwem komputerowym, dostarczając praktycznych wskazówek dotyczących skutecznego i wydajnego reagowania na incydenty. Zawiera wskazówki dotyczące tworzenia skutecznego programu reagowania na incydenty, ale głównym celem dokumentu jest wykrywanie, analizowanie, ustalanie priorytetów i obsługa incydentów. Zachęca się organizacje do dostosowywania zalecanych wytycznych i rozwiązań, aby spełniały ich specyficzne wymagania dotyczące bezpieczeństwa i misji. Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego został opracowany na podstawie specjalnej publikacji NSC 800-61, rev. 2[271].

Dokument Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0) definiuje ZT (zero trust) i ZTA (Zero trust architecture) oraz wymienia podstawowe założenia projektowania ZTA na potrzeby podmiotu. Rozdział ten zawiera również listę doktryn projektu ZT, dokumentuje komponenty logiczne lub bloki konstrukcyjne ZT - możliwe jest, że unikatowe implementacje składają komponenty ZTA w różny sposób, ale obsługują te same funkcje logiczne. Dokument wymienia kilka możliwych przypadków użycia, w których ZTA może uczynić środowisko podmiotu bezpieczniejszym i mniej podatnym na udaną eksploatację przez atakującego. Przypadki obejmują zdalną pracę pracowników, usługi w chmurze i sieci gości. Dokument omawia zagrożenia dla podmiotu korzystającego z ZTA. Wiele z tych zagrożeń jest podobnych do innych rozwiązań architektonicznych, ale mogą wymagać różnych technik łagodzenia ich skutków. Dokument omawia sposób, w jaki założenia ZTA wpisują się w istniejące wy-

[270] Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0), część II (NSC 800-60 cz. 2 wer. 1.0), KPRM, 2021, cz. I, s. 7, 10, cz. II, s. 7, 10

[271] Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer.1.0), KPRM, 2021, s. 2, 17

tyczne dla podmiotów publicznych i/lub je uzupełniają, przedstawia punkt wyjścia do przejścia podmiotu (np. ministerstwa) na ZTA. Zawiera on opis ogólnych kroków niezbędnych do planowania i wdrażania aplikacji i infrastruktury podmiotu, które są zgodne z zasadami ZT. Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" opracowana została na podstawie publikacji specjalnej NIST SP 800-207[272].

Dokument Standardy Cyberbezpieczeństwa Chmur Obliczeniowych stanowi zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych w ramach inicjatywy Wspólna Infrastruktura Informatyczna Państwa (WIIP). Załącznik 5 Katalog Zabezpieczeń zawiera wykaz zabezpieczeń organizacyjnych i technicznych niezbędnych do zapewnienia wysokiego poziomu bezpieczeństwa informacji. Katalog opracowany został na podstawie standardu NIST 800-53 rev. 4. Załącznik 4 Podstawowe Wymagania Bezpieczeństwa – macierz zabezpieczeń - zawiera listę zabezpieczeń i zabezpieczeń rozszerzonych, mających zastosowanie do każdego z poziomów SCCO, modyfikującą wymagania zabezpieczeń dla określonego poziomu wpływu na atrybuty bezpieczeństwa zawarte w Załączniku 5[273].

2.7.5. Normy, metodyki i standardy bezpieczeństwa teleinformatycznego systemów przemysłowych

Bezpieczeństwo teleinformatycznych systemów przemysłowych (tzw. OT) jest szczególnie istotne dla podmiotów wykorzystujących zaawansowane systemy przemysłowe, tj. operatorów infrastruktury krytycznej czy operatorów usług kluczowych. Normy, metodyki i standardy bezpieczeństwa teleinformatycznych systemów przemysłowych wskazane w dokumentach systemu zarządzania kryzysowego są podstawowymi dokumentami standaryzacyjnymi w tym zakresie. Normy wskazane w NPOIK[274]:

- PN-EN ISO 27002 w zakresie systemu zarządzania bezpieczeństwem informacji;
- IEC 62443 / ISA 62433 – stanowi zbiór standardów zawierających rekomendacje, co do zakresu i realizacji programów poprawy bezpieczeństwa w przedsiębiorstwach będących operatorami przemysłowych systemów sterowania, wskaźników dla oceny stanu bezpieczeństwa w organizacji, definicji pojęć z zakresu bezpieczeństwa;

[272] Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0), KPRM, 2021, s. 2, 7
[273] Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, Ministerstwo Cyfryzacji, 2020, s. 4
[274] Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje 2018

- NIST 800-82 – zawiera wiele rekomendacji z zakresu bezpieczeństwa teleinformatycznego systemów automatyki, w tym w szczególności w obszarze architektury sieci i separacji sieci IK od pozostałych sieci przedsiębiorstwa;
- NERC CIP – amerykański standard poświęcony bezpieczeństwu teleinformatycznemu infrastruktury krytycznej w segmencie energetyki;
- API-1164 „Pipeline SCADA Security" – zbiór zasad dla bezpieczeństwa systemów ICS opracowany przez American Petroleum Institute specjalnie dla sektora rafineryjnego. Wytyczne w nim zawarte mogą być z powodzeniem zastosowane w systemach przemysłowych innych sektorów;
- TIA-942 – amerykański standard opisujący minimalne wymagania dla infrastruktury telekomunikacyjnej i centrów przetwarzania;
- ISO/IEC 24762[275] – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie;
- Protecting Industrial Control Systems – Recommendations for Europe and Member States (ENISA), dokument, który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz 7 głównych kroków jak podnieść poziom bezpieczeństwa w takim środowisku.

2.7.6. Normy ISO ciągłości działania

Wśród metodyk, norm i standardów oferujących rozwiązania ogólnoorganizacyjne zarządzania i zapewnienia ciągłości działania i aspektów pokrewnych, z nim związanych można wyróżnić normy międzynarodowe ISO:

- ISO 22301 – System zarządzania ciągłością działania;
- ISO 22316 – Odporność organizacji – pryncypia i atrybuty;
- ISO 28000 – System zarządzania bezpieczeństwem łańcucha dostaw.

Normy ISO 22301 i 22316 są standardami zarządzania w obszarze ciągłości działania, definiującymi systemowe podejście w odniesieniu do całości organizacji lub jej wydzielonej, zorganizowanej części. Z kolei norma ISO 28000 definiuje system zarządzania bezpieczeństwem łańcucha dostaw, a więc obszaru, który nie występuje we wszystkich podmio-

[275] Norma została wycofana w 2014 r., źródło: iso.org. Norma aktualna do stosowania, źródło gov.pl/mc

tach, a jeśli już występuje, to jest on zawsze specyficzny dla rodzaju działalności danej organizacji. Niezależnie od tego, jest to obszar mający bardzo duży wpływ na bieżącą zdolność operacyjną każdego podmiotu i jego możliwości zapewnienia ciągłości działania.

Norma ISO 22301 określa strukturę oraz wymagania wdrożenia oraz utrzymania systemu zarządzania ciągłością działania (SZCD), który rozwija ciągłość działania odpowiednią do wielkości i rodzaju wpływu, który organizacja może zaakceptować lub nie w wyniku zakłócenia jej działania. Rezultaty utrzymania SZCD są kształtowane przez wymagania prawne, regulacyjne, organizacyjne i branżowe organizacji, dostarczane wyroby i usługi, stosowane procesy, wielkość i strukturę organizacji oraz wymagania jej zainteresowanych stron (interesariuszy). Celem normy jest przygotowanie, dostarczenie oraz utrzymanie nadzoru oraz możliwości zarządzania całościową zdolnością organizacji do sprostania incydentom zakłócającym jej pracę. Norma określa wymagania do wdrożenia, utrzymania i doskonalenia systemu zarządzania, którego celem jest ochrona przed incydentami, zmniejszenie prawdopodobieństwa ich wystąpienia, przygotowanie się na nie, a także umiejętności odpowiedniego reagowania i powrotu do normalnego funkcjonowania w przypadku ich wystąpienia[276].

Norma ISO 22316 definiuje system zapewnienia odporności organizacji. Odporność organizacji to jej zdolność adaptacyjna w zmieniającym się środowisku, umożliwiająca jej realizację celów oraz przetrwanie i prosperowanie. Bardziej odporne organizacje mogą przewidywać zagrożenia i szanse oraz reagować na nie, wynikające z nagłych lub stopniowych zmian w ich kontekście wewnętrznym i zewnętrznym. Zwiększenie odporności może być strategicznym celem organizacyjnym i jest wynikiem dobrych praktyk biznesowych i skutecznego zarządzania ryzykiem. Norma zawiera pryncypia i zasady stanowiące podstawę do wzmacniania odporności organizacji, atrybuty opisujące cechy organizacji, które pozwalają na przyjęcie zasad, działania kierujące wykorzystaniem, oceną i wzmocnieniem atrybutów. System zapewnienia odporności organizacyjnej zbudowany jest z pryncypiów, atrybutów odporności organizacyjnej i związanych z nimi procesów oraz procesów ewaluacji (oceny) czynników mających wpływ na odporność[277].

Norma ISO 28000 określa wymagania dotyczące systemu zarządzania bezpieczeństwem, w tym aspekty krytyczne dla zapewnienia bezpieczeństwa łańcucha dostaw. Aspekty obejmują wszystkie działania kontrolowane lub będące pod wpływem organizacji, które

[276] PN-EN ISO 22301:2020 Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania – Wymagania, s.13
[277] ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes, s. v

mają wpływ na bezpieczeństwo łańcucha dostaw. ISO 28000 jest to standard zarządzania wysokiego poziomu, który umożliwia organizacji ustanowienie ogólnego systemu zarządzania bezpieczeństwem łańcucha dostaw. Norma wymaga od organizacji oceny środowiska bezpieczeństwa, w którym działa i określenia, czy istnieją odpowiednie środki bezpieczeństwa i czy istnieją inne wymagania regulacyjne, które organizacja już spełnia. Ponieważ łańcuchy dostaw mają charakter dynamiczny, niektóre organizacje zarządzające wieloma łańcuchami dostaw mogą wymagać od swoich usługodawców spełnienia odpowiednich rządowych lub normatywnych (np. norm ISO) wymagań bezpieczeństwa łańcucha dostaw, jako warunku włączenia do tego łańcucha dostaw w celu uproszczenia zarządzania bezpieczeństwem. System zarządzania bezpieczeństwem łańcucha dostaw ISO 28000 zbudowany jest z procesów definiujących generalne wymagania dla systemu, politykę bezpieczeństwa, szacowanie ryzyka bezpieczeństwa i planowania działań, wdrożenia i funkcjonowania, sprawdzania, weryfikacji i akcji korekcyjnych oraz przeglądu zarządzania i ciągłego doskonalenia[278].

Przegląd metodyk, norm i standardów dotyczących zarządzania bezpieczeństwem teleinformatycznym wykazał, że istnieje znacząca pula różnych rozwiązań normatywnych i metodycznych w tym zakresie. Metodyki, normy i standardy zapewnienia i zarządzania bezpieczeństwem teleinformatycznym i ciągłością działania oferują wiele rozwiązań i podejść. Rozpoznanie metodyk, norm i standardów bezpieczeństwa i ciągłości działania systemów teleinformatycznych stanowi ogromną wartość merytoryczną i skuteczne wsparcie w projektowaniu i wdrażaniu rozwiązań bezpieczeństwa teleinformatycznego.

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa teleinformatycznego systemów informacyjnych, usług i podmiotów, zdefiniowane w normach, metodykach i standardach wskazanych do stosowania przez przepisy prawne (ustawy i rozporządzenia) systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych, do których wdrożenia są zobowiązane podmioty systemu cyberbezpieczeństwa, właściwe dla zakresu niniejszej dysertacji zostaną opisane i przybliżone kontekstowo, w dedykowanym temu problemowi badawczemu rozprawy rozdziale szóstym – dotyczącym kwestii doboru wymaganych norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

[278] ISO 28000:2007 Specification for security management systems for the supply chain, s. 1

2.8. Podsumowanie i wnioski

W rozdziale drugim dokonano próby rozstrzygnięcia problemu badawczego dotyczącego kontekstu, warunków i środowiska systemu cyberbezpieczeństwa RP, sformułowanego jako pytanie: *jakie są aktualne kontekst, warunki i środowisko prawne, strategiczne, funkcjonalne i normatywno-standaryzacyjne systemu cyberbezpieczeństwa RP i czy ich rozpoznanie umożliwi opracowanie koncepcji doskonalenia systemu cyberbezpieczeństwa RP?*
W rozdziale przedstawiono w ujęciu teoretycznym wybraną w kontekście tematu i zakresu rozprawy problematykę bezpieczeństwa narodowego i cyberbezpieczeństwa państwa. Omówiono i przedstawiono pojęcia, istotę i definicje bezpieczeństwa w ujęciu bezpieczeństwa narodowego, bezpieczeństwa państwa, bezpieczeństwa międzynarodowego, bezpieczeństwa wewnętrznego, podając różne definicje, ujęcia, rodzaje i konteksty bezpieczeństwa. Poruszono zagadnienie bezpieczeństwa w zależności od polityki bezpieczeństwa państwa i strategii bezpieczeństwa oraz jako zależne od i funkcjonujące w ramach środowiska bezpieczeństwa i jego szczególnej formy – strategicznego środowiska bezpieczeństwa. Podniesiono zapewnianie bezpieczeństwa państwa w ramach i przez system bezpieczeństwa narodowego. Omówiono strukturę system bezpieczeństwa i jego składowe komponenty oraz zakres obejmowanych dziedzin na podstawie literatury przedmiotu oraz treści sformułowanych w dokumentach strategicznych bezpieczeństwa Polski. Przedstawiono bezpieczeństwo narodowe w ujęciu koncepcji sektorów bezpieczeństwa, przedstawiając sektory bezpieczeństwa i transsektorowe obszary bezpieczeństwa. Przedstawiono i omówiono pojęcia, istotę i definicje cyberbezpieczeństwa i zagadnień z nim związanych, scharakteryzowano wymiar, zakres i skalę oddziaływania cyberbezpieczeństwa na bezpieczeństwo narodowe zawarte w literaturze, normach i w dokumentach strategicznych bezpieczeństwa Polski. Przywołano powiązania cyberbepieczeństwa z bezpieczeństwem teleinformatycznym i informacyjnym oraz jego transsektorowy charakter w bezpieczeństwie państwa. Autor przedstawił własne pojmowanie i charakterystykę cyberbezpieczeństwa i cyberprzestrzeni oraz ich powiązań i zależności z bezpieczeństwem teleinformatycznym. Przedstawiono wyzwania, zagrożenia i incydenty cyberbezpieczeństwa w kontekście rozwoju i powszechnego wykorzystywania technologii i systemów teleinformatycznych w ujęciu zagadnień teoretycznych oraz działań i zdarzeń faktycznych. Szeroko scharakteryzowano cyberzagrożenia, przedstawiono występujące cyberataki, omówiono i scharakteryzowano działania o charakterze agresywnym podejmowane w cyberprzestrzeni, takie jak cyberwalka i cyberwojna. Przedstawiono i omó-

wiono stan bezpieczeństwa polskiej cyberprzestrzeni i działania w tym zakresie dedykowanych organów. Przedstawiono i omówiono w kilkuletnim przedziale czasowym skalę i trendy występowania incydentów, ich typy, atakowane sektory i typy instytucji wskazano zagraniczne kierunki, z których wrogie działania są prowadzone. Przeprowadzono rekonstrukcję regulacji prawnych i postanowień strategicznych dokumentów normatywnych bezpieczeństwa i ich analizę w zakresie zagadnień systemu cyberbezpieczeństwa oraz omówiono szereg norm, metodyk i standardów zarządzania bezpieczeństwem teleinformatycznym. Omówiono zagadnienia cyberbezpieczeństwa ujęte w dokumentach strategicznych bezpieczeństwa państwa. Przedstawiono podejście do cyberbezpieczeństwa, strategiczne cele bezpieczeństwa państwa i cele cyberbezpieczeństwa oraz działania, programy i strategie ich realizacji. Wskazano ich powiązania z problematyką podjętą w niniejszej rozprawie. Przedstawiono i omówiono ujęcie problematyki cyberbezpieczeństwa, systemu cyberbezpieczeństwa i działań w tym zakresie w dedykowanych tym zagadnieniom i zagadnieniom pokrewnym regulacjach prawnych. Scharakteryzowano zagadnienia cyberbezpieczeństwa w kontekście podjętych problemów badawczych. Przedstawiono i omówiono normy, standardy i metodyki zarządzania bezpieczeństwem informacji, systemów teleinformatycznych i zarządzania systemami teleinformatycznymi, takie jak normy ISO, NIST, Narodowe Standardy Bezpieczeństwa i inne standardy branżowe.

Rozdział drugi realizuje cel szczegółowy rozprawy, jakim jest *przybliżenie kontekstu, warunków i środowiska systemu cyberbezpieczeństwa RP, poprzez przedstawienie istoty i roli cyberbezpieczeństwa w systemie bezpieczeństwa narodowego, zrekonstruowanie obowiązujących przepisów prawnych i strategicznych dokumentów normatywnych w sposób formalny definiujących organizację systemu cyberbezpieczeństwa RP oraz poprzez rozpoznanie międzynarodowych i krajowych norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych, możliwych do zastosowania w systemie cyberbezpieczeństwa RP*.

Poznanie i uświadomienie przedstawionych w niniejszym rozdziale treści pozwala na pozytywną weryfikację przyjętej hipotezy pomocniczej mówiącej, że: *rozpoznanie aktualnych zagrożeń i stanu bezpieczeństwa polskiej cyberprzestrzeni oraz kontekstu, warunków i środowiska prawnego, strategicznego, normatywno-standaryzacyjnego systemu cyberbezpieczeństwa umożliwi opracowanie koncepcji doskonalenia rozwiązań organizacji systemu cyberbezpieczeństwa RP i zapewni jego efektywność i odpowiedni poziom bezpieczeństwa państwa.*

Problematyka i zagadnienia przedstawione w niniejszym rozdziale są bezpośrednio powiązane z problematyką rozprawy – jej przedmiotem badań, problemami badawczymi, celami i hipotezami. Rozpoznanie tych zagadnień ma służyć realizacji celów rozprawy. Jak wykazała analiza treści dokumentów strategicznych bezpieczeństwa w zakresie cyberbezpieczeństwa zdefiniowane w rozprawie przedmiot badań, problemy badawcze, cele i hipotezy wprost odnoszą się i adresują cele i zadania sformułowane w dokumentach strategicznych bezpieczeństwa RP zdefiniowane dla zakresu cyberbezpieczeństwa.

Rozwiązania organizacyjne systemu cyberbezpieczeństwa dotyczące zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa, wymaganych norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa zdefiniowane w przepisach prawnych krajowego systemu cyberbezpieczeństwa (Ustawy KSC i rozporządzeń), systemu zarządzania kryzysowego (Ustawy ZK, rozporządzeń, NPOIK), systemu informatyzacji podmiotów publicznych (Ustawy IPP, Rozporządzenia KRI) oraz w normach, metodykach i standardach zarządzania bezpieczeństwem systemów teleinformatycznych zostaną przybliżone w kontekście sformułowanych problemów badawczych niniejszej dysertacji w kolejnych, dedykowanych poszczególnym zagadnieniom rozdziałach: trzecim w odniesieniu do organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym, czwartym – odnośnie zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, piątym – dotyczącym kwestii doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i szóstym – adresującym kwestie wymaganych norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa państwa.

Rozdział III. ORGANIZACJA ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM NA POZIOMIE KRAJOWYM

Bezpieczeństwo narodowe, tak jak i cyberbezpieczeństwo państwa powinny być zapewniane w ramach systemu bezpieczeństwa państwa składającego się z systemu kierowania i systemów wykonawczych – operacyjnych i wsparcia. Zarządzanie cyberbezpieczeństwem musi być realizowane w podejściu zintegrowanym i kompleksowym. System cyberbezpieczeństwa jako system transsektorowy, powinien być zintegrowany w ramach systemu bezpieczeństwa państwa z innymi sektorowymi podsystemami oraz zarządzany ponadresortowo i ponadsektorowo. System taki powinien obejmować podsystem kierowania, który będzie zdolny do organizowania i koordynowania działań dotyczących strategicznych procesów i dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym przez podmioty rządowe i pozarządowe.

W polskim porządku prawnym rozwiązania systemu bezpieczeństwa cyberprzestrzeni państwa kształtowane są przez regulacje obejmujące system zarządzania kryzysowego oraz krajowy system cyberbezpieczeństwa. System zarządzania kryzysowego ustanawia m.in. procesy i dokumentację planowania i zarządzania bezpieczeństwem na poziomie krajowym angażujące organy władzy na najwyższym poziomie oraz dedykowane instytucje, natomiast krajowy system cyberbezpieczeństwa w ogóle nie adresuje zagadnień zarządzania cyberbezpieczeństwem na poziomie krajowym, skupiając się na poziomie operacyjnym. Rozwiązania te są niespójne, nie są ze sobą powiązane i nie mogą zapewnić odpowiedniego poziomu cyberbezpieczeństwa kraju. Nie kształtują koncepcji systemu bezpieczeństwa państwa uwzględniającego i wyodrębniającego podsystem cyberbezpieczeństwa i jego integralny i transsektorowy charakter. System taki powinien zapewniać koncepcję funkcjonalnego systemu cyberbezpieczeństwa w całościowym systemie bezpieczeństwa państwa, jego kompleksowy, całościowy model w praktycznym i aplikowalnym ujęciu metodycznym i strukturalnym, kształtujący strukturę procesów i dokumentów zarządzania strategicznego i operacyjnego cyberbezpieczeństwem państwa. Zdaniem autora *ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie*

z zasadami określonymi w systemie zarządzania kryzysowego zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.

Celem niniejszego rozdziału, w kontekście celu rozprawy, jest realizacja jej celu szczegółowego *opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym.* W niniejszym rozdziale dokonano próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym poprzez weryfikację przyjętej hipotezy pomocniczej. W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu rozwiązań organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa oraz dokonano analizy porównawczej rozwiązań. Przedstawiono także wyniki badań własnych autora w tym zakresie, przedstawiające stanowiska respondentów nt. efektywności dotychczasowych oraz rozważanych nowych rozwiązań, adresujących przyjęte założenia ujednolicenia i zharmonizowania zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego oraz dokonano ich analizy. Została opracowana i przedstawiona autorska koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym adresująca wyniki badania.

Zorganizowanie zarządzania cyberbezpieczeństwem na poziomie krajowym przedstawione jest w niniejszym rozdziale rozprawy z perspektywy dwóch funkcjonujących w Polsce systemów bezpieczeństwa, w ujęciu wybranych aspektów dotyczących problematyki niniejszego rozdziału, adresujących kwestie cyberbezpieczeństwa - systemu zarządzania kryzysowego, zdefiniowanego przez dokumenty strategiczne i właściwe regulacje prawne, dotyczące zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, zdefiniowanego przez właściwe dokumenty strategiczne i regulacje prawne, tworzące system cyberbezpieczeństwa państwa. Rozwiązania tworzące system informatyzacji podmiotów publicznych nie będą rozważane w kontekście problematyki niniejszego rozdziału, ponieważ nie odnoszą się one do przedmiotowych zagadnień.

3.1. Rozwiązania organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym

Rozwiązania organizacji (zorganizowania) zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie struktury procesów i dokumentów planistycznych i wykonawczych zostały rozpatrzone w ujęciu dwóch systemów bezpieczeństwa analizowanych

w niniejszej rozprawie – systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Charakterystyka systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w zakresie zorganizowania krajowego bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa została przedstawiona w rozdziale 2.6 pracy. W niniejszym rozdziale zostaną zaprezentowane rozwiązania systemowe tych regulacji w zakresie szczególnych rozwiązań organizacji zarządzania bezpieczeństwem na poziomie krajowym w zakresie struktury procesów i dokumentów planistycznych i wykonawczych tego poziomu zarządzania bezpieczeństwem.

System zarządzania kryzysowego jest rozpatrywany z perspektywy zależności bezpieczeństwa na poziomie krajowym od bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych, wspierających funkcjonowanie usług systemów infrastruktury krytycznej, czyli cyberbezpieczeństwa tej infrastruktury i jej usług. Zarządzanie kryzysowe i planowanie cywilne w tym zakresie są rozumiane i rozpatrywane jako zarządzanie cyberbezpieczeństwem.

3.1.1. Organizacja zarządzania cyberbezpieczeństwem w systemie zarządzania kryzysowego

System bezpieczeństwa państwa jest kształtowany w ogromnej mierze przez Ustawę o zarządzaniu kryzysowym (Ustawa ZK). Ustawa ta ustanawia proces zarządzania kryzysowego, będący elementem kierowania bezpieczeństwem narodowych, który polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków i odtwarzaniu zasobów i infrastruktury krytycznej[279].

Ustawa ZK w ramach zarządzania kryzysowego ustanawia proces planowania cywilnego, którym jest całokształt przedsięwzięć organizacyjnych mających na celu przygotowanie administracji publicznej i Sił Zbrojnych RP do zarządzania kryzysowego. Planowanie cywilne jest realizowane w ramach cyklu planowania, tzn. okresowego realizowania etapów: analizowania, programowania, opracowywania planu lub programu, jego wdrażania, testowania i uruchamiania. Zadania z zakresu planowania cywilnego obejmują przygotowanie planów zarządzania kryzysowego, przygotowanie struktur uruchamianych w sytuacjach kry-

[279] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 2

zysowych, przygotowanie i utrzymywanie zasobów niezbędnych do wykonania zadań ujętych w planie zarządzania kryzysowego, utrzymywanie baz danych niezbędnych w procesie zarządzania kryzysowego, przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzanymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wykonania wynika z odrębnych przepisów[280].

W systemie zarządzania kryzysowego w ramach procesów planowania bezpieczeństwa tworzone są oraz okresowo weryfikowane i aktualizowane niezbędne w tym zakresie dokumenty poziomu krajowego oraz spójne z nimi dokumenty poziomów ministerialnego i regionalnego – samorządowego wszystkich poziomów. W ramach dokumentów planistycznych bezpieczeństwa powstają: Krajowy Plan Zarządzania Kryzysowego (KPZK) oraz ministerialne i regionalne Plany Zarządzania Kryzysowego (PZK) oraz Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Na potrzeby opracowania tych planów przygotowywany jest Raport o zagrożeniach bezpieczeństwa narodowego zawierający również informacje o zagrożeniach cyberbezpieczeństwa.

Ustawa ZK w ramach planowania cywilnego ustanawia tworzenie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego (KPZK) oraz wojewódzkich, powiatowych i gminnych planów zarządzania kryzysowego (plany zarządzania kryzysowego). W skład planów zarządzania kryzysowego wchodzą plan główny, zespół przedsięwzięć na wypadek sytuacji kryzysowych i załączniki funkcjonalne planu głównego[281]. Plan główny zawiera:

- charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej, oraz mapy ryzyka i mapy zagrożeń;
- zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa;
- zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych;
- zadania określone planami działań krótkoterminowych dotyczących ochrony środowiska.

W ramach zespołu przedsięwzięć na wypadek sytuacji kryzysowych definiuje się:

- zadania w zakresie monitorowania zagrożeń;

[280] tamże, art. 3
[281] tamże, art. 5, 12

- tryb uruchamiania niezbędnych sił i środków, uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej oraz współdziałanie między siłami;
- procedury reagowania kryzysowego, określające sposób postępowania w sytuacjach kryzysowych.

Załączniki funkcjonalne planu głównego określają:

- procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej;
- organizację łączności;
- organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania;
- zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń;
- organizację ewakuacji z obszarów zagrożonych;
- organizację ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej;
- organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru;
- wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego;
- zasady oraz tryb oceniania i dokumentowania szkód;
- procedury uruchamiania rezerw państwowych;
- wykaz infrastruktury krytycznej znajdującej się odpowiednio na terenie województwa, powiatu lub gminy objętej planem zarządzania kryzysowego;
- priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

Załącznikami funkcjonalnymi do Krajowego Planu Zarządzania Kryzysowego są plany zarządzania kryzysowego opracowywane przez ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych w ramach realizacji powierzonych im zadań dotyczących zarządzania kryzysowego. W planach tych w szczególności uwzględnia się:

- analizę i ocenę możliwości wystąpienia zagrożeń dla infrastruktury krytycznej uwzględnionej w wykazie;
- szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków;

- organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa;
- organizację realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Plany zarządzana kryzysowego budowane są w strukturze wielopoziomowej – na poziomach centralnym - ogólnokrajowym, ministerialnym, wojewódzkim, powiatowym i gminnym.

Krajowy Plan Zarządzania Kryzysowego (KPZK) obejmuje swoją treścią wszystkie fazy zarządzania kryzysowego, tj. zapobieganie, przygotowanie, reagowanie i odbudowę, pogrupowane w dwóch częściach (A i B). Część A KPZK odnosi się do przedsięwzięć realizowanych przez administrację publiczną w fazach zarządzania kryzysowego: zapobieganie i przygotowanie. W części tej wyszczególniono przede wszystkim katalog przedsięwzięć, które powinny być realizowane w celu zminimalizowania ryzyka wystąpienia zagrożeń i/lub ograniczenia ich skutków. Ta część Planu zawiera następujące elementy[282]:

1) charakterystyka zagrożeń oraz ocena ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej, oraz mapy ryzyka i mapy zagrożeń;
2) zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa (opis przedsięwzięć realizowanych przez ministrów i wojewodów wymienionych w siatce bezpieczeństwa).

Część B KPZK zawiera z kolei rozwiązania stosowane przez administrację publiczną w ramach faz: reagowanie i odbudowa, koncentrując się w szczególności na procedurach reagowania oraz opisie mechanizmów i zasad wykonania zadań przez podmioty wiodące i współpracujące w przypadku wystąpienia sytuacji kryzysowej, a także działaniach na rzecz powrotu do normalnego funkcjonowania administracji publicznej, społeczeństwa i infrastruktury. Część B zawiera niżej wymienione elementy[283]:

1) zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa;
2) zadania w zakresie monitorowania zagrożeń;
3) procedury reagowania kryzysowego, określające sposób postępowania w sytuacjach kryzysowych – zestawienie modułów zadaniowych ministrów i wojewodów;
4) współdziałanie między siłami, uczestniczącymi w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej;

[282] Krajowy Plan Zarządzania Kryzysowego, cz. A, RCB, 2017, s. 2
[283] tamże, s. 2

5) tryb uruchamiania niezbędnych sił i środków, uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej;
6) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych (mapy w formacie GIS);
7) procedury realizacji zadań z zakresu zarządzania kryzysowego – Standardowe Procedury Operacyjne, w tym związane z ochroną infrastruktury krytycznej;
8) organizacja łączności;
9) organizacja systemu monitorowania zagrożeń, ostrzegania i alarmowania;
10) zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń;
11) organizacja ewakuacji z obszarów zagrożonych;
12) organizacja ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej;
13) zasady oraz tryb oceniania i dokumentowania szkód;
14) procedury uruchamiania rezerw strategicznych;
15) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej;
16) wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego.

Wskazany w Ustawie ZK układ strukturalny KPZK, który obejmuje wszystkie fazy zarządzania kryzysowego, a także uwzględnia składowe elementy tego procesu oraz zestawienie sił i środków na mapach opracowanych przy użyciu sytemu informacji geograficznej (GIS), dostępnych na potrzeby sytuacji kryzysowej na poziomie krajowym, czynią z KPZK funkcjonalne narzędzie zarządzania procesami w zarządzaniu kryzysowym. KPZK jest narzędziem wspomagającym system zarządzania kryzysowego, mającym na celu zapobieganie powstaniu sytuacji kryzysowej lub w przypadku jej wystąpienia, podjęcie zaplanowanych działań, które nie dopuszczałyby do jej rozwoju i minimalizowały skutki zdarzenia.

Na potrzeby Krajowego Planu Zarządzania Kryzysowego opracowywany jest Raport o zagrożeniach bezpieczeństwa narodowego (Raport). Raport jest dokumentem zawierającym następujące elementy[284]:

1) wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka;
2) określenie celów strategicznych;
3) określenie priorytetów w reagowaniu na określone zagrożenia;

[284] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 5a

4) wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych;
5) programowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnianie regionalnych i lokalnych inicjatyw;
6) wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych.

Kierunki działania wynikające z wniosków z Raportu stanowią element Krajowego Planu Zarządzania Kryzysowego oraz są uwzględniane w planach zarządzania kryzysowego. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji, a cykl planowania nie może być dłuższy niż dwa lata. Cykl planowania realizują właściwe organy administracji publicznej oraz podmioty przewidywane do realizacji przedsięwzięć określonych w planie zarządzania kryzysowego, w zakresie ich dotyczącym. Plany zarządzania kryzysowego uzgadnia się z kierownikami jednostek organizacyjnych, w zakresie ich dotyczącym, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planie[285].

W systemie zarządzania kryzysowego tworzony jest Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, który określa m.in. narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej. NPOIK przygotowuje dyrektor RCB we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy oraz właściwymi w sprawach bezpieczeństwa narodowego[286].

Krajowy Plan Zarządzania Kryzysowego oraz plany ministerialne, wojewódzkie, powiatowe i gminne wraz z Raportem i NPOIK stanowią materializację zintegrowanego rozwiązania zarządzania bezpieczeństwem i cyberbezpieczeństwem, uwzględniającego wszechstronne i metodyczne podejście agregujące rozwiązania z niższych poziomów hierarchii administracji do wyższych. Zapewniają w ten sposób spójność całego rozwiązania[287]. Realizują tym samym postulat zintegrowanego systemu bezpieczeństwa integrującego aspekty cyberbezpieczeństwa z innymi aspektami bezpieczeństwa oraz podsystem kierowania z podsystemami wykonawczymi.

[285] tamże, art. 5, 5a
[286] tamże, art. 5b
[287] Mąkosa G., *Zarządzanie kryzysowe a krajowy system cyberbezpieczeństwa*, [w:] K. Śmiałek (red.), Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa", wyd. WAT, Warszawa 2020, s. 200

3.1.2. Organizacja zarządzania cyberbezpieczeństwem w krajowym systemie cyberbezpieczeństwa

System cyberbezpieczeństwa Polski jest przypisany do Ustawy o krajowym systemie cyberbezpieczeństwa (Ustawa KSC) kształtującej rozwiązania i ustrój tego systemu od czasu jej ustanowienia. Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa KSC) określa m.in. organizację krajowego systemu cyberbezpieczeństwa, który ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[288].

W krajowym systemie cyberbezpieczeństwa nie ma formalnych procesów planowania i zarządzania cyberbezpieczeństwem ani dokumentów planistycznych, organizacyjnych, operacyjnych i zarządczych poziomu krajowego. Należy stwierdzić, że nie ma systemowego podejścia, procesów i dokumentów zarządzania cyberbezpieczeństwem. W zakresie formalnych działań dotyczących organizacji procesów zarządzania cyberbezpieczeństwem na poziomie krajowym Pełnomocnik Rządu do spraw Cyberbezpieczeństwa (Pełnomocnik) przygotowuje Raport o zagrożeniach bezpieczeństwa narodowego (Raport) w części dotyczącej zagrożeń cyberbezpieczeństwa, mogących doprowadzić do sytuacji kryzysowej, opracowywany w ramach planowania cywilnego, realizowanego w systemie zarządzania kryzysowego, na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego. Raport jest więc dokumentem systemu zarządzania kryzysowego, a nie krajowego systemu cyberbezpieczeństwa.

W zakresie planowania, organizacji i zarządzania cyberbezpieczeństwem na poziomie krajowym współpracują ze sobą różne powołane ustawą KSC organy, zapewniając działania o charakterze współpracy, koordynacji, analizy i nadzoru w odniesieniu do systemu zarządzania ryzykiem na poziomie krajowym i procesu zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa, przy czym ani system, ani proces nie zostały zdefiniowane, jak też działania z nich wynikające dla organizacji systemu na poziomie krajowym.

W krajowym systemie cyberbezpieczeństwa jako dokumenty formalne, w jakiś sposób definiujące działania konieczne do podjęcia w ramach tego systemu, ale nie w formule stałego, zdefiniowanego systemu organizacyjnego, lecz rozwiązań doraźnych, ad hoc, wy-

[288] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 1, 3

stępują wnioski i rekomendacje Pełnomocnika oraz Kolegium ds. cyberbezpieczeństwa (Kolegium) dotyczące działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Prezes Rady Ministrów (Premier) wydaje rekomendacje i wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa, dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie[289].

Krajowy system cyberbezpieczeństwa nie posiada w swojej strukturze takiego rozwiązania organizacyjnego zarządzania bezpieczeństwem poziomu krajowego, jak planowanie cywilne w systemie zarządzania kryzysowego, przez co najważniejsze dla funkcjonowania kraju i jego systemów administracyjno-społeczno-gospodarczych usługi są narażone działania nieskoordynowane i improwizowane w sytuacjach kryzysowych, powstałych w wyniku incydentów krytycznych dotykających systemów teleinformatycznych[290]. Krajowy system cyberbezpieczeństwa, oparty o Ustawę KSC, nie realizuje postulatu zintegrowanego systemu bezpieczeństwa integrującego aspekty cyberbezpieczeństwa z innymi aspektami bezpieczeństwa oraz podsystem kierowania z podsystemami wykonawczymi.

3.1.3. Organizacja zarządzania cyberbezpieczeństwem w systemie informatyzacji podmiotów publicznych

W systemie informatyzacji podmiotów realizujących zadania publiczne nie została zdefiniowana organizacja systemu cyberbezpieczeństwa na poziomie krajowym w kontekście planowania, zapobiegania, reagowania i odbudowy w sytuacjach zagrażających bezpieczeństwu, sytuacjach kryzysowych czy incydentach cyberbezpieczeństwa. Zagadnienia organizacji zarządzania cyberbezpieczeństwem czy bezpieczeństwem systemów teleinformatycznych na poziomie krajowym nie będą rozpatrywane w niniejszej rozprawie.

3.2. Analiza porównawcza rozwiązań organizacji zarządzania cyberbezpieczeństwem

System zarządzania kryzysowego ma dobrze zorganizowany system organizacyjny zarządzania bezpieczeństwem na poziomie krajowym. Zarządzaniu bezpieczeństwem służy

[289] tamże, art. 63, 65
[290] Mąkosa G., *Organizacja systemu cyberbezpieczeństwa*, wyd. cyt., s. 185

cykliczne planowanie cywilne, w ramach którego ustanawiany jest Krajowy Plan Zarządzania Kryzysowego (KPZK), a w jego ramach plany zarządzania kryzysowego na poziomie ministerstw i urzędów centralnych, jak również wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego. Na potrzeby opracowania KPZK przygotowywany jest Raport o zagrożeniach bezpieczeństwa narodowego (Raport), zawierający również odniesienia do aspektów cyberbezpieczeństwa. Zapewnieniu bezpieczeństwa na poziomie krajowym, w tym cyberbezpieczeństwa, służy ustanowiony i okresowo aktualizowany Narodowy Program Ochrony Infrastruktury Krytycznej w jego części definiującej narodowe priorytety, cele oraz wymagania i standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej. W realizację zadań planowania, organizowania i operacjonalizacji działań z zakresu zarządzania bezpieczeństwem na poziomie krajowym zaangażowane są organy od poziomu najwyższego – rządowego (Rada Ministrów, właściwe ministerstwa) i urzędów centralnych (Rządowe Centrum Bezpieczeństwa (RCB)), przez organy wojewódzkie do powiatowych i gminnych.

Zarządzanie kryzysowe jest dobrze zorganizowane pod względem struktury i zawartości tworzących je dokumentów planistycznych i zarządczych poziomu krajowego. Krajowy Plan Zarządzania Kryzysowego oraz plany ministerialne, wojewódzkie, powiatowe i gminne wraz z Raportem i NPOIK stanowią materializację zintegrowanego rozwiązania zarządzania bezpieczeństwem i cyberbezpieczeństwem.

Krajowy system cyberbezpieczeństwa nie posiada w swojej strukturze rozwiązania organizacyjnego ani dokumentów planowania, organizowania i zarządzania cyberbezpieczeństwem poziomu krajowego, przez co najważniejsze usługi dla funkcjonowania kraju i jego systemów administracyjno-społeczno-gospodarczych są narażone działania nieskoordynowane i improwizowane w sytuacjach kryzysowych, powstałych w wyniku incydentów krytycznych dotykających systemów teleinformatycznych. Krajowy system cyberbezpieczeństwa nie ma systemowego podejścia ani procesów i dokumentów zarządzania cyberbezpieczeństwem poziomu krajowego. W zakresie formalnych działań dotyczących organizacji cyberbezpieczeństwa na poziomie krajowym Pełnomocnik Rządu do spraw Cyberbezpieczeństwa (Pełnomocnik) przygotowuje Raport o zagrożeniach bezpieczeństwa narodowego (Raport) w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, opracowywany w ramach planowania cywilnego w systemie zarządzania kryzysowego na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego. Raport jest więc dokumentem systemu zarządzania kryzysowego, a nie systemu cyberbezpieczeństwa.

Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w ujęciu porównawczym przestawiona jest w tabeli 19.

Tabela 19. Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa

System zarządzania kryzysowego (SZK)	Krajowy system cyberbezpieczeństwa (KSC)
Krajowy Plan Zarządzania Kryzysowego	-
Raport o zagrożeniach bezpieczeństwa narodowego	-
Plan Zarządzania Kryzysowego ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych	-
Wojewódzkie, powiatowe, gminne plany zarządzania kryzysowego	-
Narodowy Program Ochrony Infrastruktury Krytycznej	-

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

Z przedstawionej analizy porównawczej rozwiązań organizacji zarządzania cyberbezpieczeństwem wynika, że system zarządzania kryzysowego posiada kompleksowe rozwiązanie planistyczne i zarządcze w zakresie zarządzania bezpieczeństwem, w tym cyberbezpieczeństwem, na poziomie krajowym, w ramach którego została zbudowana struktura odpowiedzialności i struktura dokumentów zarządczych poziomu krajowego. W zakresie tych dokumentów zarządczych i strategicznych zostały ustanowione: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe Plany Zarządzania Kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej oraz Raport o zagrożeniach bezpieczeństwa narodowego. System zarządzania kryzysowego odnosi się do zarządzania sytuacjami kryzysowymi dotyczącymi infrastruktury krytycznej, w tym teleinformatycznej infrastruktury krytycznej, w ramach zdefiniowanych systemów. Organizację zarządzania bezpieczeństwem w odniesieniu do teleinformatycznej infrastruktury krytycznej należy traktować jako organizację zarządzania bezpieczeństwem części cyberprzestrzeni, a więc również organizację zarządzania cyberbezpieczeństwem.

Za całościowe zorganizowanie zarządzania cyberbezpieczeństwem RP odpowiada ustanowiony krajowy system cyberbezpieczeństwa. Niestety, krajowy system cyberbezpieczeństwa nie posiada w swojej strukturze rozwiązania organizacyjnego wyrażonego w procesach i dokumentach zarządzania cyberbezpieczeństwem poziomu krajowego, pomimo że jego celem jest zapewnienie cyberbezpieczeństwa na poziomie krajowym usługom realizowanym przy zastosowaniu systemów teleinformatycznych poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa tych systemów. Krajowy system cyberbezpieczeństwa koncentruje się natomiast na zapewnieniu operacyjnego, funkcjonalnego bezpieczeństwa systemów teleinformatycznych podmiotów tego systemu oraz na ustanowieniu rozwiązań zarządzania incydentami cyberbezpieczeństwa. Taka sytuacja jest niezrozumiała i nie powinna mieć miejsca. Krajowy system cyberbezpieczeństwa potrzebuje rozwiązania organizacji zarządzania na poziomie krajowym.

Zdaniem autora zasadnym jest, zgodnie ze zdefiniowaną hipotezą, dotyczącą przedmiotowych zagadnień niniejszego rozdziału, ujednolicenie i zharmonizowanie organizacji cyberbezpieczeństwa RP zgodnie z zasadami określonymi w systemie zarządzania kryzysowego, co przyczyni się do zapewnienia efektywnego zarządzania cyberbezpieczeństwem na poziomie krajowym.

3.3. Wyniki przeprowadzonych badań

W ramach procesu badawczego, realizowanego w zakresie zagadnienia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, stanowiącym przedmiotową problematykę niniejszego rozdziału, poddano weryfikacji hipotezę brzmiącą:

Ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego zapewnieni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa,

sformułowaną jako odpowiedź na postawione pytanie badawcze:

Jaka jest aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić jej efektywność?

W celu znalezienia odpowiedzi na postawione pytanie badawcze oraz zweryfikowania sformułowanej hipotezy, w procesie badawczym zostały postawione respondentom – ekspertom pytania skonstruowane, jak niżej:

1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

   1.1. Zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

   1.2. Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.

   1.3. Proponowane w pkt. 1.2. powyżej zorganizowanie, planowanie i dokumentowanie zarządzania cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione, jako:

   1) *funkcjonujące niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego,*
   2) *funkcjonujące równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim połączone,*
   3) *w pełni zintegrowane z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa.*

W wyniku przeprowadzonego badania uzyskano od respondentów – ekspertów szereg odpowiedzi na postawione pytania. Analiza uzyskanych odpowiedzi na poszczególne

pytania, wyrażone w tezach w nich zawartych, została przestawiona i omówiona poniżej tekście niniejszego podrozdziału.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 1.

Wynik badania w zakresie pytania 1.1.

Wobec tezy pytania 1.1.,

Zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa,

wśród udzielonych przez respondentów odpowiedzi: 13 (28,8%) osób wyraziło zgodę z tezą, przy czym zdecydowana większość (10) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana, natomiast 25 (55,56%) osób nie zgodziło się z tezą, przy czym zdecydowana większość (16) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że większość respondentów nie zgadza się, a ściślej, raczej się nie zgadza z tezą zawartą w pytaniu.

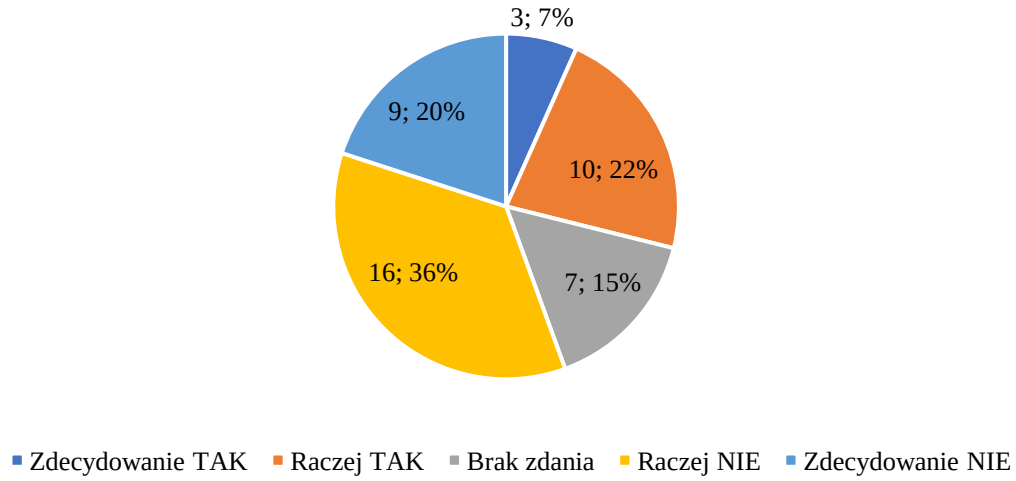
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 20 i na rysunku 14.

Tabela 20. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.1.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	13 / 25	3	10	7	16	9
%	100	28,89 / 55,56	6,67	22,22	15,55	35,56	20,00

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 14. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.1.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie ujawnia dominujące stanowisko respondentów. Uważają oni, że zarządzanie cyberbezpieczeństwem RP na poziomie krajowym i na niższych poziomach nie jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i wymaga wdrożenia zmian doskonalących system cyberbezpieczeństwa Polski. Wynik badania wskazuje na konieczność opracowania konkretnych rozwiązań procesowych i dokumentacyjnych krajowego planowania i zarządzania cyberbezpieczeństwem w celu zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedniego poziomu bezpieczeństwa państwa. Szczególnie należy uwzględnić fakt wykazany w przeprowadzonej analizie w tym zakresie, że krajowy system cyberbezpieczeństwa nie posiada w swojej strukturze żadnego rozwiązania organizacyjnego wyrażonego w procesach i dokumentach zarządzania cyberbezpieczeństwem poziomu krajowego.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze przedstawione przez respondentów w uzupełnieniu do swojego wyboru opcji odpowiedzi często odnoszą się do rozwiązań cyberbezpieczeństwa w ujęciu ogólnym, nie tylko do zorganizowania zarządzania na poziomie krajowym, lecz także na poziomie operacyjnym, strukturalnym oraz odnoszącym się do bezpieczeństwa systemów teleinformatycznych, czemu ostatecznie ma służyć system cyberbezpieczeństwa. Podane treści często są jakby daleko od podstawowego problemu, którego dotyczy pytanie,

z drugiej strony należy zwrócić uwagę, że odpowiednie i efektywne zorganizowanie zarządzania na poziomie krajowym przekłada się na wszystkie poziomy do regionalnego oraz na wszystkie aspekty i obszary merytorycznie związane z cyberbezpieczeństwem. Należy uwzględnić, że jest to pierwsze pytanie badania i należy przyjąć, że przedstawione opinie i komentarze odnoszą się do indywidualnej oceny i opinii funkcjonowania całego systemu cyberbezpieczeństwa, a nie tylko na trudnoidentyfikowalnej części procesów i dokumentów zarządzania na poziomie krajowym, które w Ustawie KSC nie zostało sformułowane. Dlatego należy zaakceptować tak szeroki zakres tematyczny podnoszony w argumentach i opiniach przez respondentów, i zauważyć w nich odniesienie do problemu zawartego w pytaniu. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w swoich argumentach, opiniach i komentarzach wyrażali przekonanie, że zarządzanie cyberbezpieczeństwem RP jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnia efektywność krajowego systemu cyberbezpieczeństwa. Zwracali uwagę na to, że ustawa o krajowym systemie cyberbezpieczeństwa jest pierwszym aktem prawnym, który w całości skupia się na zagadnieniach cyberbezpieczeństwa oraz, że jest implementacją europejskiej Dyrektywy NIS, co sprzyja unifikacji działań w UE, a także, że poza ustawą jest ustanowiona Strategia Cyberbezpieczeństwa RP, która formułuje stosowne cele i działania w tym zakresie. Ustawa KSC pozwala na zapewnienie efektywnego funkcjonowania krajowego systemu cyberbezpieczeństwa i dostatecznie reguluje te kwestie. Rozwiązania organizacyjne związane z cyberbezpieczeństwem na poziomie krajowym są dobrze zaprojektowane i funkcjonalnie sprawne i skuteczne, w szczególności na poziomie rządowym są jasno określone podmioty, kompetencje i zasady współpracy. Natomiast w obszarze sektorowym i samorządowym działania są słabo doinwestowane. Respondenci formułowali zdanie, że wprowadzenie kar finansowych i administracyjnych za niestosowanie jej zapisów oraz obowiązkowego procesu audytu i kontroli wymuszają na pomiotach jej stosowanie. Natomiast odesłanie w przepisach wykonawczych do uznanych standardów (ISO27001, ISO22301) powoduje, że organizacja cyberbezpieczeństwa pod względem procesowym, dokumentacyjnym, planistycznym i operacyjnym ma szansę zapewnić efektywność tego systemu. Zauważono, że pomimo że Istnieje kilka przepisów prawa, które są rozłączne zarówno na poziomie centralnym, jak oddzielne są zespoły odpowiedzialne za ich realizację. Każdy

oddzielnie realizuje wymagania jednak nigdy nie wystąpiła sytuacja wymagająca koordynacji realnych działań, nawet ćwiczenia i gry sztabowe każdy z podmiotów realizuje oddzielnie. Respondenci zwracali uwagę na konieczność doskonalenia procesów zarządzania i regularnej weryfikacji przepisów określających sposób funkcjonowania systemu cyberbezpieczeństwa w dynamicznie zmieniającym się obszarze cyberprzestrzeni.

Respondenci **nie zgadzający się z tezą pytania** w swoich argumentach, opiniach i komentarzach wyrażali przekonanie, że ogólne założenia krajowego systemu cyberbezpieczeństwa są słuszne, natomiast wykonanie jest dalekie od ideału. Organizacja cyberbezpieczeństwa zorganizowana jest adekwatnie do obowiązujących przepisów, co nie znaczy, że system jest adekwatny do wyzwań, jakie niesie obecny kontekst zagrożeń cyberprzestrzeni. Kluczowym wyzwaniem jest funkcjonowanie KSC równolegle do innych systemów zarządzania, a co za tym idzie ryzyko pojawiania się rozdźwięków, szczególnie sprzeczności z ustawą o zarządzaniu kryzysowym (procesy vs. obiekty). Regulacje, takie jak Ustawa KSC i RODO, spowodowały, że o cyberbezpieczeństwie wreszcie się mówi, nie ma niestety programu wspierania sposobu osiągniecia celów jakie stawiał sobie ustawodawca. Respondenci zwracali uwagę, że zarządzanie cyberbezpieczeństwem nie jest w ogóle zorganizowane na poziomie operacyjnym, nie podejmowane są działania w celu synchronizacji działań dla wszystkich jednostek, brak jest jednego organu czy podmiotu merytorycznego i jednocześnie operacyjnego, który potrafi skutecznie nadzorować i koordynować działania wszystkich w zakresie cyberbezpieczeństwa, że wymagane jest dopracowanie odpowiedzialności podmiotów systemu. Zwrócono uwagę, że w większości obszarów cyberbezpieczeństwo opiera się na biurokracji, a nie na rzeczywistych zdolnościach cyberobrony. Zostały wskazane wady systemowe tj.: niejednolite podejście sektorowe, brak odpowiedzialności osobistej kierowników jednostek OUK, brak skuteczności w egzekwowaniu wymagań wobec OUK, brak egzekwowania wymagań dla dostawców usług dla OUK, nie istnieje efektywne współdzielenie informacji o incydentach pomiędzy wszystkimi interesariuszami, brak planu krajowego na wypadek cyberataków terrorystycznych czy hybrydowych, brak współpracy pomiędzy CSIRT'ami. Zwrócono uwagę na brak uwzględnienia poziomu regionalnego, resortowo – samorządowego i JST, i zaniedbania na tym poziomie. Wskazano również na brak wiedzy po stronie firm świadczących usługi kluczowe, brak regularnych szkoleń i ćwiczeń a także zapewnienia budżetu dla rozwiązań w zakresie cyberbezpieczeństwa, zarówno technicznych, jak i usługowych. Respondenci zwrócili uwagę na niski poziom cyberbezpieczeństwa, niedofinansowanie, brak wsparcia i pozostawienie samym sobie podmiotów systemu.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 1., ppkt 1.1.

Autor rozprawy podziela dominujące zdanie respondentów i również nie zgadza się tezą. Zdaniem autora zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym nie jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, nie zapewnia efektywności krajowego systemu cyberbezpieczeństwa i odpowiedniego poziomu bezpieczeństwa państwa. W krajowym systemie cyberbezpieczeństwa brak zdefiniowanego formalnego procesu i dokumentów planistycznych i operacyjnych w zakresie analizy, planowania, programowania celów, działań i zadań w zakresie zapewnienia i zarządzania cyberbezpieczeństwem na poziomie krajowym.

Wynik badania w zakresie pytania 1.2.

Wobec tezy pytania 1.2.:

Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej,

spośród udzielonych przez respondentów odpowiedzi: 23 (51,11%) respondentów zgodziło się z tak postawioną tezą, przy czym większość (16) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana, natomiast 18 respondentów (40%) nie wyraziło zgody z taką tezą, przy czym większość (12) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zgadzają się, a ściślej, raczej się zgadzają z tak postawioną tezą.

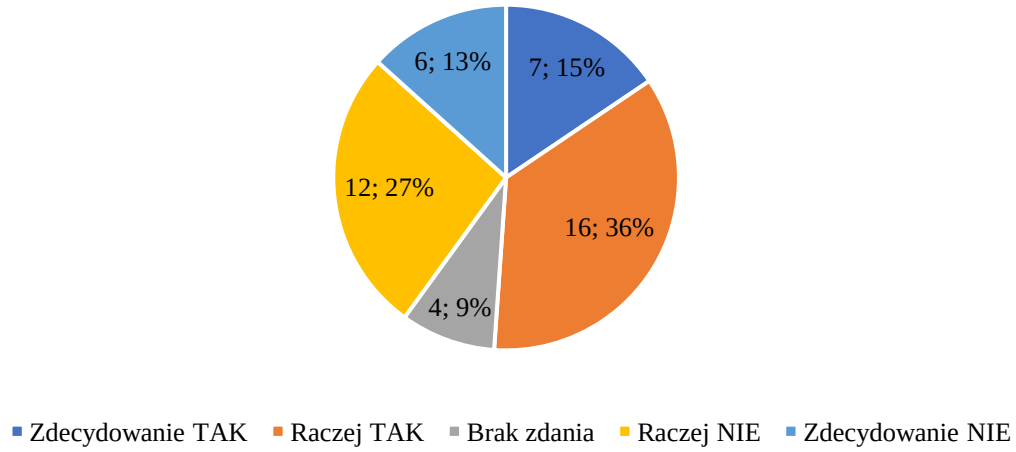
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 21 i na rysunku 14.

Tabela 21. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.2.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	23 / 18	7	16	4	12	6
%	100	51,11 / 40,00	15,55	35,56	8,89	26,67	13,33

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 15. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.2.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Uzyskany wynik badania w zakresie powyższego pytania odzwierciedla zdanie większości respondentów, którzy uważają, że konieczne do wdrożenia rozwiązania cyberbezpieczeństwem RP i ich organizacja powinna być ustanowiona i zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego funkcjonujących od wielu lat. Wynik badania w powyższym zakresie wskazuje, że zorganizowanie zarządzania cyberbezpieczeństwem powinno zawierać tożsame procesy i dokumenty zarządcze, jak w systemie zarządzania kryzysowego, tj. właściwe odpowiedniki: Krajowego

Planu Zarządzania Kryzysowego, ministerialnych, regionalnych i sektorowych planów zarządzania kryzysowego, Narodowego Programu Ochrony Infrastruktury Krytycznej, adresujące kwestie cyberbezpieczeństwa.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów, przedstawione w uzupełnieniu do wyboru opcji odpowiedzi, często odnoszą się do różnych aspektów działania i współdziałania systemów zarządzania kryzowego i cyberbezpieczeństwa. Niektóre z nich stanowią bezpośrednią argumentację, inne pośrednią, czasami w ujęciu ogólnym. W tak szerokim spektrum treści należy uwzględnić odniesienie do problematyki pytania. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** przedstawiali argumenty, opinie i komentarze, w których podnieśli, że w szerokim ujęciu krajowy system cyberbezpieczeństwa jest powiązany z systemem zarządzania kryzysowego, że skoro cyberprzestrzeń jest traktowana na równi z terytorium kraju, to absolutnie powinna być uwzględniona w systemie zarządzania kryzysowego, a nawet, że system cyberbezpieczeństwa państwa to element zarządzania kryzysowego, zatem organizacja zarządzania cyberbezpieczeństwem RP mogłaby być rozpatrywana podobnie, co zwiększyłoby sprawność i skuteczność działań na poziomie centralnym i lokalnym, choć pojawiają się opinie o braku zasadności dla sprowadzenia cyberbezpieczeństwa na poziom regionalny. Zwrócono uwagę, że cyberbezpieczeństwa jest odmianą bezpieczeństwa narodowego, a buduje się odrębny silos pt. cyberbezpieczeństwo. Respondenci wyrażali przekonanie, że bezpieczeństwo powinno posiadać zdefiniowane procesy i hierarchię, a organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/zdefiniowana zgodnie z określonymi i wdrożonymi zasadami oraz ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym poprzez realizację dedykowanych procesów cyberbezpieczeństwa. Ujednolicenie i zharmonizowanie oraz realizacja tożsamych procesów, stanowi podstawę efektywnego działania, może spowodować podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa, a jednolitość zarządzania umożliwia eliminację luk oraz sprawniejsze zarządzanie. Spójność metod działania jest bardzo zasadna, gdyż prowadzi do unifikacji rozwiązań (procesowych, technicznych, etc), zatem oparcie się o „szkielet" KPZK (który już jest) jest jak najbardziej racjonalne i w takim przypadku jest szansa na systemowe ujednolicone rozwiązania. Spójność w tym zakresie jest dobra i tańsza ze względu na skalę, to oszczędność czasu,

pracy i ograniczenie strat, są już ustalone procesy a kadry są wyszkolone. Zwracano też uwagę, że przedstawione rozwiązanie pozwoli na efektywne funkcjonowanie dwóch systemów – zarządzania kryzysowego i cyberbezpieczeństwa, a gdy struktury, dokumenty i procesy będą tożsame, to istnieje duża szansa na sprawne działanie i wymianę informacji na każdym poziomie - krajowym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym. W takim przypadku istnieje prawdopodobieństwo, że w przypadku wystąpienia kryzysu nie dojdzie do sytuacji, w której poszczególne podmioty będą operować różniącymi się procedurami i procesami. Respondenci przedstawili poglądy, że prawdopodobnie najlepszym rozwiązaniem będzie harmonizacja obu regulacji, być może powinna powstać jedna regulacja zarządzająca kryzysem w obu obszarach. Regulowanie tego samego obszaru w różnych aktach prawnych nie sprzyja jakości procesu, a korelacja działań w obszarze cyberbezpieczeństwa powinna być większa, jednak z uwzględnieniem specyficznych wymogów poszczególnych sektorów. Obszary cyberbezpieczeństwa powinny być, co do zasady, modelowane przy bezpośrednim uwzględnieniu zakresów IK oraz być aktualizowane/rozrastać się wspólnie z nimi na inne moduły funkcjonowania społeczeństwa wynikające z analizy bieżących zagrożeń ujawniających się na świecie. System cyberbezpieczeństwa powinien być zharmonizowany z innymi obszarami bezpieczeństwa Państwa, jednak jego struktura może być inna. Zwrócono również uwagę na zintegrowany charakter regulacji bezpieczeństwa tworzonych na poziomie UE i na zasadność w tym kontekście unifikacji zarządzania bezpieczeństwem IK i cyberbezpieczeństwem.

Respondenci **nie zgadzający się z tezą pytania** w swoich wypowiedziach przedstawiali argumenty, opinie i komentarze podnoszące, że konieczne jest ustandaryzowanie zarządzania cyberbezpieczeństwem RP oraz zarządzania kryzysowego, jednak przyjęcie modelu zarządzania kryzysowego nie jest rozwiązaniem, które powinno być wzorcem. Docelowy model powinien korzystać zarówno z dobrych rozwiązań jakie wnosi model zarządzania kryzysowego, jak również model zarządzania z aktualnego KSC. Zadania cyberbezpieczeństwa w wielu aspektach są inne niż zarządzania kryzysowego, które również powinny obejmować te aspekty. Zwrócono uwagę, że zarządzanie cyberbezpieczeństwem to proces ciągły i nie może mieć charakteru działań kryzysowych, które z natury koncentrują się na zdarzeniach incydentalnych, a więc są responsywne wobec zagrożeń. Jest dużo elementów, które się przecinają, ale z kwestiami ochrony infrastruktury krytycznej, a nie zarządzania kryzysowego, które jest kolejnym etapem, kiedy incydent wymknie się spod kontroli. Cyberbezpieczeństwo nie opiera się wyłącznie na realizacji strategii i operacji zarządzania incydentami, przez co nie może być postrzegane przez pryzmat jedynie sytuacji kryzysowej.

Proces zarządzania cyberbezpieczeństwem powinien opierać się na planowaniu odpowiedzi na znane ryzyka z uwzględnieniem mechanizmów detekcyjnych, prewencyjnych i korekcyjnych. Większość działań z obszaru cyberbezpieczeństwa to kwestie przygotowania na incydent, zabezpieczenia systemów IT/OT, szkolenia pracowników, monitorowania sieci, reagowania na incydent. Kluczową kwestią jest czas detekcji, czas reakcji, możliwość skutecznego współdziałania, odpowiedzi i gromadzenie informacji dla właściwej oceny ryzyka i skutecznej odpowiedzi w skali kraju, a nie pojedynczej firmy czy urzędu. Inni respondenci zwracają uwagę, że cyberbezpieczeństwo RP warunkowane jest w dużym stopniu odpornością operatorów kluczowych usług, natomiast ochrona infrastruktury krytycznej obejmuje wiele elementów, nie ograniczając się do cyberbezpieczeństwa. Zarządzanie cyberbezpieczeństwem, a w szczególności, procedury reakcji na incydenty, powinny uzupełniać się i nawiązywać do zarządzania kryzysowego, a samo zarządzanie kryzysowe pozostaje inną, wydaje się szerszą dziedziną aniżeli cyberbezpieczeństwo. Respondenci uważają, że zarządzanie kryzysowe i zarządzanie cyberbezpieczeństwem nie są tożsamymi procesami, ustawa o ZK skupia się na reagowaniu na określony poziom dolegliwości zdarzenia (patrz definicja sytuacji kryzysowej), natomiast w obszarze cyberbezpieczeństwa dominuje podejście oparte o budowanie odporności. Obecna ustawa o zarządzaniu kryzysowym nie odpowiada wyzwaniom obszaru cyber. Próba dostosowania ustawy o cyberbezpieczeństwie RP do obecnej ustawy o zarządzaniu kryzysowym przyniosłaby więcej szkód niż pożytku. Respondenci zwracają również uwagę, że zarządzanie kryzysowe jest systemem papierowym i biurokratycznym, powstaje dużo dokumentów, które nie mają realnego wpływu na funkcjonowanie organizacji. Ponadto zmiany planów bezpieczeństwa będą się ciągnąć miesiącami, a potrzebna jest większa granulacja, żeby mogły być szybciej dostosowywane pod kątem nowych wektorów ataku. Podniesiono również, że wskazane rozwiązania funkcjonują już w ramach Narodowego Programu Ochrony Infrastruktury Krytycznej w obszarze bezpieczeństwa teleinformatycznego. Poza tym analiza sposobu organizacji krajowego systemu cyberbezpieczeństwa, w tym jego powiązań ze sferą zarządzania kryzysowego, ustawą o działaniach antyterrorystycznych została przeprowadzona na etapie projektowania ustawy o krajowym systemie cyberbezpieczeństwa. Respondenci wskazują również propozycje kierunkowych zmian i sposobów funkcjonoiwania systemu cyberbezpieczeństwa. System powinien być stopniowalny: od infrastruktury krytycznej (absolutnie niezbędne funkcje państwa), przez usługi kluczowe (ochrona życia i zdrowia, skuteczność państwa, stabilność i bezpieczeństwo gospodarki) do pozostałych podmiotów (inne firmy, dostawcy, obywatele). W związku z cyfryzacją informacji i usług w gospodarce oraz strukturach państwowych,

cyberbezpieczeństwo powinno być zintegrowane z systemem zarządzania kryzysowego, jednak powinno również zostać zintegrowane z systemem edukacji, systemem zdrowia i każdym innym, w którym występują procesy cyfryzacji. Inne podejście, odnoszące się do aspektów operacyjnych, wskazuje model, w którym organizacja zarządzania cyberbezpieczeństwem powinna przypominać odpowiednik WOT (ze stopniami analogicznymi do poziomu kompetencji i okresowymi ćwiczeniami, szkoleniami i centralnie (regionalnie, sektorowo) przygotowanymi wytycznymi) oraz kadrą menadżerską, ekspercką w stałych strukturach. Zadaniem takiej stałej struktury powinna być bieżąca współpraca z Policją i wojskiem, tak, aby z jednej strony wspierać osoby narażone na ataki, wspierać firmy (zwłaszcza infrastruktury krytycznej oraz urzędy). Organizacja zarządzania cyberbezpieczeństwem powinna de facto pełnić rolę aktywnego przeciwdziałania, a nie reaktywnego działania. Według zasady „si vis pacem para bellum" (chcesz pokoju szykuj wojnę). Taki model całkowicie zmienia aktualny stan organizacyjny zarządzania cyberbezpieczeństwem w sposób rewolucyjny, jednakże wydaje się być ciekawym elementem uzupełniającym ten system na poziomie operacyjnym.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 1., ppkt 1.2.

Autor rozprawy w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora w systemie zarządzania bezpieczeństwem narodowym powinna być ujęta jednorodna i zharmonizowana organizacja zarządzania cyberbezpieczeństwem na poziomie krajowym. Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.

Wynik badania w zakresie pytania 1.3.

Wobec pytania 1.3.:

Proponowane w pkt. 1.2. powyżej zorganizowanie, planowanie i dokumentowanie zarządzania cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione, jako wariant wyboru,
respondenci udzielili w sumie 104 odpowiedzi, w tym odnośnie wariantu 1 – 30 głosów, wariantu 2 – 38 głosów, wariantu 3 – 36 głosów, w których:

- wariant 1 przedstawionego rozwiązania uzyskał poparcie 7 (6,73%) głosów, przy czym większość głosów (5) raczej go poparła, jest to więc „miękkie" poparcie, natomiast 19 (18,27%) głosów nie poparła tego wariantu, przy czym większość (11) głosów zdecydowanie nie poparła, co jest zdecydowanym brakiem poparcia;
- wariant 2 przedstawionego rozwiązania uzyskał poparcie 29 (27,88%) głosów, przy czym większość głosów (18) raczej go poparła, jest to więc „miękkie" poparcie, natomiast 9 (8,65%) głosów nie poparła tego wariantu, przy czym większość (6) głosów raczej nie poparła;
- wariant 3 przedstawionego rozwiązania uzyskał poparcie 18 (17,31%) głosów, przy czym zdecydowana większość głosów (13) zdecydowanie go poparła, natomiast 16 (15,38%) głosów nie wyraziło poparcia dla tego wariantu.

Podsumowując uzyskane wyniki, należy stwierdzić, że respondenci, w swojej większości, najbardziej poparli rozwiązanie wariantu 2 (29 głosów na tak, przy 9 głosach na nie), a następnie wariant 3 (18 głosów na tak, przy 16 głosach na nie). Respondenci byli zdecydowanie przeciwni wariantowi 1 (19 głosów na nie, przy 7 głosach na tak).

W odpowiedziach na postawione pytanie 1.3. odniesiono się do udzielonych głosów na „tak" lub na „nie", ponieważ nie wszyscy respondenci zdecydowali się w ogóle udzielić odpowiedzi na to pytanie, a spośród udzielających odpowiedzi, część oddała tylko jeden głos, wskazując wybrany wariant, inni respondenci wskazywali każdy z wariantów przypisując go do wybranej opcji standardowej odpowiedzi. Stąd pod uwagę nie jest brana liczba respondentów, a liczba oddanych głosów w wyborze wariantu rozwiązania.

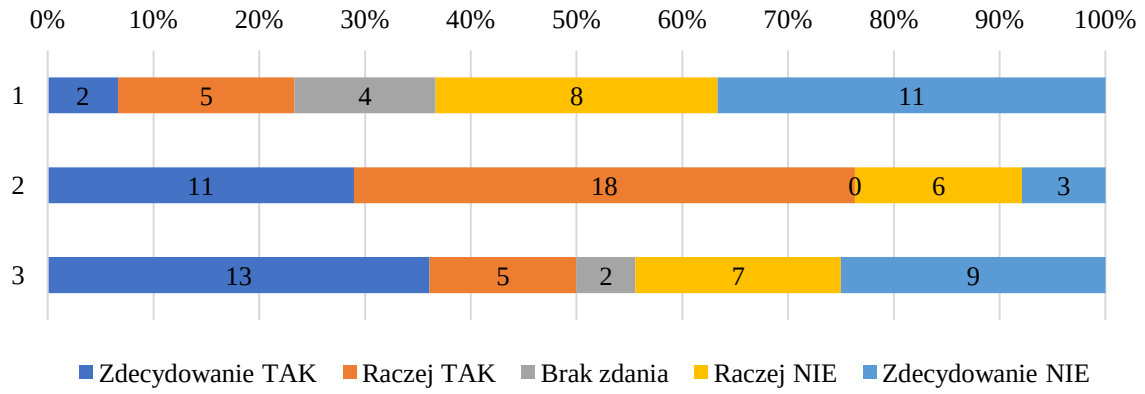
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 22 i na rysunku 16.

Tabela 22. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.3.

Lp.	Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP	Suma 104	Wynik T / N Szt./ %	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	funkcjonujące niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego	30	7 / 19 6,73 / 18,27	2 1,92	5 4,80	4 3,85	8 7,69	11 10,58
2	funkcjonujące równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim połączone	38	29 / 9 27,88 / 8,65	11 10,58	18 17,31	0 0	6 5,77	3 2,88
3	w pełni zintegrowane z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa	36	18 / 16 17,31 / 15,38	13 12,50	5 4,80	2 1,92	7 6,73	9 8,65

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 16. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 1.3.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie prezentuje zdecydowanie dominujące stanowisko większości respondentów uważających, że rozwiązania zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie procesów i dokumentów zarządczych, zsynchronizowanych i ujednoliconych z procesami i dokumentami zarządczymi zarządzania kryzysowego powinny funkcjonować równolegle do siebie, ale być punktowo/problemowo połączonymi. Niewielka większość respondentów uważa, że rozwiązania te powinny być w pełni

zintegrowane z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący łącznie problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa. Zdecydowana większość respondentów uważa, że rozwiązania zarządzania cyberbezpieczeństwem nie powinny funkcjonować niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego. Wynik badania w powyższym zakresie wskazuje, że na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym należy ustanowić dedykowane cyberbezpieczeństwu procesy i dokumenty zarządcze.

Konkludując, należy stwierdzić, że zdaniem większości respondentów (oddanych głosów) organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej, i:

1) powinna funkcjonować równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona (rozwiązanie preferowane – wariant 2 proponowanej odpowiedzi pytania ankietowego),
2) powinna być w pełni zintegrowana z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie drugiego wyboru – wariant 3 proponowanej odpowiedzi pytania ankietowego),
3) zdecydowanie nie powinna być funkcjonująca niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego (wariant 1 proponowanej odpowiedzi pytania ankietowego).

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Ze względu na charakter pytania i specyfikę odpowiedzi wskazane przez respondentów argumenty, opinie i komentarze należy uznać za uniwersalne, nie odnoszące się do

akceptacji lub braku akceptacji dla problemowego zagadnienia, lecz jako odniesienie się do dokonanego wyboru opcji odpowiedzi. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci uzasadniając swoje odpowiedzi, w uzupełnieniu do dokonanego wyboru opcji, wskazywali argumenty, opinie i komentarze, w których zwracali uwagę, że system cyberbezpieczeństwa powinien być zharmonizowany z innymi obszarami bezpieczeństwa Państwa, jednak jego struktura może być inna, obecna struktura wydaje się poprawna, nie musi odwoływać się do innych rozwiązań. Z założenia KSC, zarządzanie kryzysowe i infrastruktura krytyczna to są obszary które powinny się integrować, korelacja tych obszarów jest jak najbardziej pożądana, może być jednak trudna, trzeba uwzględniać specyfikę poszczególnych sektorów. Podniesiono również, że nie da się w pełni niezależnie zaprojektować tych systemów, bo incydent bezpieczeństwa komputerowego może prowadzić do sytuacji kryzysowych. Wskazano na trudność oceny, czy istnieje realna szansa połączenia zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w jednym dokumencie planistycznym, ponieważ obszary te obejmują bardzo szerokie spektrum działania i bardziej zasadne jest, aby osobno określać reguły działania i funkcjonowania tych systemów, które powinny być one ze sobą punktowo/problemowo połączone. Jeżeli system cyberbezpieczeństwa będzie niezależnie funkcjonować, to będzie działał dla własnych celów, jeżeli będzie w pełni zintegrowany z zarządzaniem kryzysowym, to stanie się zbiurokratyzowaną reaktywną strukturą z długim czasem reakcji. Zwrócono uwagę, że przepisy o zarządzeniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa powinny się uzupełniać i nie powinno się ich integrować do jednego systemu bezpieczeństwa. W obecnym stanie prawnym zarówno podmiot, który jest operatorem infrastruktury krytycznej oraz operatorem usługi kluczowej/operatorem usługi cyfrowej nie ma problemu w stosowaniu tych dwóch przepisów. Respondenci uważają, że dotychczasowy system zarządzania kryzysowego wymaga zmiany podejścia z zarządzania sytuacjami kryzysowymi na budowanie odporności. Ścisłe współdziałanie może się okazać niezbędne w obsłudze incydentu oraz zarządzaniu incydentem. System KSC dotyczy zdarzeń o dużej skali dotykających wielu obywateli. Integracja na poziomie systemowym pozwoli na skuteczne i pełne wykorzystanie możliwości jakie już posiadamy i tych, które tworzymy. Spójność w tym zakresie to oszczędność czasu, pracy i ograniczenie strat. Obszary cyberbezpieczeństwa powinny być, co do zasady modelowane

przy bezpośrednim uwzględnieniu zakresów IK oraz być aktualizowane/rozrastać się wspólnie z nimi na inne moduły funkcjonowania społeczeństwa. Cyberprzestrzeń jako terytorium kraju, powinna być uwzględniona w systemie zarządzania kryzysowego.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 1., ppkt 1.3.

Autor rozprawy prawie w pełni zgadza się z uzyskaną z odpowiedzi respondentów konkluzją. Zdaniem autora przedstawiona w pytaniu 1.2. propozycja organizacji zarządzania cyberbezpieczeństwem RP:

1) powinna być w pełni zintegrowana z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny proces i dokumentację zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie preferowane – wariant 3 proponowanej odpowiedzi pytania ankietowego);
2) funkcjonować równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona (rozwiązanie drugiego wyboru – wariant 2 proponowanej odpowiedzi pytania ankietowego);
3) natomiast zdecydowanie nie powinna być funkcjonująca niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego (wariant 1 proponowanej odpowiedzi pytania ankietowego).

3.4. Podsumowanie wyników badania

Wyniki przeprowadzonego badania realizowanego w zakresie zagadnienia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, stanowiącym przedmiotową problematykę niniejszego rozdziału pozytywnie zweryfikowały postawioną hipotezę stanowiącą, że: *ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego zapewnieni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

Wyniki badania pozwalają na sformułowanie wniosków do zastosowania w opracowaniu proponowanej koncepcji rozwiązań udoskonalenia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym. Wnioski z wyników badania są następujące:

1. Zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym **nie jest dobrze**

zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, **i nie zapewnia efektywności** krajowego systemu cyberbezpieczeństwa **i odpowiedniego poziomu bezpieczeństwa** państwa.

2. Organizacja zarządzania cyberbezpieczeństwem RP **powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór** rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim **ujednolicona i zharmonizowana** pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.
3. Proponowane w pkt 2. powyżej zorganizowanie, planowanie i dokumentowanie zarządzania cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania:
    1) **powinno funkcjonować równolegle** do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona. (rozwiązanie preferowane – wariant 2 proponowanej odpowiedzi pytania ankietowego) lub
    2) **powinno być w pełni zintegrowane** z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny zestaw procesów i dokumentów planistyczno-zarządczych, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie drugiego wyboru – wariant 3 proponowanej odpowiedzi pytania ankietowego).
    3) **nie powinno być funkcjonujące niezależnie i równolegle** do rozwiązań systemu zarządzania kryzysowego (wariant 1 proponowanej odpowiedzi pytania ankietowego).

Krajowy system cyberbezpieczeństwa potrzebuje rozwiązania organizacji zarządzania na poziomie krajowym. W systemie zarządzania bezpieczeństwem narodowym na po-

ziomie krajowym powinna być ujęta jednorodna, spójna i zharmonizowana organizacja zarządzania cyberbezpieczeństwem powiązana z zarządzaniem sytuacjami kryzysowymi, również zależnymi od bezpieczeństwa systemów teleinformatycznych infrastruktury krytycznej.

3.5. Koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym

W ramach przeprowadzonego procesu badawczego w zakresie organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym, stanowiącym przedmiotową problematykę niniejszego rozdziału, na podstawie wyników przeprowadzonego badania zweryfikowano pozytywnie postawioną przez autora hipotezę i sformułowano wnioski wynikające z uzyskanych od respondentów odpowiedzi na postawione w badaniu pytania, które zostały wykorzystane w opracowaniu proponowanej koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym.

Koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, adresująca wyniki i wnioski z badania, oparta na hipotezie badawczej przedstawia się następująco:

Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej, i powinna funkcjonować równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona – co może zostać zrealizowane poprzez ustanowienie dedykowanej, tożsamej struktury procesów i dokumentów zarządczych dla systemu cyberbezpieczeństwa RP, jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie. Koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym brzmi następująco:

Organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym powinna obejmować funkcjonującą równolegle, dedykowaną, tożsamą strukturę procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP (SCRP), jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie. System cyberbezpieczeństwa RP (SCRP) powinien obejmować dedykowane i skoncentrowane na kwestiach cyberbezpieczeństwa procesy oraz dokumenty zarządcze poziomu krajowego, jako odpowiedniki dokumentów systemu zarządzania kryzysowego, np.: **Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC)**, ministerialne, sektorowe i regionalne **Plany Zarządzania Cyberbezpieczeństwem (PZC)**, **Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT) oraz** dedykowany **Raport o zagrożeniach cyberbezpieczeństwa.**

Opracowana koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym stanowi nowum pracy, wypełnia zdiagnozowaną lukę, brak i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwej struktury procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP zsynchronizowanych z i wzorowanych na systemie zarządzania kryzysowego. Implementacja sformułowanej koncepcji w porządku prawnym i w dokumentach strategicznych i operacyjnych bezpieczeństwa pozwoli zarządzać cyberbezpieczeństwem kraju i zapewnić efektywność systemu cyberbezpieczeństwa RP i przez to odpowiedni poziom bezpieczeństwa państwa.

Aktualnie funkcjonujący krajowy system cyberbezpieczeństwa nie posiada żadnych procesów i dokumentów planowania i zarządzania cyberbebezpieczeństwem na poziomie krajowym i niższych poziomach strukturalnych i sektorowych, w przeciwieństwie do systemu zarządzania kryzysowego, dobrze zorganizowanego w tym zakresie.

Zestawienie porównawcze dotychczasowych rozwiązań organizacji zarządzania cyberbezpieczeństwem i struktury dokumentów zarządczych na poziomie krajowym w systemie zarządzania kryzysowego (SZK) i krajowym systemie cyberbezpieczeństwa (KSC) oraz koncepcji zorganizowania zarządzania cyberbezpieczeństwem systemu cyberbezpieczeństwa RP (SCRP) przestawione jest w tabeli 23.

Tabela 23. Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i koncepcji systemu cyberbezpieczeństwa RP

Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym		
Rozwiązania aktualne		**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**Koncepcja systemu cyberbezpieczeństwa RP (SCRP)**
Krajowy Plan Zarządzania Kryzysowego	-	**Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC)**
Raport o zagrożeniach bezpieczeństwa narodowego	-	**Raport o zagrożeniach cyberbezpieczeństwa**
Plan Zarządzania Kryzysowego (PZK) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych	-	**Plan Zarządzania Cyberbezpieczeństwem (PZC)** ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych, ministrów odpowiedzialnych za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa
Wojewódzkie, powiatowe, gminne **plany zarządzania kryzysowego**	-	Wojewódzkie, powiatowe, gminne **Plany Zarządzania Cyberbezpieczeństwem**
Narodowy Program Ochrony Infrastruktury Krytycznej	-	**Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT)**

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560; wyniki badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Procesy i dokumenty koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym powinny stanowić zintegrowane rozwiązanie planistyczne, uwzględniające wszechstronne i metodyczne podejście agregujące rozwiązania z niższych poziomów hierarchii administracji do wyższych w celu zapewnienia spójności całego rozwiązania. Dokumenty takie powinny powstawać w ramach cyklicznego planowania cyberbezpieczeństwa. W realizację zadań planowania, organizowania i operacjonalizacji działań z zakresu zarządzania cyberbezpieczeństwem na poziomie krajowym powinny być zaangażowane organy od poziomu najwyższego – rządowego (Rada Ministrów, właściwe ministerstwa, organy powołane Ustawą KSC) i urzędów centralnych (Rządowe Centrum Bezpieczeństwa (RCB)), przez CSIRTy poziomu krajowego i sektorowe, po organy wojewódzkie, a nawet powiatowe i gminne.

System cyberbezpieczeństwa RP (SCRP), w ramach koncepcji udoskonalenia zgodnie z założeniami wyników badania, powinien w ramach zarządzania na poziomie krajowym ustanawiać tworzenie i aktualizowanie **Krajowego Planu Zarządzania Cyberbezpieczeństwem (KPZC)** oraz ministerialnych, sektorowych, regionalnych - wojewódzkich, powiatowych i gminnych Planów Zarządzania Cyberbezpieczeństwem (**Plany Zarządzania Cyberbezpieczeństwem (PZC)**). W skład Planów Zarządzania Cyberbezpieczeństwem powinny wchodzić plan główny, zespół przedsięwzięć na wypadek incydentów krytycznych cyberbezpieczeństwa i sytuacji kryzysowych w wyniku incydentów krytycznych oraz załączniki funkcjonalne planu głównego.

Plan główny powinien zawierać:

- charakterystykę zagrożeń cyberbezpieczeństwa, ocenę ryzyka ich wystąpienia, w tym dotyczących teleinformatycznej infrastruktury krytycznej, systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze oraz mapy ryzyka i mapy cyberzagrożeń;
- zadania i obowiązki uczestników zarządzania cyberbezpieczeństwem w formie siatki bezpieczeństwa;
- zestawienie sił i środków planowanych do wykorzystania do obsługi incydentów krytycznych cyberbezpieczeństwa i w sytuacjach kryzysowych w wyniku incydentów krytycznych.

W ramach zespołu przedsięwzięć na wypadek incydentów krytycznych cyberbezpieczeństwa i sytuacji kryzysowych w wyniku incydentów krytycznych powinny być definiowane:

- zadania w zakresie monitorowania cyberzagrożeń;
- tryb uruchamiania niezbędnych sił i środków, uczestniczących w realizacji planowanych przedsięwzięć na wypadek incydentów krytycznych cyberbezpieczeństwa i sytuacjach kryzysowych w wyniku incydentów krytycznych oraz współdziałanie między siłami;
- procedury reagowania kryzysowego, określające sposób postępowania w przypadku wystąpienia incydentów krytycznych cyberbezpieczeństwa i w sytuacjach kryzysowych w wyniku incydentów krytycznych.

Załączniki funkcjonalne planu głównego powinny określać:

- procedury realizacji zadań z zakresu zarządzania cyberbezpieczeństwem, w tym związane z ochroną teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze;
- organizację łączności;
- organizację systemu monitorowania cyberzagrożeń, ostrzegania i alarmowania;
- zasady informowania ludności o cyberzagrożeniach i sposobach postępowania na wypadek cyberzagrożeń;
- zasady informowania administracji regionalnej (wojewódzkiej, powiatowej, gminnej) i jej struktur zarządzania kryzysowego w sytuacjach kryzysowych w wyniku incydentów cyberbezpieczeństwa - krytycznych, poważnych, istotnych i w podmiotach publicznych;
- organizację ochrony przed cyberzagrożeniami charakterystycznymi dla danego sektora i systemu;
- wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie zarządzania cyberbezpieczeństwem;
- zasady oraz tryb oceniania i dokumentowania szkód;
- procedury uruchamiania rezerw państwowych;
- wykaz teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze przynależnych do danego sektora oraz znajdujących się odpowiednio na terenie województwa, powiatu lub gminy, objętej Planem Zarządzania Cyberbezpieczeństwem;
- priorytety w zakresie ochrony oraz odtwarzania teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze.

Załącznikami funkcjonalnymi do Krajowego Planu Zarządzania Cyberbezpieczeństwem powinny być **Plany Zarządzania Cyberbezpieczeństwem** opracowywane przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych,

ministrów odpowiedzialnych za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa w ramach realizacji powierzonych im zadań dotyczących zarządzania cyberbezpieczeństwem i zarządzania kryzysowego. W planach tych w szczególności powinny być uwzględnione:

- analiza i ocena możliwości wystąpienia cyberzagrożeń dla teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze;
- szczegółowe sposoby i środki reagowania na cyberzagrożenia oraz ograniczania i likwidacji ich skutków;
- organizację monitoringu cyberzagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa;
- organizację realizacji zadań z zakresu ochrony teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze.

Plany Zarządzana Cyberbezpieczeństwem budowane powinny być w strukturze wielopoziomowej – na poziomach centralnym - ogólnokrajowym, ministerialnym, sektorowym, wojewódzkim, powiatowym i gminnym.

Na potrzeby Krajowego Planu Zarządzania Cyberbezpieczeństwem powinien być opracowywany dedykowany **Raport o zagrożeniach cyberbezpieczeństwa.** Raport powinien być dokumentem zawierającym następujące elementy:

1. wskazanie najważniejszych cyberzagrożeń przez stworzenie mapy ryzyka;
2. określenie celów strategicznych cyberbezpieczeństwa;
3. określenie priorytetów w reagowaniu na określone cyberzagrożenia;
4. wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych cyberbezpieczeństwa;
5. programowanie zadań w zakresie poprawy cyberbezpieczeństwa przez uwzględnianie sektorowych, regionalnych i lokalnych inicjatyw;
6. wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych cyberbezpieczeństwa.

Kierunki działania wynikające z wniosków z Raportu powinny stanowić element Krajowego Planu Zarządzania Cyberbezpieczeństwem oraz być uwzględniane w planach zarządzania cyberbezpieczeństwem. Plany Zarządzania Cyberbezpieczeństwem powinny podlegać systematycznej aktualizacji, a cykl planowania nie powinien być dłuższy niż dwa lata. Cykl planowania powinny realizować właściwe organy administracji publicznej oraz podmioty przewidywane do realizacji przedsięwzięć określonych w planach zarządzania cyberbezpieczeństwem, w zakresie ich dotyczącym. Plany Zarządzania Cyberbezpieczeństwem powinny być uzgadniane z kierownikami jednostek organizacyjnych, w zakresie ich dotyczącym, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach.

W systemie cyberbezpieczeństwa RP powinien być tworzony **Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT)**, którego celem powinno być stworzenie warunków do poprawy bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze, który powinien określać m.in. narodowe priorytety, cele, wymagania oraz standardy służące zapewnieniu sprawnego funkcjonowania ww. teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych. NPOIT powinien przygotowywać dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z organami ustanowionymi przez Ustawę KSC, ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy i sektory oraz właściwymi w sprawach bezpieczeństwa narodowego.

Tak skonstruowany dla systemu cyberbezpieczeństwa RP zbiór procesów i dokumentów zarządczych mógłby spełnić zdefiniowane postulaty i warunki koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa na poziomie krajowym, zakładające ustanowienie dedykowanej, tożsamej struktury procesów i dokumentów zarządczych dla systemu cyberbezpieczeństwa RP, jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie.

3.6. Podsumowanie i wnioski

W rozdziale trzecim dokonano próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, sfor-

mułowanego jako pytanie badawcze: *jaka jest aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić jej efektywność?* Rozstrzygnięcie problemu zostało przeprowadzone poprzez weryfikację w procesie badawczym przyjętej hipotezy pomocniczej stwierdzającej, że: *ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego zapewnieni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

W celu weryfikacji hipotezy przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu rozwiązań zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa. Przedstawiono i omówiono rozwiązania organizacji (zorganizowania) zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie struktury procesów i dokumentów planistycznych i wykonawczych w ujęciu regulacji prawnych dwóch systemów bezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Dokonano analizy porównawczej tych rozwiązań w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego posiada kompleksowe rozwiązanie planistyczne i zarządcze w zakresie zarządzania bezpieczeństwem, w tym cyberbezpieczeństwem, na poziomie krajowym, w ramach którego została zbudowana struktura odpowiedzialności i struktura dokumentów zarządczych poziomu krajowego oraz, że krajowy system cyberbezpieczeństwa nie posiada wyrażonego w procesach i powiązanych dokumentach rozwiązania planowania i zarządzania cyberbezpieczeństwem na poziomie krajowym, natomiast koncentruje się na zapewnieniu operacyjnego, funkcjonalnego bezpieczeństwa systemów teleinformatycznych podmiotów tego systemu oraz na ustanowieniu rozwiązań zarządzania incydentami cyberbezpieczeństwa. Przeprowadzono badania własne autora w tym zakresie i dokonano ich analizy. Wyniki badania wykazały, że aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowy nie jest dobrze zorganizowana, uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań i uzyskanych opinii od respondentów sformułowana została koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, wskazująca wytyczne dla jego struktury i dedykowane krajowemu cyberbezpieczeństwu dokumenty zarządcze. Koncepcja adresuje wyniki i wnioski z badania, i jest oparta na hipotezie badawczej. Opracowano tabelaryczne zestawienie porównawcze dotychczasowych rozwiązań or-

ganizacji zarządzania cyberbezpieczeństwem i struktury dokumentów zarządczych na poziomie krajowym w systemie zarządzania kryzysowego (SZK) i krajowym systemie cyberbezpieczeństwa (KSC) oraz koncepcji zorganizowania zarządzania cyberbezpieczeństwem systemu cyberbezpieczeństwa RP (SCRP). W wyniku przeprowadzonego procesu badawczego sformułowana hipoteza pomocnicza została pozytywnie zweryfikowana.

W ramach realizacji celu głównego rozprawy, którym jest: *opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa,* w ramach niniejszego rozdziału został zrealizowany cel szczegółowy rozprawy: *opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym*.

Na podstawie przyjętej hipotezy, wyników badań, sformułowanych konkluzji i wniosków opracowano koncepcję doskonalenia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym. Tym samym przyjęty cel szczegółowy rozprawy został osiągnięty, przez co przyczynił się do osiągnięcia celu głównego rozprawy.

Rozdział IV. STRUKTURY I RELACJE OPERACYJNE ZARZĄDZANIA W SYSTEMIE CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo państwa jest częścią składową bezpieczeństwa narodowego, które jest zarządzane i zapewniane w ramach systemu bezpieczeństwa państwa. System ten składa się ze zintegrowanych ze sobą systemu kierowania i systemów wykonawczych – operacyjnych i wsparcia. Zarówno w podsystemie kierowania i w podsystemach wykonawczych kluczową rolę pełnią dedykowane zadaniom zarządzania i zapewniania bezpieczeństwa podmioty i instytucje oraz ich struktury i relacje w systemie bezpieczeństwa. Zarządzanie cyberbezpieczeństwem musi być realizowane w ramach systemu bezpieczeństwa państwa w sposób transsektorowy, kompleksowy i zintegrowany z innymi sektorowymi podsystemami. System taki powinien obejmować niezbędne podmioty i instytucje oraz ich struktury i relacje operacyjne i organizacyjne, które będą zdolne do organizowania i koordynowania działań i procesów w zakresie strategicznego planowania i zarządzania cyberbezpieczeństwem oraz zarządzania incydentami cyberbezpieczeństwa na poziomie krajowym.

Rozwiązania systemu bezpieczeństwa cyberprzestrzeni państwa, w polskim porządku prawnym, kształtowane są przez regulacje obejmujące system zarządzania kryzysowego oraz krajowy system cyberbezpieczeństwa. System zarządzania kryzysowego ustanawia m.in. organy państwowe i instytucje odpowiedzialne za realizację procesów i dokumentacji planowania i zarządzania bezpieczeństwem oraz za zarządzanie sytuacjami kryzysowymi, w tym wynikającymi z incydentów cyberbezpieczeństwa. Krajowy system cyberbezpieczeństwa nie definiuje zagadnień zarządzania cyberbezpieczeństwem na poziomie krajowym, w związku z czym nie ustanawia dla tych działań odpowiedzialnych organów i instytucji. System ten skupia się na poziomie operacyjnym, dla którego ustanawia strukturę podmiotów – organów i instytucji – odpowiedzialnych za zarządzanie incydentami cyberbezpieczeństwa. Rozwiązania obu systemów są niespójne, nie są ze sobą powiązane, nie angażują struktur organizacyjnych w sposób zintegrowany i nie mogą zapewnić odpowiedniego poziomu cyberbezpieczeństwa kraju. Rozwiązania te nie kształtują koncepcji systemu bez-

pieczeństwa państwa uwzględniającego i wyodrębniającego zintegrowany podsystem cyberbezpieczeństwa i jego integralny i transsektorowy charakter. Taki system bezpieczeństwa powinien zapewniać funkcjonalny system cyberbezpieczeństwa w całościowym systemie bezpieczeństwa państwa, jego kompleksowy, całościowy model w praktycznym i aplikowalnym ujęciu metodycznym i strukturalnym, wskazując niezbędne w takim systemie organy i podmioty, ich struktury i relacje organizacyjne i operacyjne niezbędne dla efektywnego realizowania procesów i dokumentów zarządzania strategicznego i operacyjnego cyberbezpieczeństwem państwa oraz zapewnienia bezpieczeństwa i zarządzania cyberincydentami i sytuacjami kryzysowymi na poziomie krajowym. Zdaniem autora *ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

Celem niniejszego rozdziału, w kontekście celu rozprawy, jest realizacja jej celu szczegółowego *opracowanie koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.* W niniejszym rozdziale dokonano próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym poprzez weryfikację przyjętej hipotezy pomocniczej. W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa oraz dokonano analizy porównawczej rozwiązań. Przedstawiono także wyniki badań własnych autora w tym zakresie, przedstawiające stanowiska respondentów nt. efektywności dotychczasowych oraz rozważanych w badaniu nowych rozwiązań, adresujących przyjęte założenia ujednolicenia i zharmonizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym oraz zapewniania cyberbezpieczeństwa i zarządzania cyberincydentami i sytuacjami kryzysowymi, występujących w systemie zarządzania kryzysowego i w krajowym systemie cyberbezpieczeństwa oraz dokonano ich analizy. Została opracowana i przedstawiona autorska koncepcja zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, adresująca wyniki badania.

Zorganizowanie struktur i relacji operacyjnych zarządzania w systemie cyberbezpieczeństwa na poziomie krajowym jest przedstawione w niniejszym rozdziale rozprawy z perspektywy dwóch funkcjonujących w Polsce systemów bezpieczeństwa, w ujęciu wybranych

aspektów dotyczących problematyki niniejszego rozdziału, adresujących kwestie cyberbezpieczeństwa - systemu zarządzania kryzysowego, zdefiniowanego przez dokumenty strategiczne i właściwe regulacje prawne, dotyczące zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, zdefiniowanego przez właściwe dokumenty strategiczne i regulacje prawne, tworzące krajowy system cyberbezpieczeństwa.

Rozwiązania tworzące system informatyzacji podmiotów publicznych nie będą rozważane w kontekście problematyki niniejszego rozdziału, ponieważ nie odnoszą się one do przedmiotowych zagadnień.

4.1. Rozwiązania struktur i relacji operacyjnych cyberbezpieczeństwa w Polsce

Rozwiązania w zakresie struktur i relacji operacyjnych zarządzania systemu cyberbezpieczeństwa zostaną rozpatrzone w ujęciu dwóch systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Charakterystyka systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w zakresie zorganizowania krajowego bezpieczeństwa systemów teleinformatycznych i cyberbezpieczeństwa została przedstawiona w rozdziale 2.6 pracy. W niniejszym rozdziale zostaną zaprezentowane rozwiązania systemowe tych regulacji w zakresie szczególnych rozwiązań organizacji struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.

System zarządzania kryzysowego jest rozpatrywany z perspektywy zależności bezpieczeństwa na poziomie krajowym od bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych wspierających funkcjonowanie usług systemów infrastruktury krytycznej, czyli cyberbezpieczeństwa tej infrastruktury i jej usług. Zarządzanie kryzysowe i planowanie cywilne w tym zakresie są rozumiane i rozpatrywane jako zarządzanie cyberbezpieczeństwem.

4.1.1. Struktury i relacje operacyjne w systemie zarządzania kryzysowego

Ustawa o zarządzaniu kryzysowym (Ustawa ZK) określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tej dziedzinie. Struktura zarządzania jest wielopoziomowa i wielowymiarowa. Rozciąga się od poziomu rządowego, przez ministerialny, wojewódzki, powiatowy, do gminnego. Dla każdego poziomu

zdefiniowane są zespół zarządzania kryzysowego, centrum zarządzania kryzysowego, organ właściwy i organ pomocniczy (ten ostatni tylko dla poziomów wojewódzkiego, powiatowego i gminnego). Ustawa ZK określa organy właściwe w sprawach zarządzania kryzysowego i podmioty systemu, definiuje również ich struktury i relacje w kontekście zarządzania kryzysowego, w tym zarządzania bezpieczeństwem systemów i sieci teleinformatycznych, co wiąże się z cyberbezpieczeństwem.

W systemie zarządzania kryzysowego jako organy i podmioty występują[291]:

- Prezes Rady Ministrów,
- Rada Ministrów,
- Rządowy Zespół Zarządzania Kryzysowego (RZZK),
- dyrektor Rządowego Centrum Bezpieczeństwa (RCB),
- Rządowe Centrum Bezpieczeństwa (RCB),
- ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego,
- zespoły zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych (ZZK),
- centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych (CZK),
- minister właściwy do spraw administracji publicznej,
- minister właściwy do spraw wewnętrznych,
- kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego,
- Szef Agencji Bezpieczeństwa Wewnętrznego,
- Pełnomocnik Rządu do spraw Cyberbezpieczeństwa,
- wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim,
- wojewódzki zespół zarządzania kryzysowego (WZZK), wojewódzkie centrum zarządzania kryzysowego (WCZK),
- starosta, powiatowy zespół zarządzania kryzysowego (PZZK), powiatowe centrum zarządzania kryzysowego (PCZK),

[291] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 1

- wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK), gminne centrum zarządzania kryzysowego (GCZK),
- operator infrastruktury krytycznej – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej (OIK).

Strukturę i relacje organów właściwych i podmiotów w systemie zarządzania kryzysowego przedstawia rysunek 17.

Rys. 17. Struktury i relacje operacyjne w systemie zarządzania kryzysowego – model relacji

Struktury i relacje operacyjne systemu zarządzania kryzysowego – model relacji				
	POZIOMY WSPÓŁPRACY			
ZWIERZCHNOŚĆ	**ORGAN**	**ZESPÓŁ ZARZĄDZANIA KRYZYSOWEGO**	**CENTRUM ZARZĄDZANIA KRYZYSOWEGO**	**ORGAN POMOCNICZY**
	Rada Ministrów Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa – (Krajowe centrum zarządzania kryzysowego)	
	Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych (centralne organy administracji rządowej)	Zespół zarządzania kryzysowego	Centrum zarządzania kryzysowego	
	Wojewoda	Wojewódzki zespół zarządzania kryzysowego	Wojewódzkie centrum zarządzania kryzysowego	Komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim
	Starosta	Powiatowy zespół zarządzania kryzysowego	Powiatowe centrum zarządzania kryzysowego	Powiatowa administracja zespolona i jednostki organizacyjne powiatu
	Wójt, burmistrz, prezydent miasta	Gminny zespół zarządzania kryzysowego	Gminne centrum zarządzania kryzysowego	Komórka organizacyjna urzędu gminy (miasta) właściwa w sprawach zarządzania kryzysowego
	Operator infrastruktury krytycznej			Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej

Źródło: Opracowanie własne na podstawie: Ustawa o zarządzaniu kryzysowym Dz. U. 2007 Nr 89 poz. 590, z późn. zmianami - Dz.U. 159 2021

Struktury zarządzania systemem zarządzania kryzysowego obejmują Radę Ministrów, Prezesa Rady Ministrów, Rządowy Zespół Zarządzania Kryzysowego, Rządowe Centrum Bezpieczeństwa, ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych, wojewodów, starostów, wójtów, burmistrzów i prezydentów miast – na rys. Struktura i relacje operacyjne w systemie zarządzania kryzysowego obszar zaznaczony na szaro.

Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Rządowy Zespół Zarządzania Kryzysowego (RZZK) przy Radzie Ministrów jest organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Prezes Rady Ministrów przewodniczy RZZK i nadzoruje Rządowe Centrum Bezpieczeństwa. Rządowe Centrum Bezpieczeństwa (RCB) pełni funkcję krajowego centrum zarządzania kryzysowego, jest kluczowym podmiotem w systemie zarządzania bezpieczeństwem państwa. RCB zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, RZZK i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w ustawie o krajowym systemie cyberbezpieczeństwa. Rada Ministrów lub Prezes Rady Ministrów mogą zlecić Centrum dodatkowe zadania związane z zarządzaniem kryzysowym. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, zgodnie z zakresem swojej właściwości, zadania dotyczące zarządzania kryzysowego. Ministrowie i kierownicy na potrzeby realizacji zadań z zakresu zarządzania kryzysowego tworzą zespoły zarządzania kryzysowego i centra zarządzania kryzysowego[292].

Wojewoda jest organem właściwym w sprawach zarządzania kryzysowego na terenie województwa. Wojewoda wykonuje zadania we współpracy z właściwymi organami administracji publicznej, operuje za pomocą komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim oraz powoływanych wojewódzkiego zespołu zarządzania kryzysowego i wojewódzkiego centrum zarządzania kryzysowego. Zarząd województwa uczestniczy w realizacji zadań z zakresu zarządzania kryzysowego, w tym planowania cywilnego, wynikających z jego kompetencji[293].

[292] tamże, art. 7, 8, 10, 11, 12, 13
[293] tamże, art. 14, 15, 16

Starosta jako przewodniczący zarządu powiatu jest organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu. Starosta wykonuje swoje obowiązki za pomocą powiatowej administracji zespolonej i jednostek organizacyjnych powiatu oraz powoływanych powiatowego zespołu zarządzania kryzysowego i powiatowego centrum zarządzania kryzysowego[294].

Wójt, burmistrz i prezydent miasta są organami właściwymi w sprawach zarządzania kryzysowego na terenie gminy. Zadania wykonują przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego oraz powoływanych gminnego zespołu zarządzania kryzysowego i gminnego centrum zarządzania kryzysowego[295].

Operatorzy infrastruktury krytycznej - właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. Nie są oni zobowiązani i nie tworzą zespołów i centrów zarządzania kryzysowego. Odpowiednikiem organu właściwego może być tu kierownik jednostki organizacyjnej, a organu pomocniczego – wyznaczona, na mocy ustawy, osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej[296].

4.1.2. Struktury i relacje zarządzania bezpieczeństwem na poziomie krajowym

System zarządzania kryzysowego definiuje strukturę i relacje oraz zakres zaangażowania i odpowiedzialności organów i podmiotów systemu zarządzania kryzysowego w ramach działania w zakresie organizacji zarządzania kryzysowego na poziomie krajowym. Organizacja zarządzania na poziomie krajowym odnosi się do realizacji procesów i tworzenia dokumentów zarządczych bezpieczeństwa i cyberbezpieczeństwa na poziomie krajowym, omówionych w rozdziale trzecim. W ramach tej struktury znajdują się organy i podmioty od

[294] tamże, art. 17
[295] tamże, art. 19, 20
[296] tamże, art. 6

poziomu rządowego, przez ministerialny – ministerstwa i urzędy centralne – po poziom administracji samorządowej.

W systemie zarządzania kryzysowego, w ramach zarządzania bezpieczeństwem i cyberbezpieczeństwem poprzez planowanie cywilne, tworzone są dokumenty planowania, organizowania i zarządzania bezpieczeństwem na poziomie krajowym. W ramach tych działań powstają dokumenty zarządcze poziomu krajowego, omówione w rozdziale trzecim, tj.: Krajowy Plan Zarządzania Kryzysowego, Plany Zarządzania Kryzysowego poziomu krajowego – ministerstw i urzędów centralnych – oraz poziomów wojewódzkiego, powiatowego i gminnego, Raport o zagrożeniach bezpieczeństwa narodowego, Narodowy Program Ochrony Infrastruktury Krytycznej.

W realizację procesów i dokumentów zarządczych bezpieczeństwa i cyberbezpieczeństwa na poziomie krajowym i poziomach niższych zaangażowane są organy i podmioty od poziomu rządowego, przez ministerialny – ministerstwa i urzędy centralne – po poziom administracji samorządowej. Struktury zarządzania systemem zarządzania kryzysowego obejmują: Radę Ministrów, Prezesa Rady Ministrów, Rządowy Zespół Zarządzania Kryzysowego, Rządowe Centrum Bezpieczeństwa, Ministrów kierujących działami administracji rządowej, Kierowników urzędów centralnych, Ministra właściwego do spraw administracji publicznej, Ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Pełnomocnika Rządu do spraw Cyberbezpieczeństwa (z zakresie opracowania Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa, mogących doprowadzić do sytuacji kryzysowej), ministrów właściwych w sprawach bezpieczeństwa narodowego, ministrów odpowiedzialnych za systemy IK, wojewodów, starostów, wójtów, burmistrzów i prezydentów miast.

Szczegółowe przedstawienie struktur i relacji organów i podmiotów zarządzania bezpieczeństwem w odniesieniu do procesów i dokumentów organizacji zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym w zarządzaniu kryzysowym przedstawia tabela 24 poniżej.

Tabela 24. Struktury zarządzania bezpieczeństwem w odniesieniu do dokumentów zarządzania bezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego

Struktura dokumentów zarządzania bezpieczeństwem	Struktury zarządzania bezpieczeństwem SZK
Krajowy Plan Zarządzania Kryzysowego (KPZK)	Rada Ministrów Prezes Rady Ministrów Rządowe Centrum Bezpieczeństwa
Raport o zagrożeniach bezpieczeństwa narodowego	Rada Ministrów Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Wojewoda Szef Agencji Bezpieczeństwa Wewnętrznego Pełnomocnik Rządu do spraw Cyberbezpieczeństwa
Plan Zarządzania Kryzysowego (PZK) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych	Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych
Plany Zarządzania Kryzysowego wojewódzkie, powiatowe, gminne	Rządowe Centrum Bezpieczeństwa Minister właściwy do spraw administracji publicznej Minister właściwym ds. wewnętrznych Wojewoda, starosta, wójt, burmistrz i prezydent miasta
Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)	Rada Ministrów Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Ministrowie właściwi ds. bezpieczeństwa narodowego Ministrowie odpowiedzialni za systemy IK

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590

Krajowy Plan Zarządzania Kryzysowego jest przyjmowany przez Radę Ministrów po zaopiniowaniu i przedłożeniu przez Zespół Zarządzania Kryzysowego. Rządowe Centrum Bezpieczeństwa we współpracy z ministrami kierujący działami administracji rządowej i kierownikami urzędów centralnych, odpowiedzialnymi za systemy infrastruktury krytycznej oraz właściwymi w sprawach bezpieczeństwa narodowego opracowuje i aktualizuje KPZK, w tym załącznik funkcjonalny do KPZK. Na załącznik funkcjonalny składają się Plany Zarządzania Kryzysowego uwzględniające opracowywane przez wojewodę wojewódzkie plany zarządzania kryzysowego, uwzględniające i agregujące opracowywane przez starostów oraz wójtów, burmistrzów i prezydentów miast odpowiednio powiatowe i gminne plany zarządzania kryzysowego. Minister właściwy do spraw administracji publicznej

w uzgodnieniu z ministrem właściwym do spraw wewnętrznych po zaopiniowaniu przez dyrektora RCB wydaje wytyczne oraz zatwierdza wojewódzkie plany zarządzania kryzysowego. Prezes Rady Ministrów określa wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w NATO oraz organy odpowiedzialne za ich uruchamianie na podstawie projektu przygotowanego przez RCB i Rządowy Zespół Zarządzania Kryzysowego. Na potrzeby Krajowego Planu Zarządzania Kryzysowego, ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają Raport o zagrożeniach bezpieczeństwa narodowego (Raport), zatwierdzany przez Radę Ministrów. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, natomiast w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, a w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej – Pełnomocnik Rządu do spraw Cyberbezpieczeństwa[297].

Narodowy Program Ochrony Infrastruktury Krytycznej jest przyjmowany przez Radę Ministrów. Dyrektor RCB we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy infrastruktury krytycznej oraz właściwymi w sprawach bezpieczeństwa narodowego, przygotowuje NPOIK oraz sporządza we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy i informuje w tym zakresie ich właścicieli, posiadaczy samoistnych i zależnych (operatorów infrastruktury krytycznej). Wojewodowie, starostowie oraz wójtowie, burmistrze i prezydenci miast organizują i realizują zadania z zakresu ochrony infrastruktury krytycznej. Operatorzy infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. Operatorzy, będący jednocześnie operatorami usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, uwzględniają w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych[298].

[297] tamże
[298] tamże, art. 6

Struktura i relacje zarządzania bezpieczeństwem poziomu krajowego, zakres zaangażowania i odpowiedzialności organów i podmiotów są nieco inne niż struktura i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa.

4.1.3. Struktury i relacje zarządzania sytuacjami kryzysowymi w systemie zarządzania kryzysowego

System zarządzania kryzysowego definiuje strukturę i relacje oraz zakres zaangażowania i odpowiedzialności organów i podmiotów systemu zarządzania kryzysowego w ramach działania w zakresie zapewnienia bezpieczeństwa oraz monitorowania, reagowania i zarządzania sytuacjami kryzysowymi, wynikającymi ze zdarzeń będących incydentami bezpieczeństwa, w tym wynikającymi z incydentów cyberbezpieczeństwa. W działania te zaangażowane są organy i podmioty od poziomu rządowego, przez ministerialny – ministerstwa i urzędy centralne – po poziom administracji samorządowej i operatorów infrastruktury krytycznej. Struktura, relacje, zakres zaangażowania i odpowiedzialności organów i podmiotów zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa i są nieco inne niż w zakresie zarządzania bezpieczeństwem. Struktury zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa tworzą: Prezes Rady Ministrów, Rada Ministrów, Rządowy Zespół Zarządzania Kryzysowego (RZZK), dyrektor Rządowego Centrum Bezpieczeństwa (RCB), Rządowe Centrum Bezpieczeństwa (RCB), ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego, centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych (CZK), kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego, wojewoda, wojewódzki zespół zarządzania kryzysowego (WZZK), starosta, powiatowe centrum zarządzania kryzysowego (PCZK), wójt, burmistrz, prezydent miasta, gminne centrum zarządzania kryzysowego (GCZK), operatorzy infrastruktury krytycznej – właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej (OIK).

Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej. Zwierzchnią rolę w reagowaniu na sytuacje kryzysowe, w tym wynikające z incydentów cyberbezpieczeństwa zajmuje Rządowy Zespół Zarządzania Kryzysowego działający przy Radzie Ministrów, który jako organ opiniodawczo-doradczy właściwy w sprawach

inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego przygotowuje propozycje użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych, doradza w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych, opiniuje sprawozdania końcowe z działań podejmowanych w związku z zarządzaniem kryzysowym, opiniuje potrzeby w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru. Prezes Rady Ministrów Przewodniczy RZZK i nadzoruje Rządowe Centrum Bezpieczeństwa. Dyrektor RCB pełni funkcję sekretarza RZZK[299].

Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego realizują, zgodnie z zakresem swojej właściwości, zadania dotyczące zarządzania kryzysowego, będąc organami właściwymi, są odpowiedzialni za systemy infrastruktury krytycznej, w tym teleinformatyczną infrastrukturę krytyczną.

Wojewoda kieruje monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa wnioskuje o użycie pododdziałów lub oddziałów Sił Zbrojnych RP, doraźnych zgrupowań zadaniowych, Policji, Straży Granicznej lub Państwowej Straży Pożarnej do wykonywania zadań z zakresu zarządzania kryzysowego, zapobiega, przeciwdziała i usuwa skutki zdarzeń o charakterze terrorystycznym, organizuje wykonanie zadań z zakresu ochrony infrastruktury krytycznej. Gromadzi i przetwarza dane oraz ocenia zagrożenia występujące na obszarze województwa, monitoruje, analizuje i prognozuje rozwój zagrożeń na obszarze województwa, dostarcza niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego, zespołu zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz RCB, współpracuje z powiatowymi zespołami zarządzania kryzysowego, zapewnia funkcjonowanie wojewódzkiego zespołu zarządzania kryzysowego, realizuje zadania stałego dyżuru w ramach gotowości obronnej państwa, planuje wsparcie innych organów właściwych w sprawach zarządzania kryzysowego. Wojewódzki Zespół Zarządzania Kryzysowego (WZZK) ocenia występujące i potencjalne zagrożenia mogące mieć wpływ na bezpieczeństwo publiczne i prognozuje te zagrożenia, przygotowuje propozycje działań i przedstawia wojewodzie wnioski dotyczące wykonania, zmiany lub zaniechania działań ujętych w wojewódzkim planie zarządzania kryzysowego, przekazuje do wiadomości publicznej informacje związane z zagrożeniami[300].

[299] tamże
[300] tamże, art. 14

Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują dyrektora RCB o zagrożeniu, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej oraz o konieczności powiadomienia ludności o zagrożeniu[301].

Rządowe Centrum Bezpieczeństwa (RCB) zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, RZZK i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego, pełni funkcję krajowego centrum zarządzania kryzysowego, zapewnia obsługę Zespołu do spraw Incydentów Krytycznych (organu krajowego systemu cyberbezpieczeństwa), monitoruje potencjalne zagrożenia, przygotowuje uruchamianie, w przypadku zaistnienia zagrożeń, procedur związanych z zarządzaniem kryzysowym, przygotowuje projekty opinii i stanowisk RZZK, przygotowuje i obsługuje techniczno-organizacyjnie prace RZZK, zapewnia koordynację polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej, współdziała z podmiotami, komórkami i jednostkami organizacyjnymi NATO i UE oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej, zapewnia obieg informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego, realizuje zadania stałego dyżuru w ramach gotowości obronnej państwa, realizuje zadania z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym, współdziała z centrami zarządzania kryzysowego organów administracji publicznej[302].

Centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych współdziałają na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych, jak również zaburzeń funkcjonowania systemu. Centra zarządzania kryzysowego wszystkich poziomów – ministrów i dyrektorów urzędów centralnych, wojewodów, starostów oraz wójtów, burmistrzów i prezydentów miast pełnią całodobowy dyżur w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego, współdziałają z centrami zarządzania kryzysowego organów administracji publicznej, nadzorują funkcjonowanie systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności,

[301] tamże, art. 21a
[302] tamże, art. 11, art. 11a

współpracują z podmiotami realizującymi monitoring środowiska, współdziałają z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne, realizują zadania stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa[303].

Starostowie, wójtowie, burmistrze i prezydenci miast kierują monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na właściwym terenie, zapobiegają, przeciwdziałają i usuwają skutki zdarzeń o charakterze terrorystycznym, organizują i realizują zadania z zakresu ochrony infrastruktury krytycznej. Powiatowe i gminne zespoły zarządzania kryzysowego oceniają występujące i potencjalne zagrożenia mogące mieć wpływ na bezpieczeństwo publiczne i prognozują te zagrożenia, przygotowują propozycje działań i przedstawiają wnioski dotyczące wykonania, zmiany lub zaniechania działań ujętych w planach zarządzania kryzysowego, przekazują do wiadomości publicznej informacje związane z zagrożeniami[304].

Operatorzy infrastruktury krytycznej mają obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej, w tym teleinformatycznej infrastruktury krytycznej, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia, wyznaczają osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej, w tym teleinformatycznej infrastruktury krytycznej, niezwłocznie informują dyrektora RCB oraz właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej[305].

Szczegółowe przedstawienie struktur i relacji organów i podmiotów zaangażowanych w zarządzanie sytuacjami kryzysowymi, w tym wynikającymi z incydentów cyberbezpieczeństwa, w systemie zarządzania kryzysowego przedstawia rysunek 18.

[303] tamże
[304] tamże
[305] tamże, art. 6, 21a

Rys. 18. Struktury i relacje zarządzania sytuacjami kryzysowymi w systemie zarządzania kryzysowego – model relacji

<table>
<tr><th colspan="5">Struktury i relacje zarządzania sytuacjami kryzysowymi systemu zarządzania kryzysowego</th></tr>
<tr><td></td><td colspan="4">POZIOMY WSPÓŁPRACY</td></tr>
<tr><td rowspan="6">ZWIERZCHNOŚĆ</td><td colspan="2">Rada Ministrów, Prezes Rady Ministrów</td><td colspan="2" rowspan="3"></td></tr>
<tr><td colspan="2">Rządowy Zespół Zarządzania Kryzysowego</td></tr>
<tr><td colspan="2">Dyrektor RCB, RCB</td></tr>
<tr><td>Ministrowie kierujący działami administracji rządowej
Kierownicy urzędów centralnych</td><td>Wojewoda</td><td>Starosta</td><td>Wójt, burmistrz, prezydent miasta</td></tr>
<tr><td>Centrum zarządzania kryzysowego</td><td>Wojewódzkie centrum zarządzania kryzysowego</td><td>Powiatowe centrum zarządzania kryzysowego</td><td>Gminne centrum zarządzania kryzysowego</td></tr>
<tr><td></td><td>Operatorzy infrastruktury krytycznej</td><td></td><td></td></tr>
</table>

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590

Planowanie kryzysowe i zarządzanie sytuacjami kryzysowymi odbywa się od poziomu najniższego do najwyższego, przy czym na każdym wyższym poziomie następuje agregacja planów zarządzania kryzysowego niższego poziomu, a na najwyższym poziomie jest tworzony Krajowy Plan Zarządzania Kryzysowego, a w przypadku reagowania na sytuacje kryzysowe na poziomie niższym są realizowane zadania przypisane danemu poziomowi oraz ta część zadań poziomu wyższego, która dotyczy terytorialnie poziomu niższego. Obowiązek podjęcia działań w zakresie zarządzania kryzysowego w związku z wystąpieniem incydentu, w tym incydentu cyberbezpieczeństwa, mogącego skutkować sytuacją kryzysową spoczywa na tym organie właściwym w sprawach zarządzania kryzysowego, który pierwszy otrzymał informację o wystąpieniu zagrożenia. Organ ten niezwłocznie informuje o zaistniałym zdarzeniu organy odpowiednio wyższego i niższego szczebla, przedstawiając jednocześnie swoją ocenę sytuacji oraz informację o zamierzonych działaniach. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują dyrektora Rządowego Centrum Bezpieczeństwa o zagrożeniu, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej oraz o konieczności powiadomienia ludności o zagrożeniu. Operatorzy infrastruktury krytycznej niezwłocznie informują dyrektora Rządowego Centrum Bezpieczeństwa oraz właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania

tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej[306].

4.1.4. Struktury i relacje operacyjne w krajowym systemie cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa KSC) określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu oraz sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy[307].

Ustawa KSC określa struktury i relacje organów i podmiotów w sprawach funkcjonowania krajowego systemu cyberbezpieczeństwa oraz ich zadania i zasady działania w tej dziedzinie, definiuje również ich struktury i relacje w kontekście zarządzania incydentami cyberbezpieczeństwa.

W strukturach krajowego systemu cyberbezpieczeńatwa jako organy i podmioty występują[308]:

- operatorzy usług kluczowych,
- dostawcy usług cyfrowych,
- CSIRTy poziomu krajowego (CSIRT NASK, CSIRT MON, CSIRT GOV),
- sektorowe zespoły cyberbezpieczeństwa,
- urzędy centralne i podmioty publiczne,
- podmioty świadczące usługi z zakresu cyberbezpieczeństwa,
- organy właściwe do spraw cyberbezpieczeństwa,
- Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa,
- Narodowy Punkt Kontaktowy do współpracy z NATO,
- Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa,
- Kolegium do Spraw Cyberbezpieczeństwa,
- Zespół ds. Incydentów Krytycznych,
- Dyrektor Rządowego Centrum Bezpieczeństwa (RCB),
- Rządowe Centrum Bezpieczeństwa (RCB),
- Minister właściwy ds. informatyzacji,
- Minister obrony narodowej MON.

---

[306] tamże, art. 21, 21a
[307] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt.
[308] tamże, art. 4

Role nie wskazane wprost w Ustawie KSC jako podstawowe, ale występujące jako wspierające i zwierzchnie w systemie bezpieczeństwa państwa to:

- Rada Ministrów,
- Prezes Rady Ministrów,
- Rządowy Zespół Zarządzania Kryzysowego.

Struktura i relacje operacyjne w systemie cyberbezpieczeństwa są wielopoziomowe i wielowymiarowe. W krajowym systemie cyberbezpieczeństwa można zidentyfikować struktury relacji operacyjnych, struktury odpowiedzialne za zarządzanie systemem cyberbezpieczeństwa oraz odmienne struktury zarządzania incydentami cyberbezpieczeństwa[309].

Szczegółowe zobrazowanie struktur i relacji operacyjnych w krajowym systemie cyberbezpieczeństwa przedstawia rysunek 19.

Rys. 19. Struktury i relacje operacyjne krajowego systemu cyberbezpieczeństwa – model relacji

Struktury i relacje operacyjne krajowego systemu cyberbezpieczeństwa			
ZWIERZCHNOŚĆ	*POZIOMY WSPÓŁPRACY*		
	Pełnomocnik Rządu ds. Cyberbezpieczeństwa	Zespół ds. Incydentów Krytycznych	Kolegium ds. cyberbezpieczeństwa
	Minister właściwy ds. informatyzacji		Pojedynczy Punkt Kontaktowy (kontakt z organami państw członkowskich UE)
	Organ właściwy ds. cyberbezpieczeństwa	Minister obrony narodowej MON, Minister właściwy ds. wewnętrznych, ABW	Narodowy Punkt Kontaktowy do współpracy z NATO (prowadzi Minister obrony narodowej MON)
	Sektorowy zespół cyberbezpieczeństwa	CSIRT NASK, CSIRT MON, CSIRT GOV	
	Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa	

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

Struktury odpowiedzialne za zarządzanie krajowym systemem cyberbezpieczeństwa i działania koordynacyjne różnych procesów krajowych i międzynarodowych są częścią cał-

[309] Mąkosa G., *Organizacja systemu cyberbezpieczeństwa*, wyd. cyt., s. 193

kowitej struktury i relacji operacyjnych w systemie. Struktury zarządzania systemem cyberbezpieczeństwa obejmują takie organy jak: Kolegium do Spraw Cyberbezpieczeństwa, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Zespół ds. Incydentów Krytycznych, minister właściwy ds. informatyzacji i organ właściwy ds. cyberbezpieczeństwa – na rys. Struktura i relacje operacyjne krajowego systemu cyberbezpieczeństwa obszar zaznaczony na szaro. Struktury zarządzania nie obejmują podmiotów poziomu operacyjnego - zespołów cyberbezpieczeństwa i podmiotów realizujących usługi kluczowe, cyfrowe i publiczne.

Zwierzchnią rolę w systemie bezpieczeństwa państwa zajmuje Rada Ministrów. Przy Radzie Ministrów działa Kolegium ds. cyberbezpieczeństwa (Kolegium) jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. Do zadań Kolegium należy opracowywanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz wyrażanie opinii w sprawach kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa, wykonywania przez CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa i organy właściwe powierzonych im zadań, współdziałania organów prowadzących lub nadzorujących CSIRTy oraz współpracy z organami bezpieczeństwa, organizacji wymiany informacji istotnych dla cyberbezpieczeństwa RP, wniosków ws. rekomendacji stosowania sprzętu i oprogramowania[310].

Kluczową rolę w krajowym systemie cyberbezpieczeństwa zajmuje Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (Pełnomocnik), któremu Prezes Rady Ministrów powierzył koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Do zadań Pełnomocnika należy analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV, opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa, upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym, inicjowanie krajowych

[310] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 65

ćwiczeń w zakresie cyberbezpieczeństwa, wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT. Do zadań Pełnomocnika wykonywanych w porozumieniu z właściwymi ministrami należy również współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi, podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa, podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu. Pełnomocnik może przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie. Pełnomocnik koordynuje przygotowanie Raportu zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej[311].

Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z NATO w zakresie współpracy w zapewnieniu cyberbezpieczeństwa RP. Minister Obrony Narodowej jest odpowiedzialny za współpracę Sił Zbrojnych RP z właściwymi organami NATO, UE i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa, zapewnienie zdolności Siłom Zbrojnym w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych, rozwijanie umiejętności Sił Zbrojnych w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych, pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej, kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego, ocenę wpływu incydentów na system obrony państwa, ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych oraz koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa[312].

[311] tamże, art. 60, 61, 62, 63
[312] tamże, art. 51, 52

Minister właściwy do spraw informatyzacji prowadzi Pojedynczy Punkt Kontaktowy, do którego zadań należy m.in. komunikacja w zakresie zgłoszeń incydentów poważnych lub incydentów istotnych dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej pomiędzy pojedynczymi punktami kontaktowymi w innych państwach członkowskich Unii Europejskiej, a CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowymi zespołami cyberbezpieczeństwa, zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT, zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa, koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej[313].

Minister właściwy ds. informatyzacji prowadzi wykaz operatorów usług kluczowych. Minister jest odpowiedzialny za monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizację planów działań na rzecz jej wdrożenia, rekomendowanie obszarów współpracy z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa, opracowywanie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez operatorów usług kluczowych i incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników, gromadzenie informacji o incydentach poważnych, które dotyczą lub zostały przekazane przez inne państwo członkowskie Unii Europejskiej, udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych[314].

Zespoły Reagowania na Incydenty Komputerowe poziomu krajowego (CSIRT NASK, CSIRT MON, CSIRT GOV) są podległe ich właściwym organom zwierzchnim, tzn. odpowiednio CSIRT GOV - ministrowi właściwemu ds. informatyzacji, CSIRT MON - Ministrowi Obrony Narodowej, CSIRT GOV - Szefowi ABW i dalej ministrowi właściwemu ds. wewnętrznych (Ministrowi SWiA)[315].

[313] tamże, art. 48
[314] tamże
[315] tamże

Operatorzy usług kluczowy i dostawcy usług cyfrowych oraz wskazane urzędy centralne i podmioty publiczne są podstawowymi podmiotami systemu cyberbezpieczeństwa. Są one nadzorowane przez organy właściwe ds. cyberbezpieczeństwa, którymi są właściwi ministrowie, odpowiednio do sektorów, do których zaliczane są te podmioty. Organ właściwy ds. cyberbezpieczeństwa powołuje i nadzoruje sektorowy zespół cyberbezpieczeństwa. Operatorzy usług kluczowych mogą zawierać umowy dotyczące bezpieczeństwa swoich systemów teleinformatycznych z podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa, które są wyspecjalizowanymi w tym zakresie podmiotami. Minister właściwy ds. informatyzacji nadzoruje podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

4.1.5. Struktury i relacje zarządzania cyberbezpieczeństwem poziomu krajowego

Krajowy system cyberbezpieczeństwa, który ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów, nie posiada w swojej strukturze rozwiązania organizacyjnego zarządzania cyberbezpieczeństwem na poziomie krajowym ani dokumentów planowania i zarządzania cyberbezpieczeństwem poziomu krajowego. W zakresie formalnych działań dotyczących organizacji cyberbezpieczeństwa na poziomie krajowym Pełnomocnik Rządu do spraw Cyberbezpieczeństwa (Pełnomocnik) przygotowuje Raport o zagrożeniach bezpieczeństwa narodowego (Raport) w części dotyczącej zagrożeń cyberbezpieczeństwa, mogących doprowadzić do sytuacji kryzysowej, opracowywany w ramach planowania cywilnego, realizowanego w systemie zarządzania kryzysowego, na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego. Raport jest więc dokumentem systemu zarządzania kryzysowego, a nie systemu cyberbezpieczeństwa.

4.1.6. Struktury i relacje zarządzania incydentami cyberbezpieczeństwa w krajowym systemie cyberbezpieczeństwa

W krajowym systemie cyberbezpieczeństwa ustanowiono struktury i relacje organów i podmiotów systemu dla zarządzania incydentami cyberbezpieczeństwa. Struktury i relacje

te są rozbudowane i obejmują organy i podmioty od poziomu rządowego, poprzez ministerialny do poziomu podmiotów gospodarczych i publicznych operujących na najniższym poziomie. Struktura zarządzania incydentami cyberbezpieczeństwa obejmuje – Zespół ds. Incydentów Krytycznych, Pojedynczy Punkt Kontaktowy - dedykowany obsłudze incydentów transgranicznych, Rządowe Centrum Bezpieczeństwa, Ministra właściwego ds. informatyzacji, ministrów - organy właściwe ds. cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa, operatorów usług kluczowych, dostawców usług cyfrowych, podmioty publiczne oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

Szczegółowe zobrazowanie struktur i relacji w zakresie zarządzania incydentami cyberbezpieczeństwa w krajowym systemie cyberbezpieczeństwa przedstawia rysunek 20.

Rys. 20. Struktury i relacje zarządzania incydentami cyberbezpieczeństwa – model relacji

Struktury i relacje zarządzania incydentami cyberbezpieczeństwa					
	POZIOMY WSPÓŁPRACY				
ZWIERZCHNOŚĆ	Zespół ds. Incydentów Krytycznych	Pojedynczy Punkt Kontaktowy			
	CSIRT MON, CSIRT NASK, CSIRT GOV	Sektorowy zespół cyberbezpieczeństwa	Organ właściwy ds. cyberbezpieczeństwa	Minister właściwy ds. informatyzacji	Pełnomocnik Rządu ds. Cyberbezpieczeństwa
	Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa			

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

Zwierzchnią rolę w zarządzaniu incydentami cyberbezpieczeństwa pełni Rządowy Zespół Zarządzania Kryzysowego działający przy Radzie Ministrów jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej, w tym zarządzanie cyberbezpieczeństwem[316].

[316] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt.

Zespół do spraw Incydentów Krytycznych (Zespół) jest organem pomocniczym w sprawach obsługi incydentów krytycznych cyberbezpieczeństwa zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa. Dyrektor Rządowego Centrum Bezpieczeństwa przewodniczy pracom Zespołu. Obsługę prac Zespołu zapewnia RCB. Zespół wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, określa sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub CSIRT GOV, podejmuje decyzję o wystąpieniu przez dyrektora Rządowego Centrum Bezpieczeństwa z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego. W przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego. Organem pomocniczym Zespołu ds. Incydentów Krytycznych jest Pojedynczy Punkt Kontaktowy[317].

CSIRTy poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV) współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV należy m.in. monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, szacowanie ryzyka z nimi związanego, przekazywanie informacji o zagrożeniach, incydentach i ryzykach podmiotom krajowego systemu cyberbezpieczeństwa, zarządzanie incydentami – reagowanie, klasyfikowanie oraz koordynowanie obsługi incydentów krytycznych, w tym współpraca z sektorowymi zespołami cyberbezpieczeństwa. Do zadań CSIRTów należy również opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, dotyczącej cyberbezpieczeństwa, zapewnianie zaplecza analitycznego

[317] tamże, art. 36

oraz badawczo-rozwojowego cyberbezpieczeństwa, opracowywanie procedur koordynowanej obsługi incydentów wymagającej współpracy CSIRT i sektorowych zespołów cyberbezpieczeństwa[318]. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym oraz informują o nim Rządowe Centrum Bezpieczeństwa. Informacja powinna zawierać wstępną analizę potencjalnych skutków incydentu oraz ewentualnie rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego lub wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych[319].

Organ właściwy do spraw cyberbezpieczeństwa może ustanowić sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora odpowiedzialny w szczególności za przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów, wspieranie operatorów usług kluczowych w wykonywaniu ich obowiązków, analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu oraz za współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Podmioty będące operatorami usług kluczowy, dostawcami usług cyfrowych i podmiotami publicznymi realizują zadania zapewnienia bezpieczeństwa swoich systemów teleinformatycznych oraz obsługi incydentów cyberbezpieczeństwa.

Operatorzy usług kluczowych prowadzą systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem oraz wdrażają odpowiednie i proporcjonalne do oszacowanego ryzyka środki techniczne i organizacyjne bezpieczeństwa, zbierają informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zarządzają incydentami, stosują środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, stosują środki łączności umożliwiające prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa. Operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Operator usługi kluczowej zapewnia obsługę incydentu, zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań, klasyfikuje incydent jako poważny i zgłasza do właściwego CSIRT, współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub

[318] tamże, art. 26
[319] tamże, art. 35

CSIRT GOV, przekazując niezbędne dane, usuwa podatności oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa. Operator usługi kluczowej może przekazywać do właściwego CSIRT informacje o innych incydentach, o zagrożeniach cyberbezpieczeństwa, dotyczące szacowania ryzyka, o podatnościach, o wykorzystywanych technologiach. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej współdziała z tym zespołem na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane i zapewnia mu dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań[320].

Dostawca usługi cyfrowej podejmuje właściwe i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te mają zapewnić cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz mają uwzględniać bezpieczeństwo systemów informacyjnych i obiektów, postępowanie w przypadku obsługi incydentu, zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej, monitorowanie, audyt i testowanie, najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi. Dostawca usługi cyfrowej podejmuje środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi. Dostawca usługi cyfrowej przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów, zapewnia w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT poziomu krajowego o incydentach zakwalifikowanych jako krytyczne, klasyfikuje incydent jako istotny, zgłasza incydent istotny do właściwego CSIRT poziomu krajowego, zapewnia obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane, usuwa podatności, przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora[321].

Podmiot publiczny zapewnia zarządzanie incydentem w podmiocie publicznym, zgłasza incydent w podmiocie publicznym do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe, zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do

[320] tamże, art. 8, 10, 11, 13
[321] tamże, art. 17, 18

wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami[322].

4.1.7. Struktury i relacje operacyjne w systemie informatyzacji podmiotów realizujących zadania publiczne

W systemie informatyzacji podmiotów realizujących zadania publiczne nie zastały zdefiniowane struktury i relacje w kontekście zarządzania bezpieczeństwem oraz zarządzania sytuacjami kryzysowymi incydentami cyberbezpieczeństwa dotyczącymi systemów teleinformatycznych wykorzystywanych do realizacji usług i zadań publicznych.

4.2. Analiza porównawcza rozwiązań w systemie cyberbezpieczeństwa RP

W zakresie analizy porównawczej należy rozważyć struktury i relacje operacyjne w zakresie organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym oraz w zakresie zarządzania sytuacjami kryzysowymi, w tym wynikającymi z incydentów cyberbezpieczeństwa, i incydentami cyberbezpieczeństwa.

4.2.1. Analiza porównawcza struktur i relacji operacyjnych zarządzania bezpieczeństwem

Zarządzanie operacyjne bezpieczeństwem w aspekcie zarządzania kryzysowego i zarządzania cyberbezpieczeństwem angażuje zgoła odmienne struktury organów i podmiotów. W systemie zarządzania kryzysowego jest to szeroki zakres, budujący złożoną strukturę zależności i relacji. W krajowym systemie cyberbezpieczeństwa skupiono się głównie na procesach zarządzania incydentami cyberbezpieczeństwa oraz relacjami z odpowiednimi organami ds. cyberbezpieczeństwa w Unii Europejskiej.

Szczegółowe przedstawienie struktur i relacji operacyjnych organów i podmiotów zarządzania bezpieczeństwem w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa w ujęciu porównawczym zawiera tabela 25 poniżej.

[322] tamże, art. 22

Tabela 25. Struktury i relacje operacyjne systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa

Struktury i relacje operacyjne – ujęcie porównawcze	
Struktury operacyjne systemu zarządzania kryzysowego (SZK)	**Struktury operacyjne krajowego systemu cyberbezpieczeństwa (KSC)**
Rada Ministrów	-
Prezes Rady Ministrów	-
Rządowy Zespół Zarządzania Kryzysowego (RZZK)	-
	Kolegium do Spraw Cyberbezpieczeństwa
	Zespół ds. Incydentów Krytycznych
	Pojedynczy Punkt Kontaktowy
	Narodowy Punkt Kontaktowy do współpracy z NATO
Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)
Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB)
Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego	Organ właściwy ds. cyberbezpieczeństwa Minister właściwy ds. informatyzacji Minister obrony narodowej MON
Centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych (CZK)	CSIRT MON, CSIRT NASK, CSIRT GOV Sektorowy zespół cyberbezpieczeństwa
Zespoły zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych (ZZK)	
Szef Agencji Bezpieczeństwa Wewnętrznego	*Szef Agencji Bezpieczeństwa Wewnętrznego*
Pełnomocnik Rządu do spraw Cyberbezpieczeństwa	Pełnomocnik Rządu do spraw Cyberbezpieczeństwa
Minister właściwy ds. wewnętrznych Minister właściwy do spraw administracji publicznej	
kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego	
Wojewoda	
Komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim	
Wojewódzki zespół zarządzania kryzysowego	
Wojewódzkie centrum zarządzania kryzysowego	
Starosta	
Powiatowy zespół zarządzania kryzysowego	

Powiatowe centra zarządzania kryzysowego	
Wójt, burmistrz, prezydent miasta	
Gminny zespół zarządzania kryzysowego	
	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa
Operator infrastruktury krytycznej	Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

4.2.2. Analiza porównawcza struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym

Proces zarządzania bezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego jest rozwinięty i dojrzały. W jego ramach wytwarzane są dokumenty organizacji zarządzania bezpieczeństwem i cyberbezpieczeństwem, które są materializacją procesów zarządczych. W proces zarządzania i wytwarzania dokumentów zaangażowane są podmioty całej struktury zarządzania państwa – od poziomu rządowego, przez ministerstwa i urzędu centralne, po administrację samorządową.

W krajowym systemie cyberbezpieczeństwa nie ustanowiono procesu zarządzania na poziomie krajowym, nie powstają więc żadne dokumenty zarządcze poziomu krajowego, a w związku z tym nie ma zaangażowanych organów, podmiotów ani ich struktur.

Szczegółowe przedstawienie struktur i relacji organów i podmiotów zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do procesów i dokumentów zarządczych bezpieczeństwa i cyberbezpieczeństwa na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa w ujęciu porównawczym zawiera tabela 26 poniżej.

Tabela 26. Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa

System zarządzania kryzysowego (SZK)		Krajowy system cyberbezpieczeństwa (KSC)	
Struktura dokumentów zarządzania bezpieczeństwem	**Struktury zarządzania bezpieczeństwem**	**Struktura dokumentów zarządzania cyberbezpieczeństwem**	**Struktury zarządzania cyberbezpeczeństwem**
Krajowy Plan Zarządzania Kryzysowego (KPZK)	Rada Ministrów Prezes Rady Ministrów Rządowe Centrum Bezpieczeństwa	-	-
Raport o zagrożeniach bezpieczeństwa narodowego	Rada Ministrów Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów -centralnych Wojewoda Szef Agencji Bezpieczeństwa Wewnętrznego Pełnomocnik Rządu do spraw Cyberbezpieczeństwa	-	-
Plan Zarządzania Kryzysowego (PZK) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych	Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych	-	-
Plany Zarządzania Kryzysowego wojewódzkie, powiatowe, gminne	Rządowe Centrum Bezpieczeństwa Minister właściwy do spraw administracji publicznej Minister właściwym do spraw wewnętrznych Wojewoda, starosta, wójt, burmistrz i prezydent miasta	-	-
Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)	Rada Ministrów Rządowe Centrum Bezpieczeństwa Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Ministrowie właściwi w sprawach bezpieczeństwa narodowego Ministrowie odpowiedzialni za systemy IK	-	-

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

Z powyższego zestawienia podmiotów zaangażowanych w realizację procesów zarządzania cyberbezpieczeństwem i wytwarzania dokumentów zarządczych, przypisanych do poszczególnych faz zarządzania, wyrażonych w generowanych dokumentach, można zidentyfikować strukturę podmiotów generalnie zaangażowanych w proces w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa

Tym, co łączy oba systemy na tak wysokim poziomie planowania bezpieczeństwa, to Raport o zagrożeniach bezpieczeństwa narodowego, przygotowywany w obu systemach (zarządzania kryzysowego i cyberbezpieczeństwa) na potrzeby Krajowego Planu Zarządzania Kryzysowego przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów. Raport jest więc dokumentem systemu zarządzania kryzysowego, a nie systemu cyberbezpieczeństwa. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, natomiast w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, a w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej – Pełnomocnik Rządu do spraw Cyberbezpieczeństwa. W ten sposób krajowy system cyberbezpieczeństwa łączy się z systemem zarządzania kryzysowego, ale tylko w odniesieniu do systemów teleinformatycznych infrastruktury krytycznej. Niestety, jest to połączenie punktowe i zdaje się, że zbyt słabe, aby system bezpieczeństwa był skuteczny, silny i zwarty. Takie działanie formalnie nie obejmuje systemów teleinformatycznych służących do świadczenia usług cyfrowych ani usług kluczowych, choć w praktyce duża część podmiotów je realizujących (dostawców usług kluczowych), to operatorzy infrastruktury krytycznej. Niemniej jednak podmioty niebędące operatorami infrastruktury krytycznej, a będące podmiotami krajowego systemu cyberbezpieczeństwa, pozostają poza zakresem Krajowego Planu Zarządzania Kryzysowego i tym samym poza krajowym systemem zarządzania bezpieczeństwem[323].

4.2.3. Analiza porównawcza struktur i relacji zarządzania incydentami cyberbezpieczeństwa

Proces zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa w obu systemach bezpieczeństwa - systemie zarządzania kryzysowego i krajowym systemie

[323] Mąkosa G., *Organizacja systemu cyberbezpieczeństwa, wyd. cyt.*, s. 185

cyberbezpieczeństwa – ma znaczące różnice, jak i podobieństwa, a także angażuje różne organy i podmioty, tworzące różne struktury i relacje operacyjne.

System zarządzania kryzysowego i krajowy system cyberbezpieczeństwa definiują struktury i relacje oraz zakresy zaangażowania i odpowiedzialności organów i podmiotów tych systemów w ramach działania w zakresie zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa. W działania te zaangażowane są organy i podmioty od poziomu rządowego, przez ministerialny – po poziom podmiotów gospodarczych i publicznych, tj. operatorów infrastruktury krytycznej (w systemie zarządzania kryzysowego) czy operatorów usług kluczowych, dostawców usług cyfrowych i podmioty publiczne (w krajowym systemie cyberbezpieczeństwa).

Szczegółowe zestawienie struktur i relacji zaangażowania i odpowiedzialności organów i podmiotów systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w ramach działania w zakresie zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa przedstawione jest w tabeli 27.

Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Rządowy Zespół Zarządzania Kryzysowego (RZZK) przy Radzie Ministrów jest organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Prezes Rady Ministrów przewodniczy RZZK i nadzoruje Rządowe Centrum Bezpieczeństwa[324]. Te organy ich role zostały zdefiniowane w ramach systemu zarządzani kryzysowego. Krajowy system cyberbezpieczeństwa nie wskazuje wprost odwołania do tych organów, ale jako wskazanie możliwości skierowania wniosku przez RCB do Rady Ministrów o zwołanie RZZK i Zespołu ds. Incydentów Krytycznych w sytuacji obsługi incydentu krytycznego cyberbezpieczeństwa, która by tego wymagała. Zespół ds. Incydentów Krytycznych jest organem najwyżej umocowanym, zdefiniowanym w Ustawie KSC. Jest to z perspektywy systemu cyberbezpieczeństwa uznanie wyższości i ważniejszości organów ustanowionych w systemie zarządzania kryzysowego, jako systemu zarządzania bezpieczeństwem państwa.

[324] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 7, 8, 10

Tabela 27. Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa – ujęcie porównawcze

Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa – ujęcie porównawcze	
Struktury zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego (SZK)	**Struktury zarządzania incydentami cyberbezpieczeństwa krajowego systemu cyberbezpieczeństwa (KSC)**
Rada Ministrów	-
Prezes Rady Ministrów	-
Rządowy Zespół Zarządzania Kryzysowego (RZZK)	-
	Zespół ds. Incydentów Krytycznych
	Pojedynczy Punkt Kontaktowy
Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)
Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB)
Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego	Organ właściwy ds. cyberbezpieczeństwa Minister właściwy ds. informatyzacji Minister obrony narodowej MON
Centrum zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych	CSIRT MON, CSIRT NASK, CSIRT GOV Sektorowy zespół cyberbezpieczeństwa
Szef Agencji Bezpieczeństwa Wewnętrznego	*Szef Agencji Bezpieczeństwa Wewnętrznego*
Minister właściwy do spraw administracji publicznej	
Wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK), wojewódzkie centrum zarządzania kryzysowego (WCZK)	
Starosta, powiatowy zespół zarządzania kryzysowego (PZZK), powiatowe centra zarządzania kryzysowego (PCZK)	
Wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego	
	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa
Operator infrastruktury krytycznej	Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny

Źródło: opracowanie własne na podstawie: 1. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 Nr 89 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

W systemie zarządzania kryzysowego Rządowe Centrum Bezpieczeństwa (RCB) pełni funkcję krajowego centrum zarządzania kryzysowego, jest kluczowym podmiotem w systemie zarządzania bezpieczeństwem państwa. RCB zapewnia również obsługę Rady Ministrów, Prezesa Rady Ministrów, RZZK i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w ustawie o krajowym systemie cyberbezpieczeństwa[325]. W krajowym systemie cyberbezpieczeństwa RCB wspólnie z CSIRTami poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV), sektorowymi zespołami cyberbezpieczeństwa, organami właściwymi ds. cyberbezpieczeństwa, ministrem właściwy ds. informatyzacji, Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa zarządza incydentami krytycznymi. Jest organem wnioskującym do Rady Ministrów z zwołanie RZZK i Zespołu ds. Incydentów Krytycznych na wniosek CSIRTów.

W kontekście zarządzania incydentami i sytuacjami kryzysowymi – w systemie zarządzania kryzysowego RCB jest kluczowym podmiotem w systemie zarządzania bezpieczeństwem państwa, pełni funkcję krajowego centrum zarządzania kryzysowego, współpracuje z centrami zarządzani kryzysowego ministrów i urzędów centralnych, wojewódzkimi, powiatowymi i gminnymi centrami zarządzani kryzysowego oraz innymi organami i operatorami infrastruktury krytycznej. W krajowym systemie cyberbezpieczeństwa RCB jest tylko organem współpracującym w zarządzaniu incydentami krytycznymi. Rozbudowaną, koordynacyjną rolę w zarządzaniu incydentami pełnią CSITy poziomu krajowego (CSIRT NASK, CSIRT, GOV, CSIRT MON), których rola i zakres odpowiedzialności mogą być zbliżone do roli i zadań RCB w zarządzaniu sytuacjami kryzysowymi. CSIRTy bezpośrednio współpracują przy obsłudze incydentów z sektorowymi zespołami cyberbezpieczeństwa i operatorami usług kluczowych, dostawcami usług cyfrowych i podmiotami publicznymi, wydają rekomendacje i wskazówki, prowadzą badania bezpieczeństwa systemów teleinformatycznych oraz wnioskują do RCB o zwołanie Zespołu ds. Incydentów Krytycznych i RZZK.

Warto również zwrócić uwagę na czas angażowania Rządowego Centrum Bezpieczeństwa w zarządzanie incydentami i sytuacjami kryzysowymi i miejsce RCB w strukturach zarządzania. W systemie zarządzania kryzysowego ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują dyrektora RCB o zagrożeniu, które może skutkować wystąpieniem na wskazanym

[325] tamże, art. 11

obszarze sytuacji kryzysowej oraz o konieczności powiadomienia ludności o zagrożeniu. Również operatorzy infrastruktury krytycznej niezwłocznie informują dyrektora RCB oraz właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej. W krajowym systemie cyberbezpieczeństwa CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym i o zagrożeniach cyberbezpieczeństwa oraz informują RCB. Tak więc w systemie zarządzania kryzysowego RCB jest informowane o zakłóceniach i zagrożeniach już od operatora, czyli jest to komunikacja i zaangażowanie bezpośrednie, dalej jest komunikacja z wojewodami, kierownikami urzędów centralnych i ministrami. W systemie cyberbezpieczeństwa RCB jest informowane przez CSIRTy o incydentach uznanych już przez nie za krytyczne i w sytuacji, gdy zarządzanie takimi incydentami wymaga koordynowanej pracy Zespołu ds. Incydentów Krytycznych. Jest to więc komunikacja do i zaangażowanie RCB na znacznie późniejszym etapie[326].

Należy zwrócić uwagę, że struktura zarządzania incydentami w krajowym systemie cyberbezpieczeństwa nie obejmuje struktur administracji publicznej, odpowiedzialnej za reagowanie na sytuacje kryzysowe i zarządzanie kryzysowe. W proces nie zostali zaangażowani, ani nawet nie są informowani wojewodowie, starostowie, wójtowie, burmistrzowie i prezydenci miast oraz zespoły zarządzania kryzysowego, centra zarządzania kryzysowego poziomów wojewódzkiego, powiatowego i gminnego. Uwzględniając fakt, że incydenty bezpieczeństwa infrastruktury teleinformatycznej negatywnie wpływają na funkcjonowanie usług i systemów infrastruktury krytycznej wywołując sytuacje kryzysowe, za których obsługę odpowiedzialne są właśnie te struktury, wydaje się koniecznym uwzględnienie ich w procesie obsługi incydentów w systemie cyberbezpieczeństwa[327].

W obu systemach bezpieczeństwa organami właściwymi są ministrowie nadzorujący działy administracji, w ramach których zostały zdefiniowane systemy infrastruktury krytycznej w zarządzaniu kryzysowych i sektory w systemie cyberbezpieczeństwa.

W obu systemach bezpieczeństwa podmiotami działającymi na najniższym, operacyjnym poziomie, zapewniającymi bezpieczeństwo usług publicznych i bezpośrednio obsługującymi sytuacje kryzysowe i incydenty cyberbezpieczeństwa są właściciele systemów te-

[326] Mąkosa G., *Organizacja systemu cyberbezpieczeństwa*, wyd. cyt., s. 200, 201
[327] tamże, s. 200

leinformatycznych wspierających działanie tych usług. W systemie zarządzania kryzysowego są to operatorzy infrastruktury krytycznej, w krajowym systemie cyberbezpieczeństwa są to operatorzy usług kluczowych, dostawcy usług cyfrowych i podmioty publiczne.

Zdaniem autora zasadnym jest, zgodnie ze zdefiniowaną hipotezą, dotyczącą przedmiotowych zagadnień niniejszego rozdziału, ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym i zarządzania incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w celu zapewnienia efektywności operacyjnej systemu cyberbezpieczeństwa RP i odpowiedniego poziomu bezpieczeństwa państwa.

4.3. Wyniki przeprowadzonych badań

W ramach procesu badawczego, realizowanego w zakresie zagadnienia zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, stanowiącym przedmiotową problematykę niniejszego rozdziału, poddano weryfikacji hipotezę autora brzmiącą:

Ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa,

sformułowaną jako odpowiedź na postawione pytanie badawcze:

Jakie są aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić ich efektywność?

W celu znalezienia odpowiedzi na postawione pytanie badawcze oraz zweryfikowania sformułowanej hipotezy, w procesie badawczym zostały postawione respondentom – ekspertom pytania, jak niżej:

2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?
   2.1. *Struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regional-*

nym (wojewódzkim, powiatowym, gminnym) i sektorowym są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

2.2. *Struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego.*

2.3. *Struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji.*

2.4. *Proponowane w pkt. 2.3. powyżej zaangażowanie RCB w zarządzanie cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób:*

1) *RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym;*
2) *RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzy-*

sowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego;

3) *RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa.*

2.5. *Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.*

2.6. *CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych.*

W wyniku przeprowadzonego badania uzyskano od respondentów – ekspertów szereg odpowiedzi na postawione pytania. Analiza uzyskanych odpowiedzi na poszczególne pytania, wyrażone w tezach w nich zawartych, została przestawiona i omówiona poniżej tekście niniejszego podrozdziału.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2.

Wynik badania w zakresie pytania 2.1.

Wobec tezy pytania 2.1.,

Struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regionalnym (wojewódz-

kim, powiatowym, gminnym) i sektorowym są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa,

spośród udzielonych przez respondentów odpowiedzi, 15 (34,09%) osób wyraziło zgodę z tezą, przy czym zdecydowana większość (12) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana. W udzielonych odpowiedziach 22 (50,00%) osób nie zgodziło się z tezą, przy czym zdecydowana większość (16) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci nie zgadzają się, a ściślej, raczej się nie zgadzają, z tezą pytania.

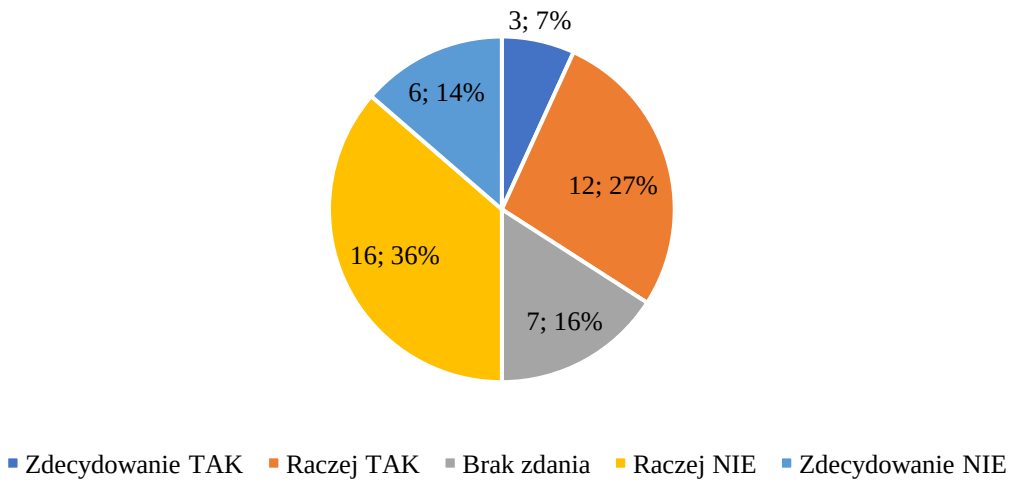
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi odpowiedzi uzyskanymi w badaniu. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 28 i na rysunku 21.

Tabela 28. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.1.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	44	15 / 22	3	12	7	16	6
%	100	34,09 / 50,00	6,82	27,27	15,91	36,36	13,64

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 21. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.1.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie ujawnia stanowisko większości respondentów. Uważają oni, że struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym nie są właściwie zdefiniowane i nie zapewniają efektywność krajowego systemu cyberbezpieczeństwa. Wynik badania w powyższym zakresie wskazuje na konieczność wskazania konkretnych podmiotów instytucjonalnych i organów odpowiedzialnych za planowanie i zarządzanie cyberbezpieczeństwem na poziomie krajowym. Szczególnie należy uwzględnić fakt wykazany w przeprowadzonej analizie w tym zakresie, że krajowy system cyberbezpieczeństwa nie posiada w swojej strukturze żadnych instytucji i organów odpowiedzialnych za zarządzanie cyberbezpieczeństwem poziomu krajowego.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów, przedstawione w uzupełnieniu do wyboru opcji odpowiedzi, często odnoszą się do różnych aspektów działania i współdziałania struktur i relacji operacyjnych zarządzania kryzowego i cyberbezpieczeństwa, czasami również do funkcjonowania rozwiązań cyberbezpieczeństwa w strukturach regionalnych i bezpośrednio podmiotach. Dominują treści bezpośrednio dotyczące pytania, zdarzają się także takie, które dotyczą zagadnień powiązanych lub dalszych problemowo. W tak szerokim spektrum treści należy uwzględnić odniesienie do problematyki pytania. Poniżej przedstawiono zestawione argumenty, opinie i komentarze respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** wskazują, że system jest zdefiniowany prawidłowo, ponieważ został stworzony na podstawie dobrze wypracowanej Dyrektywy NIS, rozwiązania organizacyjne są dobrze zaprojektowane i funkcjonalnie sprawne, właściwie funkcjonują powołane struktury, którym wskazano ich zadania i obowiązki, co pozwala na zapewnienie efektywności krajowego systemu cyberbezpieczeństwa, w szczególności w zakresie obsługi incydentów. Zwrócono uwagę, że każdym szczeblu, w szczególności na najwyższym poziomie, są jasno określone podmioty, kompetencje i zasady współpracy, obejmujące również infrastrukturę krytyczną. Respondenci podnoszą, że same struktury opisane są względnie dobrze, gorzej z relacjami między nimi. Zwracają uwagę, na konieczność koordynacji realizacji zadań i współpracy między różnymi sektorami i podmiotami oraz na utrzymanie lub ulepszenie sektorowej i międzysektorowej wymiany wiedzy o incydentach. Wskazano również, że brakuje średniego szczebla (operacyjnego) na wzór BSI lub ANSSI

w krajach zachodnich, ale obecnie te zadania są realizowane przez inne podmioty i nie wpływa to na ogólny poziom bezpieczeństwa.

Respondenci **nie zgadzający się z tezą pytania** podnoszą, że zarządzanie cyberbezpieczeństwem w formie obecnej wydaje się koncentrować na praktykach spełniania wymogów zgodności oraz prezentowania wyników operacyjnych w ujęciu ilościowym, a nie jakościowym. System głównie funkcjonuje na zasadzie realizacji wymaganych prawem dokumentacji oraz współpracy opartej na relacjach osobistych a nie służbowych. Struktury organizacyjne i relacje operacyjne nie zapewniają efektywności KSC, struktury działają reaktywnie. Występujący rozdział kompetencji na najwyższym poziomie (CSIRT krajowych) przekłada się na rozdźwięk działań na niższych poziomach i w efekcie wprowadza podatności systemowe. Respondenci zauważają, że na poziomie ministerialnym widać współpracę, jednak nawet na tym poziomie jednostki podległe MON i pozostałe działają odrębnie i bez widocznej współpracy. Na poziomie wojewódzkim i niżej nie ma w zasadzie żadnej koordynacji. Nie ma też pomocy Państwa dla podmiotów komercyjnych zaangażowanych w system cyberbezpieczeństwa, te podmioty, które mają wyższy poziom świadomości co do cyberzagrożeń samodzielnie próbują tworzyć i wdrażać strategie cyberbezpieczeństwa. W systemie powołano CSIRT-y krajowe, natomiast nie powołano CSIRTów sektorowych, co przy niespójności sektorów w ustawach o KSC i ZK powoduje chaos kompetencyjny i problemy z przepływem informacji. Nie istnieją sektorowe czy regionalne „profile bezpieczeństwa", brak jest komunikacji ryzyk i zagrożeń, brak koordynacji alertów i informacji wywiadu cybernetycznego na poziomie jednostek, ciągła rywalizacja zespołów CERT/CSIRT zamiast współpracy i współdzielenia informacji. Wskazują na brak znaczącej współpracy w sektorach i regionach, i słabą wymianę informacji o incydentach i słabościach, pomimo sporadycznych akcje przeprowadzanych przez CERT/CSIRT i sektorowych spotkań/konferencji. Respondenci wskazują rozwiązania, takie jak scentralizowany, efektywny i merytoryczny nadzór operacyjny, np. RCB, nad wszystkimi interesariuszami systemu, zwiększenie roli wojewody w zakresie organizacyjnym, kontrolnym oraz możliwości egzekwowania, włączenie regionalnych struktur cyberbezpieczeństwa policji lub ewentualnie dedykowanych CUW na poziomie regionalnym.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.1.

Autor rozprawy podziela dominujące zdanie respondentów i również nie zgadza się z przedstawioną w pytaniu tezą. Zdaniem autora struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym,

ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym nie zostały właściwie zdefiniowane, nie uwzględniono podmiotów odgrywających istotne role w systemie zarządzania kryzysowego, funkcjonującego również w celu zapewnienia bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych wspierających działanie usług kluczowych infrastruktury krytycznej, a więc ich cyberbezpieczeństwa.

Wynik badania w zakresie pytania 2.2.

Wobec tezy pytania 2.2.,

Struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego,

spośród udzielonych przez respondentów odpowiedzi, 20 (44,44%) osób wyraziło zgodę z tezą, przy czym większość (11) raczej się zgodziła. W udzielonych odpowiedziach 20 (44,44%) osób nie zgodziło się z tezą, przy czym większość (12) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, wśród których w równych częściach respondenci się zgadzają i nie zgadzają z tezą, że jest to kwestia nierozstrzygnięta oraz, że teza ta powinna zostać poddana ponownej weryfikacji po dłuższym funkcjonowaniu krajowego systemu cyberbezpieczeństwa, jak też po wprowadzonych do niego formalnoprawnych zmianach, wynikających z projektowanej zmiany Dyrektury NIS, jak też wobec projektowanych zmian regulacji zarządzania kryzysowego, tak na poziomie krajowym, jak i europejskim.

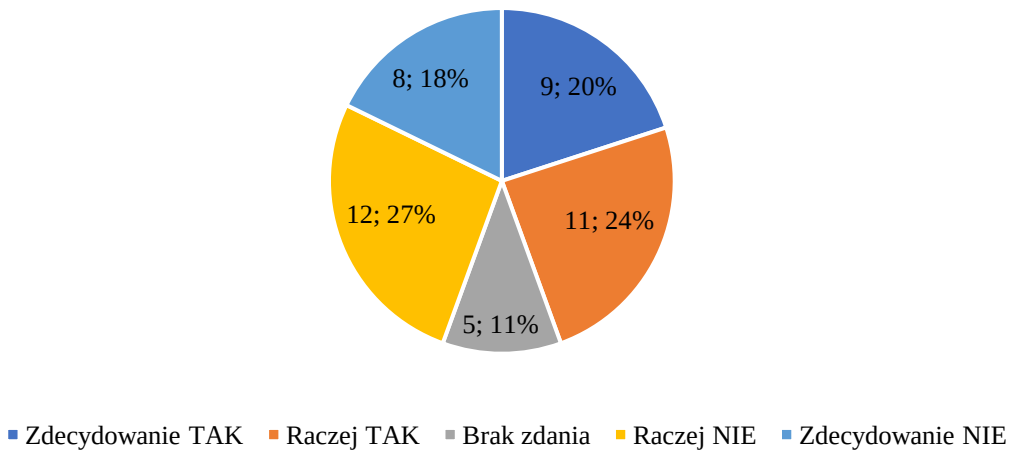
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi odpowiedzi uzyskanymi w badaniu. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 29 i na rysunku 22.

Tabela 29. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.2.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	20 / 20	9	11	5	12	8
%	100	44,44 / 44,44	20,00	24,44	11,12	26,67	17,79

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 22. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.2.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w tym zakresie wykazuje brak rozstrzygającego rozwiązania, co do składu struktur organizacyjnych zarządzania cyberbezpieczeństwem i ich ujednolicenia i zharmonizowania ze strukturami systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego. Przedstawione rozwiązanie zyskało tyluż zwolenników, co przeciwników. Należy poszukiwać rozwiązania tego zagadnienia w innej formule organizacyjnej.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów, przedstawione w uzupełnieniu do wybranej odpowiedzi, uwzględniają aspekty działania i współdziałania struktur i relacji operacyjnych zarządzania kryzowego i cyberbezpieczeństwa. Przeważają treści bezpośrednio dotyczące postawionego zagadnienia, zdarzają się także takie, które dotyczą zagadnień powiązanych lub dalszych problemowo. W szerokim zakresie przedstawionych treści należy

uwzględnić odniesienie do problematyki pytania. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w uzupełnieniu do udzielonych odpowiedzi w przedstawianych argumentach, opiniach i komentarzach zwracają uwagę, że spójność organizacyjna, zarządcza i procesowa to jedyna droga do skuteczności, tylko jednolite podejście do cyberbezpieczeństwa może zapewnić adekwatne i wystarczająco szybkie decyzje w przypadku kryzysów, unifikacja rozwiązań organizacyjnych związanych bezpieczeństwem w obszarze usług kluczowych oraz IK jest wskazana ze względu na charakter powiązań między tymi elementami, a nawet, że to jedyna słuszna droga rozwoju i implementacji KSC. Integralność obu systemów połączonych punktowo wydaje się właściwym kierunkiem. Dzięki temu możliwe jest agregowanie danych i analiza zbiorczych zagrożeń dla usług kluczowych i IK przy zachowaniu specyfiki każdego rodzaju zagrożeń. Wyrażono też stanowisko aprobaty dla podniesienia rangi i ujednolicenia organów, natomiast zdecydowanie nie dla integracji. Podniesiono również, że nadmierna ilość podmiotów nadzorujących i wykonawczych, zwłaszcza o krzyżujących się kompetencjach nie gwarantuje jakości procesu i może powodować chaos. Wyrażono zdanie, że RCB powinno być włączone w struktury systemu cyberbezpieczeństwa, bez włączania struktur regionalne, które nie wnoszą żadnej wartości jako pośrednik w obszarze cybernetycznym. Obecnie RCB i WCZK nie mają kompetencji dotyczących cyberbezpieczeństwa i nie są w stanie wykonawczo koordynować działania reagowania na zaawansowane zagrożenia. Decyzja o tym jak powinna wyglądać docelowa struktura wymaga uprzedniego sporządzenia mapy procesów tych jednostek i analizę punktów lub łańcuchów ich pokrywania się.

Argumenty, opinie i komentarze respondentów **nie zgadzających się z tezą pytania** wskazują, że organizacja zarządzania cyberbezpieczeństwem RP i przypisana odpowiedzialność powinny być ustanowione zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie, dedykowane podmioty w w/w zakresie, a nowe zadania zostały w miarę poprawnie zaprojektowane w nowelizacji UKSC. Przyjęcie rozwiązania sektorowego ustanawiającego organy właściwe ds. cyberbezpieczeństwa na poziomie właściwych ministerstw jest odpowiednie. Bardziej zasadne jest, aby funkcjonowały osobno dwa systemy – zarządzania kryzysowego i cyberbezpieczeństwa, ponieważ są wątpliwości, czy np. w przypadku wystąpienia równolegle katastrofy naturalnej i incydentu krytycznego (cyber-

bezpieczeństwa) podmioty systemów byłyby w stanie efektywnie i sprawnie realizować zadania w dwóch różnych obszarach. Cyberbezpieczeństwo w zakresie swojej aktywności nie opiera się wyłącznie na realizacji strategii i operacji zarządzania incydentami, przez co nie może być postrzegane przez pryzmat jedynie sytuacji kryzysowej. Respondenci zwracają uwagę, że zarządzanie kryzysowe/ ochrona IK nie są pojęciami tożsamymi z cyberbezpieczeństwem, zarządzanie kryzysowe jest podejmowane po wyeskalowaniu cyberincydentu do poziomu kryzysu, że te obszary tylko częściowo się pokrywają i ich zadania są inne. Respondenci podnoszą również, że system ZK jest daleki od doskonałości i strukturalnie/funkcjonalnie niedopasowany do potrzeb związanych ze sprawną komunikacją w obszarze cyberbezpieczeństwa. Jest systemem formalistycznym, w którym powstaje dużo dokumentów które nie mają realnego wpływu na funkcjonowanie organizacji. RCB zajmuje się sytuacjami kryzysowymi z powodów naturalnych, więc trudno rozszerzać kompetencje o dodatkowe role dotyczące domeny cyberbezpieczeństwa. Respondenci nie akceptują pełnej integracji i ujednolicenia, nadania pełnych kompetencji i władzy RCB w zakresie cybersecurity. Zwracają uwagę, że podejście integracyjne wzmacnia reaktywny charakter organizacji zarządzania cyberbezpieczeństwem. Urzędnicy i proponowane struktury nie zapewnią szybkiego czasu reakcji i możliwości przeciwdziałania cyberincydentom (poprzez upowszechnienie wiedzy, narzędzi i hierarchicznej struktury współdziałania). Spowoduje to nieuzasadnioną, kosztowną rozbudowę strukturalną w obszarze cyberbezpieczeństwa. Podniesione zostało również, że resorty siłowe mają tendencję do autonomizacji i unikania czynnika koordynującego, więc wyposażenie RCB w nowe kompetencje będzie trudne do przeforsowania w dyskusji z MSWiA i MON. Wskazują też, że to głównie RZZK wymaga pilnego wzmocnienia. Wskazany został też brak możliwości budowania CSIRT w każdym województwie w ramach włączania struktur regionalnych do systemu cyberbezpieczeństwa.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.2.

Autor rozprawy w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego.

Wynik badania w zakresie pytania 2.3.

Wobec tezy pytania 2.3.:

Struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji,

spośród udzielonych przez respondentów odpowiedzi, 22 (48,89%) respondentów zgodziło się z tak postawioną tezą, przy czym większość (16) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana, natomiast 15 respondentów (33,33%) nie wyraziło zgody z taką tezą, przy czym większość (12) raczej się nie zgodziła, jest to więc „miękki" brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zgadzają się, a ściślej, raczej się zgadzają, z tak postawioną tezą.

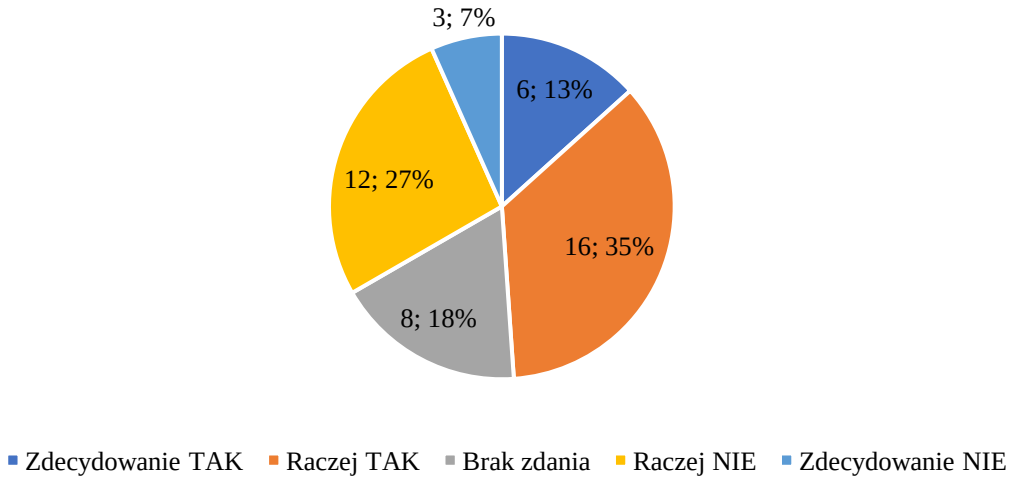
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 30 i na rysunku 23.

Tabela 30. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.3.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	22 / 15	6	16	8	12	3
%	100	48,89 / 33,33	13,33	35,56	17,77	26,67	6,67

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 23. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.3.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Uzyskany wynik badania w zakresie powyższego pytania wykazał, że większość respondentów akceptuje ujednolicenie i zharmonizowanie struktur operacyjnych systemu cyberbezpieczeństwa ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji. Implementacja takiego podejścia pozwoliłaby wykorzystać doświadczenie RCB w planowaniu i zarządzaniu bezpieczeństwem kraju. Nie wymagałoby też powoływania nowych instytucji i organów do realizacji tego zadania.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów, przedstawione w uzupełnieniu do wybranej odpowiedzi, uwzględniają aspekty działania i współdziałania struktur i relacji operacyjnych zarządzania kryzowego i cyberbezpieczeństwa. Przeważają treści bezpośrednio dotyczące postawionego zagadnienia, zdarzają się także takie, które dotyczą zagadnień powiązanych lub dalszych problemowo. W szerokim zakresie przedstawionych treści należy

uwzględnić odniesienie do problematyki pytania. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w ramach swoich argumentów, opinii i komentarzy zwracali uwagę, że zapewnienie centralizacji, spójności organizacyjnej, zarządczej i procesowej, i jednolitości podejścia do cyberbezpieczeństwa może zapewnić adekwatne i wystarczająco szybkie decyzje w przypadku kryzysów i jest kluczem do efektywności KSC. Unifikacja rozwiązań organizacyjnych jest wskazana, nadmierna ilość podmiotów nadzorujących i wykonawczych, zwłaszcza o krzyżujących się kompetencjach nie gwarantuje jakości procesu. Do zapewnienia interoperacyjności systemu cyberbezpieczeństwa niezbędny jest element między- i ponadresortowy, im prostszy model zarówno odpowiedzialności jak i decyzyjności tym lepiej dla systemu. Powinna istnieć jednostka w całości czuwająca nad zagrożeniami usług kluczowych i IK, może to być RCB lub inny powołany do tego organ. Respondenci wyrażali przekonanie, że wydzielenie kompetencji i ich harmonizacja pod egidą RCB (jako jednego miejsca przypisanej odpowiedzialności) wydaje się dobrym kierunkiem, RCB powinno zarządzać tym obszarem i może realizować tę funkcję. Zgodzono się również z włączeniem ról Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Punktów Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB i pełnej współpracy z CSIRTami krajowymi, zwracając uwagę, że interoperacyjności i sprawny przepływ komunikacji, pomiędzy tymi organami daje podstawy do zorganizowania tzw. sztabu operacyjnego akcji, z którego wynika sprawne działanie operacyjne. Zasugerowane, że RCB mogłoby stanowić centrum kompetencji centralnych i koordynacji działań, w tym również wymuszać dostęp do informacji o incydentach, koordynować reagowanie jako hub pomiędzy różnymi CERTami centralnymi/sektorowymi oraz wspierać nadzór realizacji obowiązków. Zwrócono uwagę, że ujednolicenie struktur państwowych jest odpowiednim kierunkiem, jednak sposób ich podporządkowania pod RCB wydaje się zbyt daleko idącym działaniem. Poddawano w wątpliwość kompetencje i wydolność struktur organizacyjnych RCB do realizacji zadań koordynacyjnych cyberbezpieczeństwa. Decyzja o tym jak powinna wyglądać docelowa struktura wymaga uprzedniego sporządzenia mapy procesów tych jednostek i analizę punktów lub łańcuchów ich pokrywania się.

Respondenci **nie zgadzający się z tezą pytania** w uzupełnieniu do udzielonych odpowiedzi ankietowych wyrażali zdanie, że organizacja zarządzania cyberbezpieczeństwem

RP powinna być ustanowiona zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie podmioty w w/w zakresie, że struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, ale bardziej zasadne jest, aby funkcjonowały osobno dwa systemy – zarządzania kryzysowego i cyberbezpieczeństwa, nie ma potrzeby integracji obu systemów. Optymalnym rozwiązaniem byłyby, gdyby zostało stworzone osobne ponadresortowe centrum cyberbezpieczeństwa, które ściśle współpracowałoby z Rządowym Centrum Bezpieczeństwa. Wskazano, że ABW jest krajową władzą bezpieczeństwa i może pełnić rolę integrującą, a także, że to przewodniczący RZZK powinien zarządzać cyberbezpieczeństwem. Respondenci poddają w wątpliwość bądź są wprost przeciwni rozszerzaniu kompetencji RCB, które nie ma potencjału ani władczości, aby koordynować to zagadnienie, RCB nie powinno być punktem centralnym z włączonymi strukturami KSC. Wskazano, że RCB może mieć rolę koordynującą, ale struktury KSC powinny być niezależne i posiadać własny, odrębny głos. W przeciwnym razie istnieje wysokie ryzyko obniżania priorytetów w obszarze cyberbezpieczeństwa na rzecz „bardziej namacalnych" zagrożeń np. kataklizmy naturalne. RCB jest organem wspierającym Premiera, więc taka zmiana oznaczałaby de facto poszerzenie uprawnień Premiera z czego zrezygnowano na rzecz obecnie istniejącego rozwiązania (większy udział ministrów działowych). RCB nie wydaje się w obecnej formie w pełni kompetentne do przejęcia roli centralnego zarządzania, jednocześnie zarządzanie centralne wydaje się podatne na słabości projektowe w przypadku cyberzagrożeń. Trudno sobie wyobrazić sytuację podejmowania decyzji operacyjnych przez organ centralny względem np. wyłączenia czy odbudowy systemu w jednostce samorządowej. Zintegrowana struktura daje tylko złudzenie zarządzania cyberbezpieczeństwem, bo jest reaktywne. Sugerowano rozwiązanie harmonizacji, a nie rozszerzanie roli struktur jednego podmiotu w obszarze cybersecurity, co może być nieskuteczne operacyjnie, chyba że powstanie wiele CSIRTów sektorowych, które będą proxy pomiędzy strukturami RCB i podmiotami zaangażowanymi w krajowy system cyberbezpieczeństwa. Zaproponowano również przyjęcie rozwiązania funkcjonującego w USA, gdzie agencja cyberbezpieczeństwa CISA ma kompetencje właściwe do tego, aby skutecznie realizować procedury reagowania kryzysowego, jednocześnie mając pełen mandat do zapobiegania kryzysom bez angażowania jednostek zarządzania kryzysowego. Stwierdzono też, że przyjęcie aktualnego rozwiązania sektorowego ustanawiającego organy właściwe ds. cyberbezpieczeństwa na poziomie właściwych ministerstw jest odpowiednie, w przeciwieństwie do centralnego zarządzania.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.3.

Autor rozprawy w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kos.aktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji.

Wynik badania w zakresie pytania 2.4.

Wobec tezy pytania 2.4.:

Proponowane w pkt. 2.3. powyżej zaangażowanie RCB w zarządzanie cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób, jako wariant wyboru,

respondenci udzielili w sumie 104 odpowiedzi, w tym odnośnie wariantu 1 – 36 głosów, wariantu 2 – 38 głosów, wariantu 3 – 40 głosów, w których:

- wariant 1 przedstawionego rozwiązania uzyskał poparcie 14 (12,28%) głosów, przy czym zdecydowana większość głosów (9) raczej go poparła, jest to więc „miękkie" poparcie, natomiast 16 (14,04%) głosów nie poparła tego wariantu, przy czym większość (9) głosów raczej nie poparła;
- wariant 2 przedstawionego rozwiązania uzyskał poparcie 16 (14,04%) głosów, przy czym rozkład głosów zdecydowanie i raczej popierających jest równy (8/8), natomiast 14 (12,28%) głosów nie poparła tego wariantu, przy czym większość (9) głosów raczej nie poparła, nie jest to więc zdecydowany, mocny brak poparcia;
- wariant 3 przedstawionego rozwiązania uzyskał poparcie 19 (16,67%) głosów, przy czym większość głosów (11) zdecydowanie go poparła, natomiast 14 (12,28%) głosów nie wyraziło poparcia dla tego wariantu, przy czym większość (9) głosów raczej nie poparła, nie jest to więc zdecydowany, mocny brak poparcia.

Podsumowując uzyskane wyniki, należy stwierdzić, że respondenci, w swojej większości, najbardziej poparli rozwiązanie wariantu 3 (19 głosów na tak, przy 14 głosach na nie), a następnie wariant 2 (16 głosów na tak, przy 14 głosach na nie). Respondenci nie poparli wariantu 1 (14 głosów na nie, przy 16 głosach na tak). Należy zwrócić uwagę, że uzyskane wyniki poparcia i braku poparcia dla poszczególnych wariantów niewiele się różnią, o kilka głosów, są bliskie równowagi w kwestii tezy 2.4.

W odpowiedziach na postawione pytanie 2.4. odniesiono się do udzielonych głosów na tak lub na nie, ponieważ nie wszyscy respondenci zdecydowali się w ogóle udzielić odpowiedzi na to pytania, a spośród udzielających odpowiedzi, część oddała tylko jeden głos, wskazując wybrany wariant, inni respondenci wskazywali każdy z wariantów przypisując go do wybranej opcji standardowej odpowiedzi. Stąd pod uwagę nie jest brana liczba respondentów, a liczba oddanych głosów w wyborze wariantu rozwiązania.

Wynik badania w powyższym zakresie prezentuje zdecydowanie dominujące stanowisko większości respondentów uważających, że w przypadku zaangażowania RCB w zarządzanie cyberbezpieczeństwem RP zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, powinno ono mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa. Mniejsza część respondentów wskazała na rozwiązanie, w którym RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa granicach kompetencji organów powołanych ustawą KSC. Natomiast nieznaczna mniejszość respondentów wybrała rozwiązanie, w którym RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa.

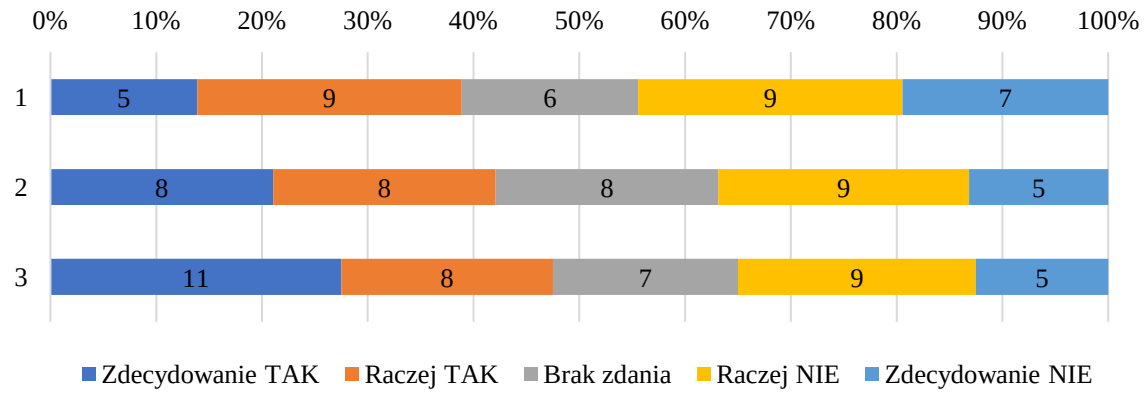
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 31 i na rysunku 24.

Tabela 31. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.4.

Lp.	Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP	Suma 114	T / N Szt./%	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym	**36**	**14 / 16** **12,28 / 14,04**	5 4,39	9 7,89	6 5,26	9 7,89	7 6,14
2	RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego	**38**	**16 / 14** **14,04 / 12,28**	8 7,02	8 7,02	8 7,02	9 7,89	5 4,39
3	RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa	**40**	**19 / 14** **16,67 / 12,28**	11 9,65	8 7,02	7 6,14	9 7,89	5 4,39

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 24. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.4.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynika badania wykazują, że zdaniem większości respondentów (oddanych głosów) struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób:

1) RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie preferowane – wariant 3 proponowanej odpowiedzi pytania ankietowego);
2) RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich

jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa., Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego (rozwiązanie drugiego wyboru – wariant 2 proponowanej odpowiedzi pytania ankietowego);

3) natomiast RCB nie powinno mieć pełnej odpowiedzialności za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym (wariant 1 proponowanej odpowiedzi pytania ankietowego).

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów często odnoszą się do różnych aspektów działania i współdziałania struktur i relacji operacyjnych zarządzania kryzowego i cyberbezpieczeństwa, jak również do funkcjonowania rozwiązań cyberbezpieczeństwa w strukturach regionalnych. Niektóre z nich stanowią bezpośrednią argumentację, inne pośrednią, czasami w ujęciu ogólnym. W tak szerokim spektrum treści należy uwzględnić odniesienie do problematyki pytania. Ze względu na charakter pytania i specyfikę odpowiedzi wskazane przez respondentów argumenty, opinie i komentarze należy uznać za odniesienie się do dokonanego wyboru opcji odpowiedzi. Poniżej przedstawiono zestawione argumenty, opinie i komentarze respondentów, zarówno wyrażających pozytywne, akceptujące podejście do zagadnienia integracji i zharmonizowania struktur obu systemów (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z przedstawionymi rozwiązaniami.

Respondenci **zgadzający się z przedstawioną opcją odpowiedzi** w ramach uzupełnienia swego wyboru, przedstawiali argumenty, opinie i komentarze, w których podnosili, że uproszczenie odpowiedzialności za zarządzanie kryzysami w obszarze takim jak cyberbezpieczeństwo jest wskazane ze względu na szybkość i konieczność podejmowania jednoznacznych decyzji, a rozłożenie kompetencji na kilka podmiotów może wydłużać proces decyzyjny, rozmywać odpowiedzialność oraz rodzić spory kompetencyjne. Należy dążyć do centralizacji kompetencji i obowiązków na szczeblu krajowych i ustanowienie jednego organu odpowiedzialnego za cyberbezpieczeństwo, gdyż jest to jedyny efektywny sposób reakcji w sytuacji kryzysowej, zaś scenariusze sytuacji kryzysowej w zarządzaniu kryzyso-

wym już zawierają incydenty cyber, podobnie jak plany obronne i plany ochrony IK. Respondenci wskazywali również, że RCB powinno pełnić wiodącą rolę w organizowaniu KSC i zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa jako podmiot ulokowany wystarczająco wysoko w strukturach Państwa, jednak powinno podlegać nadzorowi. Rozwiązanie, w którym RCB ma wiodącą rolę nie prowadzi do silnej koncentracji wszystkich zadań i uprawnień dotyczących nieraz bardzo odległych kompetencji. Nadmierna centralizacja, zwłaszcza dokonana skokowo mogłaby spowodować pogorszenie jakości procesu zarzadzania cyberbezpieczeństwem wskutek nadmiaru zadań ciążących na RCB. Respondenci zwrócili uwagę na uwarunkowania prawne pozycji RCB i relacji z innymi podmiotami odpowiedzialnymi za obszar cyberbezpieczeństwa oraz na ewentualną konieczność zmiany powiązanych aktów prawnych w celu wyeliminowania ryzyka wystąpienia ograniczeń prawnych w przyjętym modelu funkcjonalnym.

Respondenci **nie zgadzający się z przedstawioną opcją odpowiedzi** w ramach uzupełnienia swego wyboru, przedstawiali argumenty, opinie i komentarze, w których wyrażali, że powinna istnieć jednostka w całości czuwająca nad zagrożeniami usług kluczowych i IK, może ty być RCB lub inny powołany do tego organ. Zwracali uwagę, że ABW jest krajową władzą bezpieczeństwa i może pełnić rolę integrującą oraz, że zarządzanie kryzysowe w RP sprawuje Rada Ministrów i jeśli jakiś organ ma mieć decyzyjne kompetencje ponadresortowe, to RZZK. Optymalnym rozwiązaniem byłyby, gdyby zostało stworzone osobne ponadresortowe centrum cyberbezpieczeństwa, które ściśle współpracowałoby z Rządowym Centrum Bezpieczeństwa. Respondenci podnosili, że pełna odpowiedzialność RCB za koordynację cyberbezpieczeństwa to zbyt duży zakres, że RCB w obecnej formie nie jest w stanie pełnić funkcji wiodących i koordynacyjnych, nie ma potencjału ani władczości. RCB powinno być ważnym, ale nie głównym elementem całego systemu cyberbezpieczeństwa w Polsce. Zwrócono uwagę na rozwiązanie o charakterze koordynacji branżowej/sektorowej – ze względu na wspólną znajomość zagrożeń w grupie podmiotów. Sugerowano również, że organizacja cyberbezpieczeństwa nie powinna być domeną urzędników, ale raczej wojska.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.4.

Autor rozprawy prawie w pełni zgadza się z uzyskaną z dominującej części odpowiedzi respondentów konkluzją. Zdaniem autora przedstawiona w pytaniu 2.3. propozycja

organizacji zarządzania cyberbezpieczeństwem RP, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinna być ustanowiona w sposób:

1) RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie preferowane – wariant 3 proponowanej odpowiedzi pytania ankietowego);
2) RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym (rozwiązanie drugiego wyboru – wariant 1 proponowanej odpowiedzi pytania ankietowego);
3) RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego (rozwiązanie trzeciego wyboru – wariant 2 proponowanej odpowiedzi pytania ankietowego).

W systemie zarządzania bezpieczeństwem narodowym powinna być ujęta jednorodna i zharmonizowana organizacja zarządzania cyberbezpieczeństwem na poziomie krajowym.

Wynik badania w zakresie pytania 2.5.

Wobec tezy pytania 2.5.:

Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami,

spośród udzielonych przez respondentów odpowiedzi, 31 (70,46%) respondentów zgodziło się z tak postawioną tezą, przy czym zdecydowana większość (21) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana, choć zdecydowanie przeważająca nad odpowiedzią przeciwną, której udzieliło 11 (25%) respondentów, przy czym zdecydowana większość (8) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zgadzają się, a ściślej, raczej się zgadzają, z tak postawioną tezą.

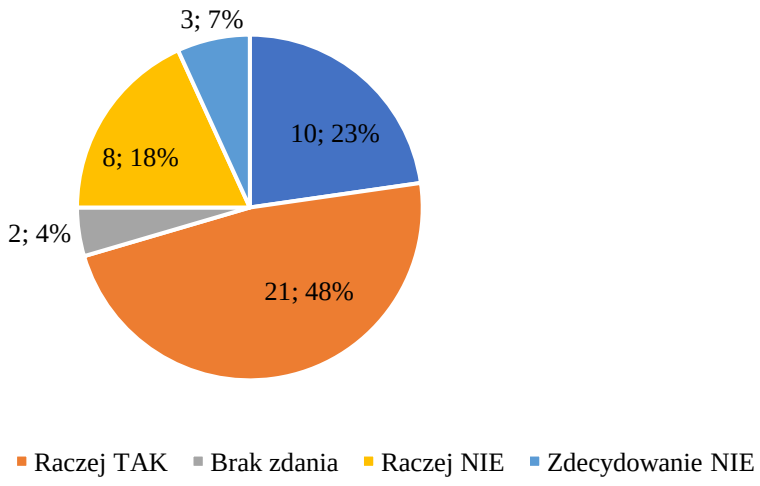
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 32 i na rysunku 25.

Tabela 32. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.5.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	44	31 / 11	10	21	2	8	3
%	100	70,45 / 25,00	22,73	47,72	4,55	18,18	6,82

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 25. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.5.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Zdecydowana większość respondentów wskazała, że RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. Oznacza to, że respondenci oczekują szerokiego włączenia organów, podmiotów i instytucji w zapewnienie cyberbezpieczeństwa i reagowanie na incydenty, co wymaga znacznego rozszerzenia zakresu podmiotów krajowego systemu cyberbezpieczeństwa.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów, przedstawione w uzupełnieniu do wyboru opcji odpowiedzi, często odnoszą się do różnych aspektów działania i współdziałania systemów zarządzania kryzowego i cyberbezpieczeństwa, jak też do funkcjonowania rozwiązań cyberbezpieczeństwa w strukturach regionalnych. Niektóre z nich bezpośrednio, a inne pośrednio odnoszą się do zagadnienia. W tak szerokim spektrum treści należy uwzględnić odniesienie do problematyki pytania. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w swoich argumentach, opiniach i komentarzach do udzielonych odpowiedzi zwracali uwagę, że zaangażowanie w/w podmiotów będzie właściwe ze względu na zakres ich zadań. Rozwiązanie to jest potencjalnie dobre i właściwy kierunek zmian, w szczególności dlatego, że takie podmioty działają operacyjnie, a domena cyber coraz częściej jest elementem zarządzania kryzysowego praktycznie w każdej innej dziedzinie, a podnoszenie kompetencji w wymienionych podmiotach jest uzasadnione, aby dzięki dostępowi do obrazu świadomości sytuacyjnej krajowego systemu cyberbezpieczeństwa były w stanie właściwie dostarczać dane oraz włączyć się do obsługi i zarządzania incydentami w miarę potrzeb. Podmioty te powinny mieć wiedzę oraz dostęp do informacji – incydent z zakresu cyberbezpieczeństwa może mieć przełożenie na zarządzanie kryzysowe. Jeżeli włączenie i informowanie podmiotów będzie zawierało właściwy kontekst, to da im szansę na przygotowanie się i ew. uniknięcie ataku. Świadomość publicznych skutków dysfunkcji operatora usługi kluczowej jest informacją ważną w procesie zarządzania kryzysowego. Respondenci wyrażali również zdanie, że RCB powinno być włączone w procesy informacyjne oraz do obsługi i zarządzania incydentami cyberbezpieczeństwa jako członek zespołu bez przejęcia pełnej odpowiedzialności, a nie lider. Przedstawiono też

stanowisko, że w przypadkach, kiedy istnieje ryzyko, że incydent doprowadzi do sytuacji kryzysowej, RCB powinno być informowane, natomiast nie powinno być włączone na poziomie operacyjnym. Obecnie RCB jest włączone do informowania o zagrożeniach cyberbezpieczeństwa oraz do informowania o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa np. poprzez przekazywanie operatorom infrastruktury krytycznej ostrzeżeń i alertów wydawanych przez CSIRT GOV. Do zarządzania incydentami dla operatorów infrastruktury krytycznej właściwym jest CSIRT GOV, a RCB jest włączone do tego procesu, gdyż organizuje pracę dla Zespołu ds. Incydentów Krytycznych. W odniesieniu do podmiotów regionalnych respondenci przedstawiali zdanie, że powinny być informowane o incydentach cyberbezpieczeństwa, natomiast nie powinny być włączane do ich obsługi i zarządzania.

Respondenci **nie zgadzający się z tezą pytania** podnosili, że podmioty dedykowane zarządzaniu kryzysowemu powinny być włączane tylko w te incydenty, które mogą prowadzić do zakłócenia funkcjonowania danych struktur państwowych. Bezzasadne wydaje się włączanie struktur dedykowanych zarządzaniu kryzysowemu wszystkim działaniom (w szczególności incydentom), którymi zajmują się jednostki dedykowane cyberbezpieczeństwu. Zarządzanie incydentami cyberbezpieczeństwa powinno pozostać domeną CSIRT. RCB, które ma kompetencje w klasycznych działaniach kryzysowych powinno uzyskiwać tylko informacje dotyczące cyberbezpieczeństwa w kontekście infrastruktury krytycznej. RCB nie ma kompetencji w działaniach cybersecurity, zarządzanie incydentami nie powinno leżeć w jego gestii. Odpowiednia jest rola informacyjna. Respondenci są zdania, że konieczne jest adekwatne powiązanie innych podmiotów, takich jak WCZK poprzez informowanie o incydentach, jednakże zwracają uwagę, że organ wojewody nie posiada obecnie stosownych kompetencji praktycznych, a zagrożenia pochodzą spoza województwa, a nawet kraju, zatem możliwa jest obsługa zarządzania incydentami tylko w niektórych przypadkach, a nie co do zasady.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.5.

Autor rozprawy w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Wynik badania w zakresie pytania 2.6.

Wobec tezy pytania 2.6.,

CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych,

wśród udzielonych przez respondentów odpowiedzi, 36 (80,00%) osób wyraziło zgodę z tezą, przy czym rozkład zdecydowane i raczej zgody jest równomierny, obie opcje poparło po 18 osób, jest to więc zgoda zdecydowanie przeważająca na brakiem zgody z tezą. W udzielonych odpowiedziach 5 (11,11%) osób nie zgodziło się z tezą, przy czym zdecydowana większość (4) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zgadzają się z tezą postawioną w pytaniu.

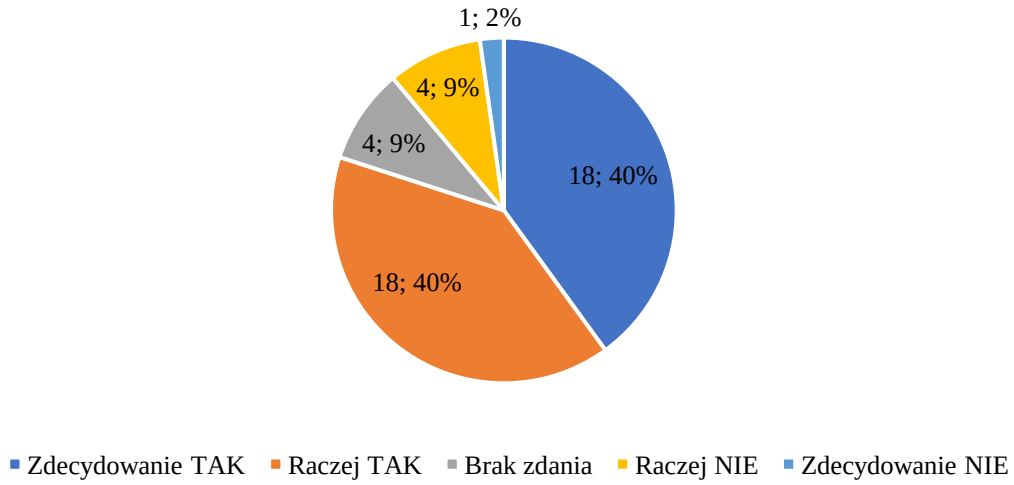
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 33 i na rysunku 26.

Tabela 33. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.6.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	36 / 5	18	18	4	4	1
%	100	80,00 / 11,11	40,00	40,00	8,89	8,89	2,22

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 26. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 2.6.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania wskazuje, że przytłaczająca większość respondentów wskazała, że CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, czego aktualnie brakuje, oraz w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych. Oznacza to, że respondenci oczekują powstawania CSIRT jak najbliżej podmiotów danego sektora oraz znających jego specyfikę, a przez to sprawniej reagujących na zagrożenia i incydenty.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Argumenty, opinie i komentarze respondentów odnoszą się w sposób jednoznaczny do postawionego zagadnienia. Poniżej przedstawiono zestawione argumenty, opinie i komentarze respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających) i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w uzupełnieniu do swojej odpowiedzi podnosili, że CSIRT sektorowe/podsektorowe powinny być ustanowione dla każdego sektora/podsektora, gdyż specyfika działania każdej branży (sektora, podsektora) jest inna, różne też mogą być m.in. standardy, protokoły i urządzenia ICT/OT oraz zasady komunikacji i słownictwo w poszczególnych sektorach. Istnieją ponadto przepisy oraz standardy sektorowe/podsektorowe, które mają lub mogą mieć wpływ na bezpieczeństwo (cyberbezpie-

czeństwo). Specyfika poszczególnych sektorów wymaga wręcz powołania specjalizowanych w danym sektorze, wykwalifikowanych jednostek posiadających wiedzę specyficzną dla danego sektora, przy jednoczesnym merytorycznym odnoszeniu jej w obszarze cyberbezpieczeństwa. CSIRT-y sektorowe/podsektorowe mają większą skuteczność w zapewnianiu właściwego i optymalnego do istniejących zagrożeń poziomu cyberbezpieczeństwa w danym sektorze/podsektorze. CSIRT sektorowe są w stanie zdecydowanie celniej rozpoznawać zagrożenia ze względu na specyficzne uwarunkowania, lepiej wdrażają działania profilaktyczne i operacyjnie przeciwdziałają zaistniałym zagrożeniom. Sugerowano, że CSIRT'y sektorowe, co do zasady, powinny się skupić na zadaniach klasy threat hunting dla swojego sektora oraz na wsparciu w realizacji zadań obsługi incydentów dla podmiotów, gdzie zapewnienie profesjonalnej kadry jest nie możliwe, lub nie ma uzasadnienia ekonomicznego. Respondenci podnieśli, że celem nadrzędnym musi być doprowadzenie do uzyskania całościowego obrazu sytuacji cyberbezpieczeństwa w kraju, struktury monitorowania stanu cyberbezpieczeństwa należy rozwijać w szerz i w dół. Obecnie system cyberbezpieczeństwa jest (podmiotowo) zbyt wąski i zbyt płytki, a przedmiotowo – zbyt niejasny i ogólny. Zakres oddziaływania CSIRT sektorowych powinien być nie tyle szerszy, co precyzyjniej zdefiniowany, tak aby unikać „problemów niczyich". Jednocześnie bariery informacyjne w zakresie współdzielenia informacji o zagrożeniach muszą być systemowo usunięte, tak aby zapewnić widzialność incydentów obejmujących więcej niż jeden sektor. Struktura CSIRT sektorowych wymaga dialogu z CSIRT poziomu krajowego oraz organami właściwymi, a także działającym CSIRT sektorowym przy KNF, co zapewniłoby właściwą wymianę doświadczeń i zwiększyło szansę na przyjęcie rekomendacji, które podniosłyby jakość nowoorganizowanych struktur. Respondenci wyrażali również zdanie, że obecny zakres działania CSIRTów sektorowych jest wystarczający, że nie ma potrzeby ich ustanawiania dla każdego sektora, choć dla kilku ważnych sektorów byłoby warto, m.in. np. dla NGO, administracji publicznej. Zwrócono też uwagę na kwestie finansowe, podnosząc, że powstanie CSIRT sektorowych jest uwarunkowane zapewnieniem finansowania, a także że ze względu na koszty nie jest rozwiązaniem ekonomicznym, więc ich ilość należy przemyśleć. Respondenci zwrócili też uwagę na korzyści wynikające z przyjęcia analizowanego rozwiązania, wskazując, że umożliwiłoby to specjalizację, dałoby szansę na wzrost cyberbepieczeństwa w sektorach i zapewniłoby przejrzystą i bezpośrednią strukturę komunikacji oraz poprawę poziomu bezpieczeństwa teleinformatycznego kraju. Zauważono również, że rozwiązanie zostanie wprowadzone po dostosowaniu polskiego systemu zarządzania kryzysowego i systemu cyberbezpieczeństwa do nowych dyrektyw unijnych CER i NIS2.

Argumenty, komentarze i opinie respondentów **nie zgadzających się z tezą pytania** wskazują, że nie powinno być z góry narzuconego obowiązku tworzenia CSIRTów dla wszystkich sektorów. Rozbudowa CSIRTów przy obecnym rynku jest kompletną utopią. Na chwilę obecną działa kilka CSIRTów sektorowych, a obecny stan wskazuje na niezdolność do wyczerpania pełnej listy zdefiniowanych CSIRT-ów sektorowych. Poszerzanie tej listy obecnie nie ma sensu. Dopiero po wdrożeniu pozostałych, zebraniu wiedzy i doświadczenia będzie można ocenić zasadność zmian. Jednym z warunków tej zmiany jest poszerzenie bazy specjalistów mających odpowiednie przygotowanie i zdecydowanie bardziej energiczne działania ministra właściwego w celu powołania CSIRTów już ustanowionych ustawowo. Respondenci wskazują, że w tej kwestii kluczowa jest współpraca i ustawa nie wymusi zmiany przy braku porozumienia. Dlatego należy tylko propagować idee CSIRTów sektorowych bez obowiązku ich ustanowienia – jednocześnie wymuszając podległość pod RCB, które, jeśli uzna za konieczne, może zawnioskować o powstanie CSIRTu w sektorach, gdzie to będzie uzasadnione.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 2., ppkt 2.6.

Autor rozprawy podziela to zdanie i w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych.

4.4. Podsumowanie wyników badania

Na podstawie wyników przeprowadzonego badania zweryfikowano pozytywnie postawioną przez autora hipotezę i sformułowano wnioski, wynikające z uzyskanych od respondentów odpowiedzi na postawione w badaniu pytania, które zostały wykorzystane w proponowanej koncepcji rozwiązań w zakresie zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa.

Wyniki badania pozwalają na sformułowanie wniosków do zastosowania w opracowaniu proponowanej koncepcji rozwiązań w zakresie zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa:

1. Struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym **nie są właściwie zdefiniowane** i **nie zapewniają efektywności** krajowego systemu cyberbezpieczeństwa **i odpowiedniego poziomu bezpieczeństwa** państwa.
2. Struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa **mogłyby być ujednolicone i zharmonizowane** ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego.
3. Struktury operacyjne systemu cyberbezpieczeństwa **powinny być ujednolicone i zharmonizowane** ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji.
4. Proponowane w pkt. 3 powyżej zaangażowanie RCB w zarządzanie cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób:
    1) RCB **powinno mieć ulokowane w swoich strukturach funkcje i kompetencje** przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa (rozwiązanie preferowane – wariant 3 proponowanej odpowiedzi pytania ankietowego),

2) RCB **powinno mieć wiodącą rolę** w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotami właściwymi i organami regionalnymi (np. wojewódzkimi) zarządzania kryzysowego (rozwiązanie drugiego wyboru – wariant 2 proponowanej odpowiedzi pytania ankietowego).
3) RCB **nie powinno mieć pełnej odpowiedzialności** za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa (wariant 1 proponowanej odpowiedzi pytania ankietowego).

5. Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) **powinny być włączone**, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.
6. CSIRT sektorowe **powinny być ustanowione dla każdego** sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych.

Koncepcja rozwiązań w zakresie struktur i relacji operacyjnych systemu cyberbezpieczeństwa ma dotyczyć ogólnej koncepcji takich struktur oraz relacji w zakresie zarządzania cyberbezpieczeństwem i zarządzania incydentami cyberbezpieczeństwa.

Sformułowane wnioski 1-5 dedykowane są do zastosowania w ogólnej koncepcji struktur i relacji operacyjnych systemu cyberbezpieczeństwa oraz struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym, natomiast wnioski 6 i 7 dedykowane są do zastosowania w proponowanej koncepcji struktur i relacji zarządzania incydentami cyberbezpieczeństwa.

4.5. Koncepcja struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP

W ramach przeprowadzonego procesu badawczego w zakresie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem, stanowiącym przedmiotową problematykę niniejszego rozdziału, na podstawie wyników przeprowadzonego badania zweryfikowano pozytywnie postawioną przez autora hipotezę i sformułowano wnioski, wynikające z uzyskanych od respondentów odpowiedzi na postawione w badaniu pytania, które zostały wykorzystane w opracowaniu proponowanej koncepcji doskonalenia rozwiązań struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem.

Koncepcja doskonalenia zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP, adresująca wyniki i wnioski z badania, sformułowana w tezie:
Ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność tego systemu na poziomie operacyjnym i odpowiedni poziom bezpieczeństwa państwa,
powinna zawierać trzy rozwiązania, dedykowane zagadnieniom organizacji przedmiotowych struktur i relacji:

1. zorganizowanie **struktur i relacji operacyjnych** systemu cyberbezpieczeństwa RP, stanowiących kompilację wywodzących się z nich struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowych i zarządzania incydentami cyberbezpieczeństwa, w ramach którego:

Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP

powinny obejmować zagregowaną listę podmiotów występujących, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

2. zorganizowanie **struktur i relacji z zarządzania cyberbezpieczeństwem** na poziomie krajowym systemu cyberbezpieczeństwa RP, w ramach którego:

Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP powinny obejmować zagregowaną listę podmiotów realizujących procesy i dokumenty zarządcze, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

3. zorganizowanie **struktur i relacji zarządzania incydentami cyberbezpieczeństwa** systemu cyberbezpieczeństwa RP, w ramach którego:

Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa na poziomie krajowym systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy po-

ziomu krajowego. Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych. Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP (SCRP) powinny obejmować zagregowaną listę podmiotów realizujących zarządzanie sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

Takie podejście jest zgodne z zakresem przeprowadzonej analizy zorganizowania struktur i relacji operacyjnych w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa w niniejszym rozdziale.

Opracowana koncepcja zorganizowania struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym stanowi nowum pracy, wypełnia zdiagnozowaną lukę, brak i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwych struktur i relacji operacyjnych.

W zakresie zorganizowania struktur i relacji z zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP zaproponowano strukturę operacyjną, mogącą realizować procesy i dokumenty zarządcze systemu cyberbezpieczeństwa RP. Aktualnie funkcjonujący krajowy system cyberbezpieczeństwa nie posiada żadnych procesów i dokumentów planowania i zarządzania cyberbebezpieczeństwem na poziomie krajowym, ani żadnych struktur zarządczych, które wypełniałyby takie zadania.

W zakresie zorganizowania struktur i relacji z zarządzania incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP, zaproponowano znaczne rozszerzenie zaangażowanych podmiotów, organów i instytucji względem aktualnie zdefiniowanego zakresu w Ustawie KSC oraz włączenie i zintegrowanie podmiotów systemu zarządzania kryzysowego, dla zapewnienia większej efektywności komunikowania i obsługi incydentów, a przez to zwiększenie poziomu bezpieczeństwa.

Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP skonstruowane są jako łączny zbiór wszystkich aktualnych i nowych podmiotów systemu cyberbezpieczeństwa, zdefiniowanych w koncepcjach struktur zarządzania cyberbezpieczeństwem na poziomie krajowym i zarządzania incydentami cyberbezpieczeństwa, oraz struktur systemu zarządzania kryzysowego, włączonych do realizacji zadań z zakresu cyberbezpieczeństwa.

Sposoby realizacji proponowanych koncepcji zorganizowania struktur i relacji operacyjnych, zarządzania cyberbezpieczeństwem i zarządzania incydentami cyberbezpieczeństwa na poziomie krajowym zostały przedstawione w kolejnych, dedykowanych każdemu z rozwiązań koncepcji, podrozdziałach.

4.5.1. Koncepcja struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP

Koncepcja zorganizowania struktur i relacji operacyjnych organów i podmiotów systemu cyberbezpieczeństwa RP zakłada ujednolicenie i zharmonizowanie takich struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP powinny obejmować zagregowaną listę podmiotów występujących, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

W składzie struktur operacyjnych systemu cyberbezpieczeństwa RP powinny się znajdować organy i podmioty:

- Prezes Rady Ministrów,
- Rada Ministrów,
- Rządowy Zespół Zarządzania Kryzysowego,

- Zespół ds. Incydentów Krytycznych,
- Dyrektor Rządowego Centrum Bezpieczeństwa (RCB),
- Rządowe Centrum Bezpieczeństwa (RCB), mające w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa
- Kolegium do Spraw Cyberbezpieczeństwa,
- ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego (organy właściwe w sprawach cyberbezpieczeństwa),
- CSIRTy poziomu krajowego (CSIRT NASK, CSIRT MON, CSIRT GOV),
- sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektorów),
- zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych,
- minister właściwy do spraw administracji publicznej,
- minister właściwy do spraw wewnętrznych,
- kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego,
- Szef Agencji Bezpieczeństwa Wewnętrznego,
- wojewoda,
- komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego, wojewódzkie centrum zarządzania kryzysowego,
- starosta, powiatowy zespół zarządzania kryzysowego, powiatowe centrum zarządzania kryzysowego,
- wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego, gminne centrum zarządzania kryzysowego,
- podmioty świadczące usługi z zakresu cyberbezpieczeństwa,
- urzędy centralne i podmioty publiczne,
- operatorzy usług kluczowych,
- dostawcy usług cyfrowych,

– operator infrastruktury krytycznej – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej.

Struktury operacyjne systemu cyberbezpieczeństwa RP opracowane w ramach koncepcji w zestawieniu porównawczym ze strukturami operacyjnymi systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa przedstawione zostały w tabeli 34.

Tabela 34. Struktury i relacje operacyjne systemu cyberbezpieczeństwa - systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i koncepcji systemu cyberbezpieczeństwa RP – ujęcie porównawcze

Struktury i relacje operacyjne systemu cyberbezpieczeństwa – ujęcie porównawcze		
Rozwiązania aktualne		**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**System cyberbezpieczeńsytwa RP (SCRP) - Koncepcja**
Rada Ministrów		Prezes Rady Ministrów
Prezes Rady Ministrów		Rada Ministrów
Rządowy Zespół Zarządzania Kryzysowego (RZZK)		Rządowy Zespół Zarządzania Kryzysowego (RZZK)
	Zespół ds. Incydentów Krytycznych	Zespół ds. Incydentów Krytycznych
	Pełnomocnik Rządu ds. Cyberbezpieczeństwa	
	Pojedynczy Punkt Kontaktowy	
	Kolegium ds. Cyberbezpieczeństwa	Kolegium ds. Cyberbezpieczeństwa
	Narodowy Punkt Kontaktowy do współpracy z NATO	Narodowy Punkt Kontaktowy do współpracy z NATO
Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)
Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB) (z funkcjami: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa)
	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON
ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego, minister właściwy		ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa oraz ministro-

do spraw administracji publicznej, minister właściwy do spraw wewnętrznych		wie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych
zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych		zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych
Szef Agencji Bezpieczeństwa Wewnętrznego	*Szef Agencji Bezpieczeństwa Wewnętrznego*	Szef Agencji Bezpieczeństwa Wewnętrznego
	CSIRT MON, CSIRT NASK, CSIRT GOV	CSIRT MON, CSIRT NASK, CSIRT GOV
	sektorowe zespoły cyberbezpieczeństwa (dla wybranych sektorów)	sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektorów)
kierownicy jednostek organizacyjnych planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego		kierownicy jednostek organizacyjnych planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego
wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK), wojewódzkie centrum zarządzania kryzysowego (WCZK)		wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK), wojewódzkie centrum zarządzania kryzysowego (WCZK)
starosta, powiatowy zespół zarządzania kryzysowego (PZZK), powiatowe centra zarządzania kryzysowego (PCZK)		starosta, powiatowy zespół zarządzania kryzysowego (PZZK), powiatowe centra zarządzania kryzysowego (PCZK)
wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK), gminne centrum zarządzania kryzysowego (GCZK)		wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK), gminne centrum zarządzania kryzysowego (GCZK)
	podmioty świadczące usługi z zakresu cyberbezpieczeństwa	podmioty świadczące usługi z zakresu cyberbezpieczeństwa
		urzędy centralne i podmioty publiczne
operator infrastruktury krytycznej	operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny	operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny operator infrastruktury krytycznej

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 27. Koncepcja struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP – model relacji

Koncepcja struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP				
	POZIOMY WSPÓŁPRACY			
ZWIERZCHNOŚĆ	Rada Ministrów Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego Zespół ds. Incydentów Krytycznych	Rządowe Centrum Bezpieczeństwa – Krajowe centrum zarządzania kryzysowego, funkcje: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa	Kolegium ds. cyberbezpieczeństwa
	Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych, kierujący działami administracji rządowej Ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa		Minister właściwy ds. informatyzacji, Minister obrony narodowej MON, Narodowy Punkt Kontaktowy do współpracy z NATO Minister właściwy ds. wewnętrznych /ABW	Organ właściwy ds. cyberbezpieczeństwa
	Zespół zarządzania kryzysowego Centrum zarządzania kryzysowego		CSIRT NASK CSIRT MON CSIRT GOV	Sektorowy zespół cyberbezpieczeństwa
	Wojewoda	Wojewódzki zespół zarządzania kryzysowego	Wojewódzkie centrum zarządzania kryzysowego	Komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim
	Starosta	Powiatowy zespół zarządzania kryzysowego	Powiatowe centrum zarządzania kryzysowego	Powiatowa administracja zespolona i jednostki organizacyjne powiatu
	Wójt, burmistrz, prezydent miasta	Gminny zespół zarządzania kryzysowego	Gminne centrum zarządzania kryzysowego	Komórka organizacyjna urzędu gminy (miasta) właściwa w sprawach zarządzania kryzysowego
	Operator infrastruktury krytycznej Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny			Podmiot świadczący usługi z zakresu cyberbezpieczeństwa

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Realizacja koncepcji rozwiązań struktur operacyjnych systemu cyberbezpieczeństwa RP zakłada zintegrowanie kompetencji, relacji i ról organów i podmiotów oraz struktur operacyjnych systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Propozycja koncepcji rozwiązań struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP przedstawiona została na rysunku 27.

Rada Ministrów powinna sprawować zarządzanie bezpieczeństwem, w tym zarządzanie kryzysowe i zarządzanie cyberbezpieczeństwem na terytorium Rzeczypospolitej Polskiej. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe powinien sprawować minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Rada Ministrów powinna przyjmować Krajowy Plan Zarzadzania Kryzysowego i (wg nowej koncepcji) Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC) lub (w miejsce obu wcześniej wymienionych) Krajowy Plan Zarzadzania Kryzysowego i Cyberbezpieczeństwa (KPZKC). Rada Ministrów powinna przyjmować Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i (wg nowej koncepcji) Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT) lub (w miejsce obu wcześniej wymienionych) Narodowy Program Ochrony Infrastruktury Krytycznej i Teleinformatycznej (NPOIKT). Rada Ministrów powinna przyjmować Raport o zagrożeniach bezpieczeństwa i (wg nowej koncepcji) Raport o zagrożeniach cyberbezpieczeństwa. Przy Radzie Ministrów powinien funkcjonować Rządowy Zespół Zarządzania Kryzysowego (RZZK), będący organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego i cyberbezpieczeństwa. Przy Radzie Ministrów powinno działać Kolegium ds. cyberbezpieczeństwa (Kolegium) jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. Do zadań Kolegium powinno należeć opracowywanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz wyrażanie opinii w sprawach kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa, wykonywania przez CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa i organy właściwe powierzonych im zadań, współdziałania organów prowadzących lub nadzorujących CSIRTy oraz współpracy z organami bezpieczeństwa, organizacji wymiany informacji istotnych dla cyberbezpieczeństwa RP, wniosków ws. rekomendacji stosowania sprzętu i oprogramowania. Prezes Rady Ministrów powinien przewodniczyć RZZK, Kolegium i nadzorować Rządowe Centrum Bezpieczeństwa.

Rządowe Centrum Bezpieczeństwa (RCB) powinno pełnić funkcję krajowego centrum zarządzania kryzysowego i być kluczowym podmiotem w systemie zarządzania bezpieczeństwem i cyberbezpieczeństwem państwa. RCB powinno zapewniać obsługę Rady Ministrów, Prezesa Rady Ministrów, RZZK i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz zapewniać obsługę Zespołu do spraw Incydentów Krytycznych. RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa. Realizując zadania Pełnomocnika Rządu ds. Cyberbezpieczeństwa powinno odpowiadać za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Do zadań RCB powinno należeć: analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV, opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa, upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym, inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa, wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT. Do zadań RCB wykonywanych w porozumieniu z właściwymi ministrami powinna należeć również współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi, podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa, podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu. RCB powinno przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie. RCB powinno opracowywać Krajowy Plan Zarzadzania Kryzysowego i (wg nowej koncepcji) Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC) lub (w miejsce obu wcześniej wymienionych) Krajowy Plan Za-

rzadzania Kryzysowego i Cyberbezpieczeństwa (KPZKC), Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i (wg nowej koncepcji) Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT) lub (w miejsce obu wcześniej wymienionych) Narodowy Program Ochrony Infrastruktury Krytycznej i Teleinformatycznej (NPOIKT) oraz Raport o zagrożeniach cyberbezpieczeństwa lub Raport o zagrożeniach bezpieczeństwa, w tym w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej. RCB powinno koordynować zadania Zespołu ds. Incydentów Krytycznych (ZIK), który powinien być organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz RCB. Dyrektor RCB powinien przewodniczyć pracom ZIK. ZIK powinien wyznaczać jednomyślnie CSIRT koordynujący obsługę incydentu, określać role pozostałych CSIRT oraz RCB w obsłudze incydentu, określać sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub CSIRT GOV, podejmować decyzje o wystąpieniu przez dyrektora RCB z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania RZZK. W przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze, powinien przygotowywać w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego. Organem pomocniczym Zespołu ds. Incydentów Krytycznych powinien być Pojedynczy Punkt Kontaktowy. RCB powinien realizować zadania Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa, do którego zadań należy m.in. komunikacja w zakresie zgłoszeń incydentów poważnych lub incydentów istotnych dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej pomiędzy pojedynczymi punktami kontaktowymi w innych państwach członkowskich Unii Europejskiej, a CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowymi zespołami cyberbezpieczeństwa, zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT, zapewnienie współpracy z Komisją Europejską w dziedzinie

cyberbezpieczeństwa, koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej. RCB powinno koordynować krajowe działania antykryzysowe i powinno być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. Rada Ministrów lub Prezes Rady Ministrów mogą zlecić RCB dodatkowe zadania związane z zarządzaniem kryzysowym i cyberbezpieczeństwem.

Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa powinni realizować, zgodnie z zakresem swojej właściwości, zadania dotyczące zarządzania kryzysowego i cyberbezpieczeństwa. Ministrowie i kierownicy na potrzeby realizacji zadań z zakresu zarządzania kryzysowego i cyberbezpieczeństwa powinni tworzyć zespoły zarządzania kryzysowego i centra zarządzania kryzysowego. Ministrowie pełniący funkcje organów właściwych ws. zarządzania kryzysowego i ws. cyberbezpieczeństwa powinni tworzyć sektorowe zespoły cyberbezpieczeństwa dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju i zapewnienia bezpieczeństwa państwa i administracji publicznej, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista możliwych CSIRT sektorowych. Ministrowie pełniący funkcje organów właściwych ws. zarządzania kryzysowego i ws. cyberbezpieczeństwa powinni ustanawiać i nadzorować, wg właściwości, operatorów infrastruktury krytycznej, operatorów usług kluczowy, dostawców usług cyfrowych oraz urzędy centralne i podmioty publiczne powoływanych ze znacznie szerszej niż aktualnie zdefiniowana liście sektorów i systemów kluczowych dla bezpieczeństwa państwa, jego administracji i systemów społeczno-gospodarczych.

W systemie cyberbezpieczeństwa powinny być powoływane Zespoły Reagowania na Incydenty Komputerowe poziomu krajowego (CSIRT NASK, CSIRT MON, CSIRT GOV), podległe ich właściwym organom zwierzchnim, tzn. odpowiednio CSIRT NASK - Ministrowi właściwemu ds. informatyzacji, CSIRT MON - Ministrowi Obrony Narodowej, CSIRT GOV - Szefowi ABW i dalej Ministrowi właściwemu ds. wewnętrznych (Ministrowi SWiA).

Wojewoda powinien być organem właściwym w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na terenie województwa. Wojewoda powinien wykonywać zadania

we współpracy z właściwymi organami administracji publicznej, operować za pomocą komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim oraz powoływanych wojewódzkiego zespołu zarządzania kryzysowego i wojewódzkiego centrum zarządzania kryzysowego. Zarząd województwa uczestniczy w realizacji zadań z zakresu zarządzania kryzysowego i cyberbezpieczeństwa, w tym planowania cywilnego, wynikających z jego kompetencji. Wojewoda i jego struktury (WCZK, WZZK) powinny być włączone przez RCB, CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Starosta jako przewodniczący zarządu powiatu powinien być organem właściwym w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na obszarze powiatu. Starosta powinien wykonywać swoje obowiązki za pomocą powiatowej administracji zespolonej i jednostek organizacyjnych powiatu oraz powoływanych powiatowego zespołu zarządzania kryzysowego i powiatowego centrum zarządzania kryzysowego. Starosta i jego struktury (PCZK, PZZK) powinny być włączone przez RCB, CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, struktury wojewody (WCZK), podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Wójt, burmistrz i prezydent miasta powinni być organami właściwymi w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na terenie gminy. Zadania powinni wykonywać przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego oraz powoływanych gminnego zespołu zarządzania kryzysowego i gminnego centrum zarządzania kryzysowego. Wójt, burmistrz i prezydent miasta i jego struktury (GCZK, GZZK) powinny być włączone przez sektorowe zespoły cyberbezpieczeństwa, struktury wojewody (WCZK), podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Operatorzy infrastruktury krytycznej - właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej, operatorzy usług kluczowy, dostawcy usług cyfrowych oraz urzędy centralne i podmioty publiczne powinny

mieć obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej, teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej, dokumentacji systemu zarządzania bezpieczeństwem systemów teleinformatycznych oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

4.5.2. Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym

Koncepcja zorganizowania struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP zakłada ujednolicenie i zharmonizowanie poprzez zintegrowanie struktur i relacji oraz kompetencji i ról organów i podmiotów zaangażowanych w realizację procesów i dokumentów zarządczych na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

Struktury i relacje zarządzania cyberbezpieczeństwem powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji zarządzania na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP powinny obejmować zagregowaną listę podmiotów realizujących procesy i dokumenty zarządcze, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

W składzie struktur zarządzania cyberbezpieczeństwem na poziomie krajowym powinny się znajdować następujące organy i podmioty:

- Prezes Rady Ministrów,
- Rada Ministrów,
- Rządowy Zespół Zarządzania Kryzysowego,
- Dyrektor Rządowego Centrum Bezpieczeństwa (RCB),
- Rządowe Centrum Bezpieczeństwa (RCB), mające w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa,
- ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego, organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON,
- zespoły zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych,
- minister właściwy do spraw administracji publicznej,
- minister właściwy do spraw wewnętrznych,
- Szef Agencji Bezpieczeństwa Wewnętrznego,
- wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego,
- starosta, powiatowy zespół zarządzania kryzysowego, wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego.

Struktury zarządzania systemu cyberbezpieczeństwa RP opracowane w ramach koncepcji w zestawieniu porównawczym ze strukturami zarządzania systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa przedstawione zostały w tabeli 35.

Tabela 35. Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i koncepcji systemu cyberbezpieczeństwa RP – ujęcie porównawcze

Struktury i relacje zarządzania cyberbezpieczeństwem – ujęcie porównawcze		
Rozwiązania aktualne		**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**System cyberbezpieczeństwa RP (SCRP) - Koncepcja**
Rada Ministrów	-	Prezes Rady Ministrów
Prezes Rady Ministrów		Rada Ministrów
Rządowy Zespół Zarządzania Kryzysowego (RZZK)		Rządowy Zespół Zarządzania Kryzysowego (RZZK)
Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)		Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)
Rządowe Centrum Bezpieczeństwa (RCB)		Rządowe Centrum Bezpieczeństwa (RCB), mające w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa
		organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON
ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych		ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych
zespoły zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych		zespoły zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych
Szef Agencji Bezpieczeństwa Wewnętrznego		Szef Agencji Bezpieczeństwa Wewnętrznego
Pełnomocnik Rządu ds. Cyberbezpieczeństwa		
wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK)		wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK)
starosta, powiatowy zespół zarządzania kryzysowego (PZZK)		starosta, powiatowy zespół zarządzania kryzysowego (PZZK)

wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK)		wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK)

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Koncepcja rozwiązań w zakresie struktur i relacji zarządzania cyberbezpieczeństwem zaangażowanych w realizację procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP przedstawiona została na rysunku 28.

Rys. 28. Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym – model relacji

Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym			
	POZIOMY WSPÓŁPRACY		
ZWIERZCHNOŚĆ	Rada Ministrów Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa – Krajowe centrum zarządzania kryzysowego, funkcje: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa
	Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych (centralne organy administracji rządowej) Ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa	Zespół zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych	Organ właściwy ds. cyberbezpieczeństwa Minister właściwy ds. informatyzacji, Ministrowie właściwi w sprawach bezpieczeństwa narodowego, Minister obrony narodowej MON, Minister właściwy ds. wewnętrznych ABW
	Wojewoda	Wojewódzki zespół zarządzania kryzysowego	Komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim
	Starosta	Powiatowy zespół zarządzania kryzysowego	Powiatowa administracja zespolona i jednostki organizacyjne powiatu
	Wójt, burmistrz, prezydent miasta	Gminny zespół zarządzania kryzysowego	Komórka organizacyjna urzędu gminy (miasta) właściwa w sprawach zarządzania kryzysowego

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Struktury zarządzania cyberbezpieczeństwem na poziomie krajowym zaangażowane są w realizację procesów i dokumentów zarządczych poziomu krajowego, takich jak Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej i ich odpowiedniki dedykowane cyberbezpieczeństwu, sformułowane w ramach koncepcji doskonalenia organizacji zarządzania cyberbezpieczeństwem w rozdziale trzecim. Struktury zarządzania cyberbezpieczeństwem sformułowane w ramach opracowanej koncepcji powinny być zaangażowane w realizację procesów i dokumentów zarządczych poziomu krajowego sformułowanych w ramach koncepcji doskonalenia organizacji zarządzania cyberbezpieczeństwem RP, wypracowanych w rozdziale trzecim.

W systemie zarządzania kryzysowego, w ramach realizacji procesów i dokumentów zarządczych poziomu krajowego zostały ustanowione: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe Plany Zarządzania Kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej oraz Raport o zagrożeniach bezpieczeństwa narodowego. Wg opracowanych, w ramach rozdziału trzeciego, koncepcji udoskonalonej organizacji zarządzania cyberbezpieczeństwem systemu cyberbezpieczeństwa RP (SCRP) odnoszącej się do procesów i dokumentów zarządczych sformułowano zestaw takich dokumentów zarządczych funkcjonujący równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim powiązana – co zostało zrealizowane poprzez ustanowienie dedykowanej, tożsamej struktury procesów i dokumentów zarządczych dla systemu cyberbezpieczeństwa RP, jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie, tj.: Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC), Plany Zarządzania Cyberbezpieczeństwem (PZC), Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT), Raport o zagrożeniach cyberbezpieczeństwa.

Zestawienie koncepcji struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do opracowanej, w ramach rozdziału trzeciego, struktury procesów i dokumentów zarządczych koncepcji zorganizowania zarządzania cyberbezpieczeństwem systemu cyberbezpieczeństwa RP (SCRP) przestawione jest w tabeli 36.

Tabela 36. Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem w odniesieniu do koncepcji dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP

Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do koncepcji dokumentów zarządzania cyberbezpieczeństwem	
Koncepcja dokumentów zarządzania cyberbezpieczeństwem (SCRP)	**Koncepcja struktur i relacji zarządzania cyberbezpieczeństwem (SCRP)**
Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC)	Rada Ministrów Prezes Rady Ministrów Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa)
Raport o zagrożeniach cyberbezpieczeństwa	Rada Ministrów Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa) Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Wojewoda Szef Agencji Bezpieczeństwa Wewnętrznego
Plan Zarządzania Cyberbezpieczeństwem (PZC) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych, ministrów odpowiedzialnych za systemy infrastruktury krytycznej, sektory krajowego systemu cyberbezpieczeństwa	Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa) Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Ministrowie odpowiedzialni za sektory i systemy IK
Plany Zarządzania Cyberbezpieczeństwem sektorowe, wojewódzkie, powiatowe, gminne	Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa) Minister właściwy do spraw administracji publicznej Minister właściwym do spraw wewnętrznych Wojewoda, starosta, wójt, burmistrz i prezydent miasta
Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT)	Rada Ministrów Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa) Ministrowie kierujący działami administracji rządowej Kierownicy urzędów centralnych Ministrowie właściwi w sprawach bezpieczeństwa narodowego Ministrowie odpowiedzialni za sektory i systemy IK

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Opracowana koncepcja struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP (SCRP) powinna adresować odpowiedzialność za realizację procesów i dokumentów zarządczych w odniesieniu do ich struktury w systemie zarządzania kryzysowego oraz w koncepcji doskonalenia organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP.

Za realizację Krajowego Planu Zarządzania Kryzysowego (KPZK) oraz odpowiadającego mu **Krajowego Planu Zarządzania Cyberbezpieczeństwem (KPZC)** powinny być odpowiedzialne: **Rada Ministrów, Prezes Rady Ministrów, Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa)**.

Za realizację ministerialnych, centralnych i sektorowych Planów Zarządzania Kryzysowego (PZK) oraz odpowiadających im **Planów Zarządzania Cyberbezpieczeństwem (PZC)** powinny być odpowiedzialne: **Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa), Ministrowie kierujący działami administracji rządowej, Kierownicy urzędów centralnych, Ministrowie odpowiedzialni za sektory i systemy IK**.

Za realizację regionalnych (wojewódzkich, powiatowych, gminnych) Planów Zarządzania Kryzysowego (PZK) oraz odpowiadających im **Planów Zarządzania Cyberbezpieczeństwem (PZC)** powinny być odpowiedzialne: **Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa), Minister właściwy do spraw administracji publicznej, Minister właściwym do spraw wewnętrznych, Wojewoda, starosta, wójt, burmistrz i prezydent miasta**.

Za realizację Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) oraz odpowiadających mu **Narodowego Programu Ochrony Infrastruktury Teleinformatycznej (NPOIT)** powinny być odpowiedzialne: **Rada Ministrów, Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa), Ministrowie kierujący działami administracji rządowej, Kierownicy urzędów centralnych, Ministrowie właściwi w sprawach bezpieczeństwa narodowego, Ministrowie odpowiedzialni za sektory i systemy IK**.

Za realizację **Raportu o zagrożeniach bezpieczeństwa narodowego** oraz odpowiadającego mu **Raportu o zagrożeniach cyberbezpieczeństwa** powinny być odpowiedzialne: **Rada Ministrów, Rządowe Centrum Bezpieczeństwa (z funkcjami Pełnomocnika**

Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa), Ministrowie kierujący działami administracji rządowej, Kierownicy urzędów centralnych, Wojewoda, Szef Agencji Bezpieczeństwa Wewnętrznego.

Przedstawione powyżej podejście pozwala zaadresować kwestię odpowiedzialności za realizację procesów i dokumentów zarządczych poziomu krajowego w systemie zarządzania kryzysowego oraz w koncepcji doskonalenia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP przez sformułowane w ramach niniejszego rozdziału koncepcyjne struktury i relacje zarządzania cyberbezpieczeństwem poziomu krajowego systemu cyberbezpieczeństwa RP.

4.5.3. Koncepcja struktur i relacji zarządzania incydentami cyberbezpieczeństwa

Koncepcja zorganizowania struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa zakłada ujednolicenie i zharmonizowanie poprzez zintegrowanie struktur i relacji oraz kompetencji i ról organów i podmiotów zaangażowanych w realizację procesów zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa na poziomie krajowym systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do infor-

mowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych. Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP (SCRP) powinny obejmować zagregowaną listę podmiotów realizujących zarządzanie sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

W składzie struktur zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa powinny się znajdować organy i podmioty:

- Prezes Rady Ministrów,
- Rada Ministrów,
- Rządowy Zespół Zarządzania Kryzysowego,
- Zespół ds. Incydentów Krytycznych,
- Dyrektor Rządowego Centrum Bezpieczeństwa (RCB),
- Rządowe Centrum Bezpieczeństwa (RCB), mające w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa
- ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego, organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON,
- CSIRTy poziomu krajowego (CSIRT NASK, CSIRT MON, CSIRT GOV),
- sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektowów),
- centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych,
- minister właściwy do spraw administracji publicznej,
- minister właściwy do spraw wewnętrznych,

- kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego,
- Szef Agencji Bezpieczeństwa Wewnętrznego,
- wojewoda, wojewódzkie centrum zarządzania kryzysowego,
- starosta, powiatowe centrum zarządzania kryzysowego,
- wójt, burmistrz, prezydent miasta, gminne centrum zarządzania kryzysowego,
- podmioty świadczące usługi z zakresu cyberbezpieczeństwa
- urzędy centralne i podmioty publiczne,
- operatorzy usług kluczowych,
- dostawcy usług cyfrowych,
- operator infrastruktury krytycznej – właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej.

Struktury zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP opracowane w ramach koncepcji w zestawieniu porównawczym ze strukturami zarządzania sytuacjami kryzysowymi systemu zarządzania kryzysowego i strukturami zarządzania cyberincydentami krajowego systemu cyberbezpieczeństwa przedstawione zostały w tabeli 37.

Tabela 37. Struktury i relacje zarządzania incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i koncepcji systemu cyberbezpieczeństwa RP – ujęcie porównawcze

Struktury i relacje zarządzania incydentami cyberbezpieczeństwa – ujęcie porównawcze		
Rozwiązania aktualne		**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**System cyberbezpieczeństwa RP (SCRP) – Koncepcja**
Rada Ministrów		Prezes Rady Ministrów
Prezes Rady Ministrów		Rada Ministrów
Rządowy Zespół Zarządzania Kryzysowego (RZZK)		Rządowy Zespół Zarządzania Kryzysowego (RZZK)
	Zespół ds. Incydentów Krytycznych	Zespół ds. Incydentów Krytycznych
	Pełnomocnik Rządu ds. Cyberbezpieczeństwa	
	Pojedynczy Punkt Kontaktowy	
Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)
Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB) (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa)
	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON
ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych odpowiedzialni za systemy infrastruktury krytycznej oraz właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych		ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministroiwe właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych
zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych		zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych
Szef Agencji Bezpieczeństwa Wewnętrznego	*Szef Agencji Bezpieczeństwa Wewnętrznego*	Szef Agencji Bezpieczeństwa Wewnętrznego
	CSIRT MON, CSIRT NASK, CSIRT GOV	CSIRT MON, CSIRT NASK, CSIRT GOV

	sektorowe zespoły cyberbezpieczeństwa	sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektorów)
kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego		kierownicy jednostek organizacyjnych, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego
wojewoda, wojewódzkie centrum zarządzania kryzysowego (WCZK)		wojewoda, wojewódzkie centrum zarządzania kryzysowego (WCZK)
starosta, powiatowe centra zarządzania kryzysowego (PCZK)		starosta, powiatowe centra zarządzania kryzysowego (PCZK)
wójt, burmistrz, prezydent miasta, gminne centrum zarządzania kryzysowego (GCZK)		wójt, burmistrz, prezydent miasta, gminne centrum zarządzania kryzysowego (GCZK)
		urzędy centralne i podmioty publiczne,
	podmioty świadczące usługi z zakresu cyberbezpieczeństwa	podmioty świadczące usługi z zakresu cyberbezpieczeństwa
operator infrastruktury krytycznej	operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny	operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny, operator infrastruktury krytycznej

Źródło: opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Koncepcja rozwiązań w zakresie struktur i relacji organów i podmiotów systemu cyberbezpieczeństwa RP zaangażowanych w zarządzanie sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa przedstawiona została na rysunku 29.

Rys. 29. Koncepcja struktur i relacji zarządzania incydentami cyberbezpieczeństwa – model relacji

<table>
<tr><th colspan="6">Koncepcja struktur i relacji zarządzania incydentami cyberbezpieczeństwa na poziomie krajowym</th></tr>
<tr><td></td><td colspan="5">POZIOMY WSPÓŁPRACY</td></tr>
<tr><td rowspan="8">ZWIERZCHNOŚĆ</td><td colspan="3">Rada Ministrów, Prezes Rady Ministrów</td><td colspan="2" rowspan="4"></td></tr>
<tr><td colspan="3">Rządowy Zespół Zarzadzania Kryzysowego (RZZK)</td></tr>
<tr><td colspan="3">Zespół ds. Incydentów Krytycznych</td></tr>
<tr><td colspan="3">Rządowe Centrum Bezpieczeństwa (RCB)
(funkcja: Krajowe Centrum Zarządzania Kryzysowego, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy)</td></tr>
<tr><td>CSIRT MON, CSIRT NASK, CSIRT GOV</td><td>Sektorowy zespół cyberbezpieczeństwa</td><td>Organ właściwy ds. cyberbezpieczeństwa</td><td></td><td></td></tr>
<tr><td>Ministrowie kierujący działami administracji rządowej,
Kierownicy urzędów centralnych
Ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa</td><td>Ministrowie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy ds. informatyzacji, minister obrony narodowej MON</td><td>Wojewoda</td><td>Starosta</td><td>Wójt, burmistrz, prezydent miasta</td></tr>
<tr><td>Centrum zarządzania kryzysowego</td><td>Centrum zarządzania kryzysowego</td><td>Wojewódzkie centrum zarządzania kryzysowego</td><td>Powiatowe centrum zarządzania kryzysowego</td><td>Gminne centrum zarządzania kryzysowego</td></tr>
<tr><td colspan="3">Podmiot świadczący usługi z zakresu cyberbezpieczeństwa</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="3">Operatorzy infrastruktury krytycznej
Operator usługi kluczowej
Dostawca usługi cyfrowej
Podmiot publiczny</td></tr>
</table>

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rada Ministrów powinna sprawować zarządzanie bezpieczeństwem, w tym zarządzanie kryzysowe i zarządzanie cyberbezpieczeństwem na terytorium Rzeczypospolitej Polskiej. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe powinien sprawować minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Przy Radzie Ministrów powinien funkcjonować Rządowy Zespół Zarządzania Kryzysowego (RZZK), będący organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego i cyberbezpieczeństwa. Rządowy Zespół Zarządzania Kryzysowego

powinien pełnić zwierzchnią rolę w zarządzaniu sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa. RZZK jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego i cyberbezpieczeństwa powinien przygotowywać propozycje użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych i incydentów cyberbezpieczeństwa, doradzać w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych i incydentów cyberbezpieczeństwa, opiniować sprawozdania końcowe z działań podejmowanych w związku z zarządzaniem kryzysowym i obsługą incydentów cyberbezpieczeństwa, opiniować potrzeby w zakresie odtwarzania infrastruktury teleinformatycznej lub przywrócenia jej pierwotnego charakteru. Prezes Rady Ministrów powinien przewodniczyć RZZK i nadzorować Rządowe Centrum Bezpieczeństwa. Dyrektor RCB powinien pełnić funkcję sekretarza RZZK.

Rządowe Centrum Bezpieczeństwa (RCB) powinno pełnić funkcję krajowego centrum zarządzania kryzysowego i być kluczowym podmiotem w systemie zarządzania bezpieczeństwem i cyberbezpieczeństwem państwa. RCB powinno zapewniać obsługę Rady Ministrów, Prezesa Rady Ministrów, RZZK i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego i cyberbezpieczeństwa oraz zapewniać obsługę Zespołu do spraw Incydentów Krytycznych. RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa. RCB powinno koordynować zadania Zespołu ds. Incydentów Krytycznych (ZIK), który powinien być organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz RCB. Dyrektor RCB powinien przewodniczyć pracom ZIK. ZIK powinien wyznaczać jednomyślnie CSIRT koordynujący obsługę incydentu, określać role pozostałych CSIRT oraz RCB w obsłudze incydentu, określać sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub CSIRT GOV, występować z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania RZZK. W przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej

lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze, RCB powinien przygotowywać w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego. Organem pomocniczym Zespołu ds. Incydentów Krytycznych powinien być Pojedynczy Punkt Kontaktowy. RCB powinien realizować zadania Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa, do którego zadań należy m.in. komunikacja w zakresie zgłoszeń incydentów poważnych lub incydentów istotnych dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej pomiędzy pojedynczymi punktami kontaktowymi w innych państwach członkowskich Unii Europejskiej, a CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowymi zespołami cyberbezpieczeństwa, zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT, zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa, koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej. RCB powinno koordynować krajowe działania antykryzysowe i cyberbezpieczeństwa, i powinno być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. RCB powinno monitorować potencjalne zagrożenia i cyberzagrożenia, przygotowywać uruchamianie, w przypadku zaistnienia zagrożeń i cyberzagrożeń, procedur związanych z zarządzaniem kryzysowym i cyberbezpieczeństwem. RCB powinno przygotowywać projekty opinii i stanowisk RZZK, przygotowywać i obsługiwać techniczno-organizacyjnie prace RZZK, zapewniać koordynację polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej i incydentów cyberbezpieczeństwa, współdziałać z podmiotami, komórkami i jednostkami organizacyjnymi NATO i UE oraz innymi organizacjami międzynarodowymi, odpowiedzialnymi za zarządzanie kryzysowe, cyberbezpieczeństwo i ochronę infrastruktury krytycznej, teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, pu-

bliczne i społeczno-gospodarcze, zapewniać obieg informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego i cyberbezpieczeństwa, realizować zadania stałego dyżuru w ramach gotowości obronnej państwa, realizować zadania z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń i cyberzagrożeń o charakterze terrorystycznym i cyberterrorystycznym. RCB powinno współdziałać z centrami zarządzania kryzysowego organów administracji publicznej, CSIRTami poziomu krajowego, sektorowymi zespołami cyberbezpieczeństwa, wojewódzkimi strukturami zarządzania kryzysowego i cyberbezpieczeństwa - WCZK. Rada Ministrów lub Prezes Rady Ministrów mogą zlecić RCB dodatkowe zadania związane z zarządzaniem kryzysowym i cyberbezpieczeństwem.

Ministrowie kierujący działami administracji rządowej i ich centra zarządzania kryzysowego, ministrowie właściwi ds. cyberbezpieczeństwa, ministrowie w sprawach zarządzania kryzysowego, kierownicy urzędów centralnych i ich centra zarządzania kryzysowego, CSIRTy poziomu krajowego, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa i ich sektorowe zespoły cyberbezpieczeństwa, wojewodowie i ich centra zarządzania kryzysowego oraz operatorzy infrastruktury krytycznej, operatorzy usługi kluczowej, dostawcy usługi cyfrowej, podmioty publiczne i ich wewnętrzne zespoły ds. cyberbezpieczeństwa lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa powinni niezwłocznie informować dyrektora RCB o zagrożeniach i cyberzagrożeniach, które mogą skutkować wystąpieniem na wskazanym obszarze, w sektorze czy systemie sytuacji kryzysowej lub incydentu cyberbezpieczeństwa.

Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa oraz ministrowie właściwi w sprawach bezpieczeństwa narodowego powinni realizować, zgodnie z zakresem swojej właściwości, zadania dotyczące zarządzania kryzysowego i obsługi incydentów, będąc organami właściwymi, są odpowiedzialni za systemy infrastruktury krytycznej i sektory systemu cyberbezpieczeństwa.

Organy właściwe do spraw cyberbezpieczeństwa (ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa) powinny ustanawiać sektorowe zespoły cyberbezpieczeństwa (CSIRT sektorowe) dla każdego systemu, sektora lub podsektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana możliwa lista CSIRT sektorowych. CSIRT sektorowe

powinny być odpowiedzialne w szczególności za przyjmowanie zgłoszeń o incydentach poważnych i istotnych oraz wsparcie w obsłudze tych incydentów, wspieranie operatorów infrastruktury krytycznej, operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych i urzędów centralnych w wykonywaniu ich obowiązków, powinny być odpowiedzialne za analizowanie incydentów, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu oraz za współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów.

CSIRTy poziomu krajowego (CSIRT MON, CSIRT NASK, CSIRT GOV) powinny współpracować ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz RCB pełniącym funkcję Pełnomocnika Rządu ds. Cyberbezpieczeństwa, zapewniać spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizować zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniać koordynację obsługi zgłoszonych incydentów.

Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV powinno należeć m.in.:

1. monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
2. szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
3. przekazywanie informacji dotyczących incydentów i ryzyk podmiotom systemu cyberbezpieczeństwa;
4. wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
5. reagowanie na zgłoszone incydenty;
6. klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
7. współpraca przy obsłudze incydentów wymagającej koordynacji;
8. współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;
9. wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, dotyczącej cyberbezpieczeństwa;
10. zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego cyberbezpieczeństwa;

11. wspólne opracowywanie głównych elementów procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga współpracy CSIRT oraz określanie we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposobu współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

CSIRT MON, CSIRT NASK i CSIRT GOV powinny współpracować i przekazywać sobie wzajemnie informacje o incydencie krytycznym oraz informować o nim Rządowe Centrum Bezpieczeństwa. Informacja powinna zawierać wstępną analizę potencjalnych skutków incydentu oraz ewentualnie rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego lub wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych.

RCB, CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa powinny przekazywać informację o zagrożeniach i incydentach cyberbezpieczeństwa oraz angażować do zarządzania incydentami wojewodę, starostę, wójta, burmistrza, prezydenta miasta i ich struktury dedykowane do zarządzania kryzysowego i cyberbezpieczeństwa.

Wojewoda powinien być organem właściwym w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na terenie województwa. Wojewoda powinien wykonywać zadania we współpracy z właściwymi organami administracji publicznej, operować za pomocą komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim oraz powoływanych wojewódzkiego zespołu zarządzania kryzysowego i wojewódzkiego centrum zarządzania kryzysowego. Zarząd województwa uczestniczy w realizacji zadań z zakresu zarządzania kryzysowego i cyberbezpieczeństwa, w tym planowania cywilnego, wynikających z jego kompetencji. Wojewoda i jego struktury (WCZK, WZZK) powinny być włączone przez RCB, CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. Wojewoda powinien kierować monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń i cyberzagrożeń na terenie województwa, wnioskować o użycie pododdziałów lub oddziałów Sił Zbrojnych RP, doraźnych zgrupowań zadaniowych, Policji, Straży Granicznej lub Państwowej Straży Pożarnej do wykonywania zadań z zakresu zarządzania kryzysowego i cyberbezpieczeństwa. Wojewoda powinien zgłaszać informację o zagrożeniach i incydentach cyberbezpieczeństwa do RCB, sektorowych zespołów cyberbez-

pieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV oraz do starosty, wójta, burmistrza, prezydenta miasta. Wojewoda powinien zapobiegać, przeciwdziałać i usuwać skutki zdarzeń o charakterze terrorystycznym i cyberterrorystycznym, organizować wykonanie zadań z zakresu ochrony infrastruktury krytycznej i teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze. Wojewoda powinien gromadzić i przetwarzać dane oraz oceniać zagrożenia i cyberzagrożenia występujące na obszarze województwa, monitorować, analizować i prognozować rozwój zagrożeń i cyberzagrożeń na obszarze województwa, dostarczać niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa i cyberbezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego i wojewódzkiego centrum zarządzania kryzysowego, zespołu zarządzania kryzysowego i centrum zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz RCB, współpracować z powiatowymi zespołami i centrami zarządzania kryzysowego, zapewniać funkcjonowanie wojewódzkiego zespołu zarządzania kryzysowego i wojewódzkiego centrum zarządzania kryzysowego, realizować zadania stałego dyżuru w ramach gotowości obronnej państwa, planować wsparcie innych organów właściwych w sprawach zarządzania kryzysowego i cyberbezpieczeństwa. WZZK powinien oceniać występujące i potencjalne zagrożenia i cyberzagrożenia mogące mieć wpływ na bezpieczeństwo publiczne i prognozować te zagrożenia i cyberzagrożenia, przygotowywać propozycje działań i przedstawiać wojewodzie wnioski dotyczące wykonania, zmiany lub zaniechania działań ujętych w wojewódzkim planie zarządzania kryzysowego i cyberbezpieczeństwa, przekazywać do wiadomości publicznej informacje związane z zagrożeniami i cyberzagrożeniami.

Starosta jako przewodniczący zarządu powiatu powinien być organem właściwym w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na obszarze powiatu. Starosta powinien wykonywać swoje obowiązki za pomocą powiatowej administracji zespolonej i jednostek organizacyjnych powiatu oraz powoływanych powiatowego zespołu zarządzania kryzysowego i powiatowego centrum zarządzania kryzysowego. Starosta i jego struktury (PCZK, PZZK) powinny być włączone przez RCB, CSIRTy poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, struktury wojewody (WCZK), podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Wójt, burmistrz i prezydent miasta powinni być organami właściwymi w sprawach zarządzania kryzysowego i cyberbezpieczeństwa na terenie gminy. Zadania powinni wykonywać przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego oraz powoływanych gminnego zespołu zarządzania kryzysowego i gminnego centrum zarządzania kryzysowego. Wójt, burmistrz i prezydent miasta i jego struktury (GCZK, GZZK) powinny być włączone przez sektorowe zespoły cyberbezpieczeństwa, struktury wojewody (WCZK), podmioty systemu cyberbezpieczeństwa (OIK OUK, DUC, PP, UC), zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Operatorzy infrastruktury krytycznej - właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej, operatorzy usług kluczowy, dostawcy usług cyfrowych oraz urzędy centralne i podmioty publiczne powinny mieć obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej, teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych realizujących mające krytyczne znaczenie dla bezpieczeństwa i funkcjonowania państwa oraz utrzymania krytycznej działalności społecznej i gospodarczej usługi kluczowe, cyfrowe, publiczne i społeczno-gospodarcze, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej, dokumentacji systemu zarządzania bezpieczeństwem systemów teleinformatycznych oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

Obowiązek podjęcia działań w zakresie zarządzania kryzysowego i cyberbezpieczeństwa w związku z wystąpieniem incydentu cyberbezpieczeństwa mogącego skutkować sytuacją kryzysową powinien spoczywać na tym organie lub podmiocie, który pierwszy wykrył cyberzagrożenie lub incydent, lub otrzymał informację o wystąpieniu cyberzagrożenia. Organ lub podmiot ten niezwłocznie powinien informować o zaistniałym zdarzeniu organy lub podmioty odpowiednio wyższego i niższego szczebla, przedstawiając jednocześnie swoją ocenę sytuacji oraz informację o zamierzonych działaniach.

4.6. Podsumowanie i wnioski

W rozdziale czwartym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania struktur i relacji operacyjnych w systemie cyberbezpieczeństwa na

poziomie krajowym, sformułowanego jako pytanie badawcze: *jakie są aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić ich efektywność?* Rozstrzygnięcie problemu zostało przeprowadzone poprzez weryfikację w procesie badawczym przyjętej hipotezy pomocniczej stwierdzającej, że: *ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa*.

W celu weryfikacji hipotezy przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu struktur i relacji operacyjnych, struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym oraz struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa. Przedstawiono i omówiono zorganizowanie struktur i relacji operacyjnych zarządzania w systemie cyberbezpieczeństwa na poziomie krajowym w zakresie całościowych zaangażowanych struktur i relacji operacyjnych, struktur i relacji zarządzania bezpieczeństwem na poziomie krajowym oraz struktur i relacji zarządzania sytuacjami kryzysowymi i cyberincydentami w ujęciu dokumentów strategicznych i właściwych regulacji prawnych dwóch systemów bezpieczeństwa – systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Dla każdego z systemów – zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa: zidentyfikowano zaangażowane organy i podmioty struktur operacyjnych oraz opracowano dedykowane tym strukturom autorskie modele relacji, zidentyfikowano organy i podmioty struktur zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym oraz opracowano dedykowane nim mapowanie tych struktur na aktualne procesy i dokumenty organizacji zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego, zidentyfikowano organy i podmioty struktur zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa oraz opracowano dedykowane tym strukturom autorskie modele relacji.

W toku procesu badawczego dokonano analizy porównawczej rozwiązań struktur i relacji zarządzania na poziomie krajowym oraz zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego ustanawia struktury i ich relacje - m.in. organy i instytucje, odpowiedzialne za realizację procesów i dokumentacji planowania i zarządzania bezpieczeń-

stwem na poziomie krajowym oraz za zarządzanie sytuacjami kryzysowymi, w tym wynikającymi z incydentów cyberbezpieczeństwa oraz, że krajowy system cyberbezpieczeństwa, w związku z tym, że nie definiuje zagadnień zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do procesów i dokumentów zarządczych (co zostało wywiedzione w rozdziale 2), nie ustanawia takich struktur i relacji zarządzania, natomiast ustanawia dedykowane struktury odpowiedzialnych organów i instytucji, i ich relacje w zakresie zarządzania incydentami cyberbezpieczeństwa. Przedstawiono w ujęciu porównawczym struktury i relacje organów i podmiotów zarządzania cyberbezpieczeństwem na poziomie krajowym obu systemów bezpieczeństwa wraz z mapowaniem tych struktur na procesy i dokumenty organizacji zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym. Przedstawiono także w ujęciu porównawczym struktury i relacje organów i podmiotów zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa każdego z systemów.

Przeprowadzono badania własne autora w zakresie zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa na poziomie krajowym i dokonano ich analizy. Wyniki badania wykazały, że aktualna organizacja struktur i relacji operacyjnych w zakresie zarządzania cyberbezpieczeństwem i zarządzania incydentami cyberbezpieczeństwa na poziomie krajowy nie jest właściwie zdefiniowana. Uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań i uzyskanych opinii od respondentów sformułowana została koncepcja zorganizowania struktur i relacji operacyjnych organów i podmiotów systemu cyberbezpieczeństwa RP na poziomie krajowym adresująca wyniki i wnioski z badania i oparta na hipotezie badawczej. Na podstawie przyjętej hipotezy, wyników badań, sformułowanych konkluzji i wniosków opracowano koncepcję zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym. W wyniku przeprowadzonych działań zostały opracowane trzy cząstkowe rozwiązania koncepcyjne, dedykowane zagadnieniom zorganizowania struktur i relacji w zakresach odpowiadających przeprowadzonej analizie i adekwatnych do zakresu przyjętej hipotezy i celu szczegółowego. Takie podejście jest zgodne z zakresem przeprowadzonej analizy organizacji struktur i relacji operacyjnych w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa w niniejszym rozdziale.

Na koncepcję zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym składają się koncepcje cząstkowe:

1. koncepcja zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP, stanowiąca kompilację wywodzących się z nich struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowych i zarządzania incydentami cyberbezpieczeństwa, dla której zdefiniowano wytyczne organizacyjne, zakres angażowanych organów i podmiotów, opracowano autorski model relacji oraz zestawienie porównawcze z obecnymi strukturami systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa;
2. koncepcja zorganizowania struktur i relacji z zarządzania cyberbezpieczeństwem na poziomie krajowym, dla której zdefiniowano wytyczne organizacyjne, zakres angażowanych organów i podmiotów, opracowano autorski model relacji, zestawienie porównawcze z obecnymi strukturami obu systemów bezpieczeństwa oraz opracowano dedykowane mapowanie tych struktur na koncepcyjną strukturę dokumentów procesów zarządzania cyberbezpieczeństwem na poziomie krajowym (wypracowaną w ramach rozdziału 3);
3. koncepcja zorganizowania struktur i relacji zarządzania incydentami cyberbezpieczeństwa, dla której zdefiniowano wytyczne organizacyjne, zakres angażowanych organów i podmiotów, opracowano autorski model relacji oraz zestawienie porównawcze z obecnymi strukturami systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

W wyniku przeprowadzonego procesu badawczego sformułowana hipoteza pomocnicza została pozytywnie zweryfikowana.

W ramach realizacji celu głównego rozprawy, którym jest: *opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa,* w ramach niniejszego rozdziału został zrealizowany cel szczegółowy rozprawy: *opracowanie koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.*

Opracowane rozwiązania koncepcji struktur i relacji operacyjnych, struktur i relacji z zarządzania cyberbezpieczeństwem oraz struktur i relacji zarządzania incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP poziomu krajowego spełniają sformułowane wnioski z badania i realizują cel szczegółowy rozprawy. Tym samym przyjęty cel szczegółowy został osiągnięty, przez co przyczynił się do osiągnięcia celu głównego rozprawy.

Rozdział V. SEKTORY I PODMIOTY SYSTEMU CYBERBEZPIECZEŃSTWA RP

System bezpieczeństwa państwa, w tym system cyberbezpieczeństwa, składa się ze zintegrowanych ze sobą systemu kierowania i systemów wykonawczych – operacyjnych i wsparcia. Podsystemy wsparcia definiowane są jako podmioty społeczne i gospodarcze przeznaczone do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania (zapobiegania i przeciwstawiania się) zewnętrznym i wewnętrznym zagrożeniom o charakterze społecznym i gospodarczym, a także do społecznego i gospodarczego zasilania operacyjnych podsystemów bezpieczeństwa narodowego w czasie pokoju, kryzysu i wojny. Podmioty te, z uwzględnieniem ich specyfiki i profilu, zostały zorganizowane w systemy infrastruktury krytycznej w systemie zarządzania kryzysowego i w sektory krajowego systemu cyberbezpieczeństwa. System informatyzacji podmiotów publicznych, zgodnie ze swoją nazwą obejmuje podmioty realizujące zadania publiczne. Typy podmiotów włączone do podsystemów bezpieczeństwa w ramach systemów i sektorów są niespójne, nie są ze sobą powiązane i zintegrowane, w dużej części się nie pokrywają, przez co nie adresują pełnego zakresu zagadnień bezpieczeństwa teleinformatycznego. Taki stan skutkuje tym, że nie może być zapewniony odpowiedni poziom cyberbezpieczeństwa kraju na najniższym, operacyjnym poziomie, będącym najbliżej osób, instytucji i podmiotów przestrzeni społecznej, gospodarczej, politycznej i prawnej. Rozwiązania te nie kształtują koncepcji systemu bezpieczeństwa państwa uwzględniającego i wyodrębniającego zintegrowany podsystem cyberbezpieczeństwa i jego integralny i transsektorowy charakter. System bezpieczeństwa powinien zapewniać funkcjonalny system cyberbezpieczeństwa w całościowym systemie bezpieczeństwa państwa, jego kompleksowy, całościowy model w praktycznym i aplikowalnym ujęciu metodycznym i strukturalnym, wskazując niezbędne w takim systemie systemy, sektory i typy podmiotów niezbędne dla efektywnego zapewnienia bezpieczeństwa teleinformatycznego i zarządzania cyberincydentami i sytuacjami kryzysowymi. Podmioty systemów bezpieczeństwa realizują zadania w zakresie zapewnienia bezpieczeństwa usług

publicznych i społecznych, i infrastruktury tych usług poprzez zapewnienie bezpieczeństwa infrastruktury systemów teleinformatycznych oraz reagowanie i zarządzanie cyberincydentami i sytuacjami kryzysowymi, w tym wynikającymi z materializacji cyberzagrożeń. Skuteczny i efektywny system cyberbezpieczeństwa państwa powinien obejmować całą jego przestrzeń i strukturę polityczno-społeczno-gospodarczą niezbędną dla zapewnienia bezpieczeństwa państwa i powinien być realizowany w wielu płaszczyznach przez sektor publiczny, komercyjny, obywatelski oraz w wymiarze transsektorowym. Uwzględnienie w systemie cyberbezpieczeństwa właściwych, niezbędnych sektorów, systemów i typów podmiotów w nim operujących może być czynnikiem determinującym poziom bezpieczeństwa państwa. Zdaniem autora *objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.*

Celem niniejszego rozdziału, w kontekście celu rozprawy, jest realizacja jej celu szczegółowego *opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP.* W niniejszym rozdziale dokonano próby rozstrzygnięcia problemu badawczego dotyczącego doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa poprzez weryfikację przyjętej hipotezy pomocniczej. W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu systemów, sektorów i typów podmiotów w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych oraz dokonano ich analizy porównawczej. Przedstawiono również wyniki przeprowadzonych badań własnych autora w tym zakresie, przedstawiające stanowiska respondentów nt. efektywności dotychczasowych oraz rozważanych w badaniu nowych rozwiązań, adresujących przyjęte założenia objęcia systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego oraz dokonano ich analizy. Została opracowana i przedstawiona autorska koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP, adresująca wyniki badania.

Kwestia doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa państwa przedstawiona jest w niniejszym rozdziale rozprawy z perspektywy trzech funkcjonujących w Polsce systemów, adresujących kwestie cyberbezpieczeństwa, w ujęciu wybranych aspektów dotyczących problematyki niniejszego rozdziału, zdefiniowanych przez dokumenty strategiczne i stosowne regulacje prawne dotyczące zarządzania kryzysowego – tworzące system zarządzania kryzysowego, dotyczące krajowego systemu cyberbezpieczeństwa – tworzące krajowy system cyberbezpieczeństwa i dotyczące informatyzacji podmiotów realizujących zadania publiczne – tworzące system informatyzacji podmiotów publicznych.

5.1. Sektory i podmioty systemu cyberbezpieczeńswa

Kwestie doboru sektorów i typów podmiotów objętych systemem cyberbezpieczeństwa państwa, zostaną rozpatrzone w ujęciu trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych. Charakterystyka systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych została przedstawiona w rozdziale 2.6 pracy. W niniejszym rozdziale zostaną zaprezentowane rozwiązania systemowe tych regulacji w zakresie szczególnych rozwiązań doboru sektorów i typów podmiotów systemu bezpieczeństwa.

System zarządzania kryzysowego jest rozpatrywany z perspektywy zależności bezpieczeństwa na poziomie krajowym od bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych wspierających funkcjonowanie usług systemów infrastruktury krytycznej, czyli cyberbezpieczeństwa tej infrastruktury i jej usług. Zarządzanie kryzysowe i planowanie cywilne w tym zakresie są rozumiane i rozpatrywane jako zarządzanie cyberbezpieczeństwem.

5.1.1. Systemy i podmioty systemu zarządzania kryzysowego

Ustawa o zarządzaniu kryzysowym[328] (Ustawa ZK) ustanawia infrastrukturę krytyczną, którą stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania

[328] Ustawa o zarządzaniu kryzysowym, wyd. cyt.

organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje 11 wskazanych systemów. Podmiotami systemu zarządzania kryzysowego są właściciele i posiadacze samoistni i zależni obiektów, instalacji, urządzeń infrastruktury krytycznej realizujący usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, czyli operatorzy infrastruktury krytycznej[329].

Operatorzy infrastruktury krytycznej jako właściciele i posiadacze samoistni i zależni obiektów, instalacji, urządzeń infrastruktury krytycznej realizujący usługi kluczowe, wyznaczani są spośród podmiotów systemów infrastruktury krytycznej, które obejmują następujące systemy zaopatrzenie w energię, surowce energetyczne i paliwa, łączność, sieci teleinformatyczne, finansowy, zaopatrzenie w żywność, zaopatrzenie w wodę, ochrona zdrowia, transport, ratownictwo, zapewniający ciągłość działania administracji publicznej, produkcja, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Dyrektor Rządowego Centrum Bezpieczeństwa sporządza we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług kluczowych wchodzących w skład infrastruktury krytycznej z podziałem na systemy, opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się w danym systemie i przekazuje je ministrom i kierownikom urzędów centralnych odpowiedzialnym za dany system oraz wyciągi z wykazu infrastruktury krytycznej, znajdującej się na terenie województw i przekazuje je właściwym wojewodom, a także informuje o ujęciu w wykazie infrastruktury krytycznej obiektów, instalacji lub urządzeń ich właścicieli, posiadaczy samoistnych i zależnych[330].

5.1.2. Sektory i podmioty krajowego systemu cyberbezpieczeństwa

Podmiotami krajowego systemu cyberbezpieczeństwa są operatorzy usług kluczowych, dostawcy usług cyfrowych, zespoły reagowania na incydenty komputerowe poziomu krajowego i sektorowe zespoły cyberbezpieczeństwa, specjalnie ustanowione organy po-

[329] tamże, art. 3
[330] tamże, art. 5b

ziomu centralnego, koordynujące kwestie cyberbezpieczeństwa, wybrane instytucje centralne, wybrane jednostki sektora finansów publicznych, wybrane spółki prawa handlowego realizujące zadania o charakterze użyteczności publicznej[331].

Podmiotami krajowego systemu cyberbezpieczeństwa nie ustanowiono przedsiębiorców telekomunikacyjnych, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów oraz dostawców usług zaufania, podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu[332].

Podmiotami krajowego systemu cyberbezpieczeństwa są operatorzy usług kluczowych, dostawcy usług cyfrowych, jednostki sektora finansów publicznych (wybrane), spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej (wybrane), instytuty badawcze, instytucje: NBP, BGK, UDT, PAŻP, PCA, NFOŚiGW, wojewódzkie FOŚiGW oraz podmioty świadczące usługi w zakresie cyberbezpieczeństwa.

Operatorzy usług kluczowych wyznaczani są spośród podmiotów operujących w sektorach wskazanych w ustawie, w dedykowanym załączniku[333]. Operatorzy usług kluczowych realizują usługi w ramach zdefiniowanych sektorów, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienione w wykazie usług kluczowych[334]. Dostawcy usług cyfrowych realizują usługi świadczone drogą elektroniczną, tj.: internetowa platforma handlowa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową, usługa przetwarzania w chmurze, która jest usługą umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników oraz wyszukiwarka internetowa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku odnośniki odnoszące się do informacji związanych z zapytaniem[335].

---

[331] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 4
[332] tamże, art. 1
[333] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., Załącznik nr1
[334] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. 2018 poz. 1806)
[335] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 2, Załącznik nr 2

Podmioty krajowego systemu cyberbezpieczeństwa wyznaczani są na podstawie zdefiniowanych kryteriów spośród podmiotów przynależnych do sektorów objętych systemem, wskazanych w załączniku do Ustawy KSC, tj.: energia, transport, bankowość i infrastruktury rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa.

Uwzględniając wszystkie kategorie podmiotów krajowego systemu cyberbezpieczeństwa można zdefiniować sektory tego systemu bezpieczeństwa, rozszerzające zakres sektorów wskazanych powyżej o sektory, z których pochodzą pozostałe kategorie podmiotów systemu, tj. usługi cyfrowe, podmioty publiczne i urzędy centralne (wybrane), usługi cyberbezpieczeństwa, które nie zostały wprost wskazane w Ustawie KSC. Rozszerzony wykaz sektorów krajowego systemu cyberbezpieczeństwa obejmuje sektory: energia, transport, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa, usługi cyfrowe, podmioty publiczne (finansów publicznych, użyteczności publicznej) i urzędy centralne (wybrane), usługi cyberbezpieczeństwa.

Organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli podmiot świadczy usługę kluczową, a świadczenie tej usługi zależy od systemów informacyjnych, a incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora. Organ właściwy do spraw cyberbezpieczeństwa może ustanowić sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora. Dostawcy usług cyfrowych oraz podmioty publiczne i urzędy centralne są wskazywane na podstawie warunków określonych w ustawie.

5.1.3. Podmioty systemu informatyzacji podmiotów publicznych

Podmiotami systemu informatyzacji podmiotów publicznych są wybrane podmioty publiczne i wybrane podmioty realizujące zadania publiczne, które zostały wskazane w Ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[336] (Ustawa IPP). Zgodnie z zapisami Ustawy IPP podmiotami są podmioty realizujące zadania publiczne oraz podmioty, którym podmioty publiczne powierzyły lub zleciły realizację zadania publicznego, jeżeli w związku z realizacją tego zadania istnieje obowiązek przekazywania informacji do lub od podmiotów niebędących organami administracji rządowej[337].

[336] Ustawa o informatyzacji, wyd. cyt.
[337] tamże, art. 2

Podmiotami systemu informatyzacji podmiotów publicznych są organy administracji rządowej, jednostki samorządu terytorialnego i ich organy, sądy i jednostki organizacyjne prokuratury, organy kontroli państwowej i ochrony prawa, jednostki budżetowe i samorządowe zakłady budżetowe (wybrane), państwowe lub samorządowe osoby prawne realizujące zadania publiczne (wybrane), podmioty, którym podmioty publiczne powierzyły lub zleciły realizację zadania publicznego, fundusze celowe, samodzielne publiczne zakłady opieki zdrowotnej oraz spółki wykonujące działalność leczniczą, Zakład Ubezpieczeń Społecznych (ZUS), Kasa Rolniczego Ubezpieczenia Społecznego (KRUS) i Narodowy Fundusz Zdrowia (NFZ), uczelnie i federacje podmiotów systemu szkolnictwa wyższego i nauki, instytuty badawcze, instytuty działające w ramach Sieci Badawczej Łukasiewicz oraz Polska Akademia Nauk (PAN), Polska Komisja Akredytacyjna (PKA) i Rada Doskonałości Naukowej (RDN). Podmioty publiczne, urzędy centralne i podmioty realizujące zadania publiczne są wskazywane na podstawie warunków określonych w Ustawie IPP.

Podmiotami systemu informatyzacji podmiotów publicznych nie są przedsiębiorstwa państwowe, spółki handlowe, służby specjalne, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezydenta Rzeczypospolitej Polskiej oraz Narodowy Bank Polski.

5.2. Analiza porównawcza rozwiązań w systemie cyberbezpieczeństwa RP

Podmioty systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych nie są tożsame, a różnice między nimi są duże. Wynika to z innego przeznaczenia tych systemów ich celów i zakresów funkcjonalnych, co skutkuje innym doborem sektorów i systemów oraz inaczej zbudowanej struktury podmiotów uczestniczących w zapewnieniu bezpieczeństwa teleinformatycznego i reagowaniu na incydenty cyberbezpieczeństwa czy sytuacje kryzysowe, bezpośrednio angażowanych i zobowiązanych do działania operacyjnego, a także innym potraktowaniem kwestii cyberbezpieczeństwa. Kwestie te realnie dotyczą znacznie szerszego kręgu sektorów i systemów oraz podmiotów gospodarczych, administracji publicznej, podmiotów publicznych i urzędów centralnych, niż zostało to zdefiniowane w regulacjach dotyczących analizowanych systemów bezpieczeństwa. Porównanie podmiotów wskazanych w regulacjach tych trzech systemów pozwala zidentyfikować podobieństwa i różnice oraz pozwala na próbę zdefiniowania najbardziej właściwej struktury i wykazu takich podmiotów w systemie cyberbezpieczeństwa RP.

Szczegółowe zestawienie porównawcze podmiotów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów publicznych zostało przedstawione w tabeli 38.

Tabela 38. Podmioty systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych – ujęcie porównawcze

Podmioty systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych – ujęcie porównawcze		
Zarządzanie kryzysowe	**Krajowy system cyberbezpieczeństwa**	**System informatyzacji podmiotów publicznych**
Operatorzy infrastruktury krytycznej	Operatorzy usług kluczowych	Organy administracji rządowej, jednostki samorządu terytorialnego i ich organy, sądy, jednostki organizacyjne prokuratury, organy kontroli państwowej i ochrony prawa
	Dostawcy usług cyfrowych	Fundusze celowe
	Jednostki sektora finansów publicznych (wybrane)	Jednostki budżetowe i samorządowe zakłady budżetowe, państwowe lub samorządowe osoby prawne realizujące zadania publiczne (wybrane)
	Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej (wybrane)	Podmioty, którym podmioty publiczne powierzyły lub zleciły realizację zadania publicznego
	Instytuty badawcze	Instytuty badawcze, instytuty działające w ramach Sieci Badawczej Łukasiewicz
	NBP, BGK, UDT, PAŻP, PCA, NFOŚiGW	ZUS, KRUS, NFZ
	Podmioty świadczące usługi w zakresie cyberbezpieczeństwa	Samodzielne publiczne zakłady opieki zdrowotnej oraz spółki wykonujące działalność leczniczą
		Uczelnie i federacje podmiotów systemu szkolnictwa wyższego i nauki
		Polska Akademia Nauk, Polska Komisja Akredytacyjna, Rada Doskonałości Naukowej

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

Podmioty systemów zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych funkcjonują w ramach i reprezentują sektory gospodarcze, działy administracji czy systemy infrastruktury krytycznej. Porównanie ich pozwala zidentyfikować podobieństwa i różnice, czyli zidentyfikowanie pokrycia tych samych obszarów oraz rozbieżności w tym zakresie, pozwala też na próbę zdefiniowania najbardziej właściwej ich struktury i wykazu w systemie cyberbezpieczeństwa RP.

Systemy zarządzania kryzysowego zawierają najszerszy zakres podmiotowy, co zapewnia najszerszy zakres bezpieczeństwa, w tym cyberbezpieczeństwa tych systemów. Podmioty systemu zarządzania kryzysowego realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Tak zdefiniowane usługi kluczowe mają znacznie szerszy zakres oddziaływania niż usługi kluczowe zdefiniowane w krajowym systemie cyberbezpieczeństwa, gdzie podmiotami są m.in. operatorzy usług kluczowych, które to usługi mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Usługi kluczowe krajowego systemu cyberbezpieczeństwa dotyczą wskazanych sektorów, które nie pokrywają się z systemami infrastruktury krytycznej, jest ich mniej, a tylko niektóre z nich się pokrywają i są wspólne dla obu systemów. Takie podejście generuje różny zakres obowiązków dla podmiotów tych sektorów i systemów i niejednorodny zakres rozwiązań bezpieczeństwa ich infrastruktury teleinformatycznej. W systemie informatyzacji podmiotów publicznych został zdefiniowany jeden sektor – podmiotów realizujących zadania publiczne – podmiotów publicznych i podmiotów, którym podmioty publiczne powierzyły realizację zadań publicznych. Jest to więc najwęższy przedmiotowo zakres podmiotów. Jednocześnie jest to sektor występujący we wszystkich rozpatrywanych systemach bezpieczeństwa. Należy zwrócić uwagę, że sektor podmiotów publicznych (wybranych) w krajowym systemie cyberbezpieczeństwa obejmuje inne podmioty publiczne i urzędy centralne (wybrane) niż system informatyzacji podmiotów publicznych i inne niż system zapewniający ciągłość działania administracji publicznej w systemie zarządzania kryzysowego. Każdy z systemów obejmuje inny zakres podmiotów publicznych. Podmioty te mają więc inne obowiązki w zakresie zapewnienia bezpieczeństwa wykorzystywanych systemów teleinformatycznych oraz zarządzania incydentami cyberbezpieczeństwa. Nie jest to sytuacja, która zapewnia odpowiedni poziom bezpieczeństwa krajowych podmiotów publicznych i ich systemów teleinformatycznych, będących częścią polskiej cyberprzestrzeni.

Tabela 39. Systemy i sektory systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych – ujęcie porównawcze

Systemy i sektory systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych – ujęcie porównawcze		
Systemy infrastruktury krytycznej (SZK)	**Sektory (KSC)**	**Sektor (SIPP)**
Zaopatrzenie w energię, surowce energetyczne i paliwa	Energia	
Łączność		
Sieci teleinformatyczne		
Finansowy	Bankowość i infrastruktury rynków finansowych	
Zaopatrzenie w żywność		
Zaopatrzenie w wodę	Zaopatrzenie w wodę	
Ochrona zdrowia	Ochrona zdrowia	
Transport	Transport	
Ratownictwo		
Zapewniający ciągłość działania administracji publicznej	Podmioty publiczne i urzędy centralne (wybrane)	Podmioty publiczne i urzędy centralne (wybrane) Podmioty realizujące zadania publiczne (wybrane)
Produkcja, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych		
	Infrastruktura cyfrowa	
	Usługi cyfrowe	
	Usługi cyberbezpieczeństwa	

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

Szczegółowe zestawienie porównawcze systemów i sektorów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych zostało przedstawione w tabeli 39.

Regulacje prawne obejmują swoim zakresem sektory podległych podmiotów. Biorąc pod uwagę, że objęte regulacjami sektory i usługi mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, są realizowane w celu ochrony interesu publicznego należałoby się spodziewać, że ich lista będzie obejmowała wszystkie istotne systemy i sektory w kraju oraz, że będzie spójna i tożsama we wszystkich regulacjach, jednakże tak nie jest. Istnieje istotna grupa systemów infrastruktury krytycznej nie uwzględnionych jako kluczowe sektory w systemie cyberbezpieczeństwa[338]. Dotyczy to takich systemów, jak systemy łączności i sieci teleinformatycznych[339], zaopatrzenia w żywność, ratowniczy czy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. W systemie cyberbezpieczeństwa pojawił się za to istotny sektor dla tego obszaru – sektor infrastruktury cyfrowej, który nie jest ujęty, jako system infrastruktury krytycznej oraz wybrane organy i podmioty publiczne i realizujące zadania publiczne, wybrane urzędy centralne, a także sektor usług cyfrowych. Podmioty sektora publicznego objęte są każdym z systemów w innym zakresie, co powoduje, że każda ich część ma inne wymagania np. dotyczące zapewnienia bezpieczeństwa systemów teleinformatycznych i inne obowiązki w zakresie bezpieczeństwa państwa.

Należy nadmienić, że wykaz sektorów systemu cyberbezpieczeństwa został określony w Załącznikach nr 1 i 2 Ustawy o krajowym systemie cyberbezpieczeństwa i Załączniku nr 2 Dyrektywy PE i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywie NIS)[340], która została wdrożona do polskiego porządku prawnego na mocy Ustawy o krajowym systemie cyberbezpieczeństwa.

---

[338] Mąkosa G., Cyberbezpieczeństwo, wyd. cyt., s. 121

[339] Na podst. art. 2 Ustawy o krajowym systemie cyberbezpieczeństwa nie ma ona zastosowania do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, dostawców usług zaufania, którzy podlegają wymogom art. 19 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym i podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu

[340] Dyrektywa NIS, Dz. U. UE L 194/1, wyd. cyt.

Zdaniem autora zasadnym jest, zgodnie ze zdefiniowaną hipotezą, dotyczącą przedmiotowych zagadnień niniejszego rozdziału, objęcie systemem cyberbezpieczeństwa RP najszerszego możliwego zakresu systemów, sektorów i typów podmiotów łącznie - wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego, co zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.

5.3. Wyniki przeprowadzonych badań

W ramach procesu badawczego, realizowanego w zakresie zagadnienia zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, stanowiącym przedmiotową problematykę niniejszego rozdziału, poddano weryfikacji hipotezę autora brzmiącą:

Objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.

Hipoteza została sformułowana jako odpowiedź na postawione pytanie badawcze:

Jakie sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP i jakie powinny zostać nim objęte, aby zapewnić jego efektywność i odpowiedni poziom bezpieczeństwa kraju?

W celu znalezienia odpowiedzi na postawione pytanie badawcze oraz zweryfikowania sformułowanej hipotezy, w procesie badawczym zostały postawione respondentom – ekspertom pytania, jak niżej:

3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?
   3.1. *Podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki*

administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) są właściwie zdefiniowane, co zapewnia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

3.2. *Krajowy system cyberbezpieczeństwa powinien obejmować znacznie szerszy katalog typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych.*

3.3. *Krajowy system cyberbezpieczeństwa powinien obejmować najszerszy możliwy katalog typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.*

3.4. *Proponowany w pkt. 3.3. powyżej najszerszy możliwy katalog typów podmiotów krajowego systemu cyberbezpieczeństwa jako mających odpowiednio duży wpływ na sferę administracyjno-społeczno-gospodarczą i bezpieczeństwa państwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinien obejmować podmioty typu:*

1) *Energetyka,*
2) *Łączność (usługi pocztowe i kurierskie),*
3) *Telekomunikacja i sieci teleinformatyczne,*
4) *Bankowość i infrastruktura rynków finansowych,*
5) *Sektor żywnościowy,*
6) *Wodociągi i kanalizacja,*
7) *Ochrona zdrowia,*
8) *Transport,*
9) *Ratownictwo,*
10) *Sektor chemiczny,*

11) *Przemysł / Produkcja,*
12) *Handel,*
13) *Usługi,*
14) *Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki,*
15) *Instytucje urzędów centralnych,*
16) *Sektor finansów publicznych,*
17) *Sektor usług komunalnych,*
18) *Sektor usług publicznych,*
19) *Sektor kosmiczny,*
20) *Nauka i szkolnictwo wyższe,*
21) *Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe),*
22) *Media (TV, radio, portale informacyjne),*
23) *Infrastruktura cyfrowa (DNS, IXP, TLD),*
24) *Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej),*
25) *Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.),*
26) *Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach,*
27) *Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/ Telekomunikacja),*
28) *Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa,*
29) *Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego,*
30) *Inny (jaki?) …*

W wyniku przeprowadzonego badania uzyskano od respondentów – ekspertów szereg odpowiedzi na postawione pytania. Analiza uzyskanych odpowiedzi na poszczególne pytania, wyrażone w tezach w nich zawartych, została przestawiona i omówiona poniżej tekście niniejszego podrozdziału.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 3.

Wynik badania w zakresie pytania 3.1.

Wobec tezy pytania 3.1.,

Podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) są właściwie zdefiniowane, co zapewnia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa,

wśród udzielonych przez respondentów odpowiedzi, 17 (37,77%) osób wyraziło zgodę z tezą, przy czym zdecydowana większość (15) raczej się zgodziła, nie jest to więc zgoda twarda, zdecydowana, natomiast 21 (46,67%) osób nie zgodziło się z tezą, przy czym zdecydowana większość (17) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci nie zgadzają się, a ściślej, raczej się nie zgadzają (21 głosami braku zgody, przy 17 głosach zgody), z tezą pytania.

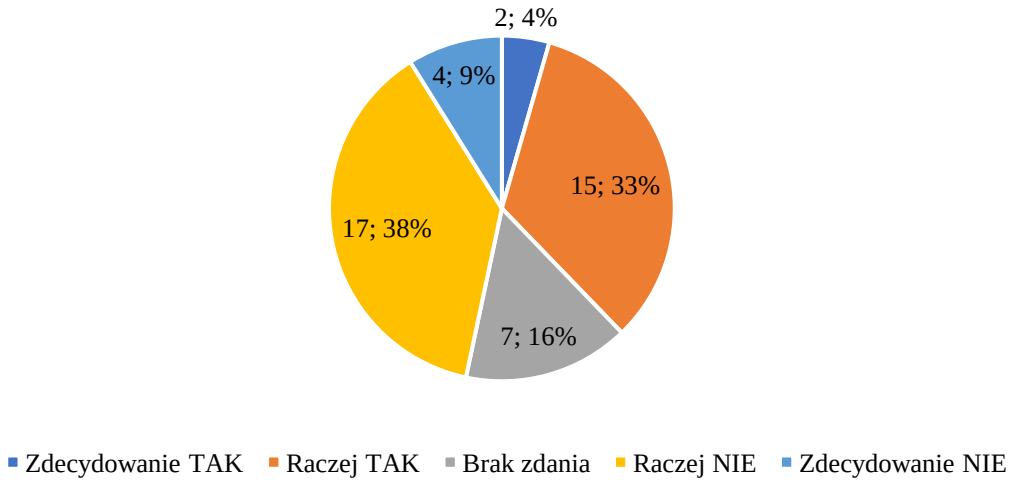
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 40 i na rysunku 30.

Tabela 40. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.1.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	17 / 21	2	15	7	17	4
%	100	37,77 / 46,67	4,44	33,33	15,56	37,78	8,89

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 30. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.1.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania wskazuje, że większość respondentów uważa, że podmioty krajowego systemu cyberbezpieczeństwa nie są właściwie zdefiniowane. Zachodzi więc konieczność zmiany zakresu tych podmiotów.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Przedstawione przez respondentów argumenty, opinie i komentarze do wybranych opcji odpowiedzi odnoszą się do ściśle do zagadnienia podległych sektorów oraz procesu wyboru podmiotów systemu cyberbezpieczeństwa. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających), i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Argumenty, opinie i komentarze respondentów **zgadzających się z tezą pytania** wskazywały, że w ustawie o krajowym systemie cyberbezpieczeństwa oraz w odpowiednich rozporządzeniach podmioty te zostały szczegółowo zdefiniowane wraz z kryteriami ich kwalifikacji, mających podstawy w prawie unijnym (Dyrektywie NIS), co zapewnia porównywalność z innymi państwami, uwzględnia potrzeby sektorowe i różnice w podejściu do krytyczności usług i stosowanych technologii. Respondenci wskazywali, że nie ma błędu w zdefiniowaniu podmiotów, nie są znane szczególne problemy związane z tym zdefiniowaniem, ani opinie o jakichś niedociągnięciach w zakresie podmiotów.

Respondenci **nie zgadzający się z tezą pytania** w swoich argumentach, komentarzach i opiniach zwracali uwagę, że zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Respondenci są zdania, że nie ma jasnego kryterium wyłaniania operatorów usług kluczowych, zdecydowanie zawyżono kryteria uznania w co najmniej kilku sektorach podmiotów będących OUK. Praktyka pokazuje wiele błędnie wydanych decyzji dla OUK i pomijanie podmiotów o znacznie większym wpływie na cyberbezpieczeństwo i instytucji niezwykle ważnych dla bezpieczeństwa ekonomicznego państwa, które nie zostały wskazane jako OUK. Aktualnie wśród pomiotów KSC brakuje m.in. przedsiębiorstw telekomunikacyjnych/komunikacji elektronicznej, podmiotów odpowiadających za rejestry państwowe, jednostki finansów publicznych i realizujących zadania publiczne. Błędnie są wskazywani OUK np. z sektorów energetycznego, wodociągów, szpitali. Sektor DUC również nie jest dobrze zdefiniowany. Respondenci zwrócili uwagę, że obecny system, gdzie OUK wskazywane są przez organ właściwy generuje z jednej strony prostotę, a z drugiej strony łatwe zwolnienie się części podmiotów z spełniania obowiązków, które powinny wypełniać. Podnoszono, że Dyrektywa NIS2 znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC. przyjęcie NIS2 między innymi ma rozwiązać problem z niespójnym definiowaniem OUK przez poszczególne państwa członkowskie. Podejście proponowane w NIS2 są w tym względzie dużo bardziej adekwatne. Rozszerzenie grup podmiotów, które niesie ze sobą dyrektywa NIS2 dodatkowo zwiększy spektrum wyzwań związanych z reorganizacją KSC, ale jednocześnie podniesie potencjalną efektywność systemu, którą będzie trzeba osiągnąć.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 3., ppkt 3.1.

Autor rozprawy podziela to zdanie i również nie zgadza się z tezą zawartą w pytaniu. Zdaniem autora podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) nie są właściwie zdefiniowane, co nie zapewnia efektywności krajowego systemu cyberbezpieczeństwa i odpowiedniego poziomu bezpieczeństwa państwa.

Wynik badania w zakresie pytania 3.2.

Wobec tezy pytania 3.2.,

Krajowy system cyberbezpieczeństwa powinien obejmować znacznie szerszy katalog typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych,

wśród udzielonych przez respondentów odpowiedzi, 33 (75%) osób wyraziło zgodę z tezą, przy czym minimalna większość (18) raczej się zgodziła, należy zatem uznać, że rozkład zdecydowanej i raczej zgody jest porównywalny i równomierny, natomiast 3 (0,07%) osoby nie zgodziło się z tezą, przy czym raczej się nie zgodziło.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zdecydowanie zgadzają się (33 głosami zgody, przy 3 głosach braku zgody), z tezą pytania.

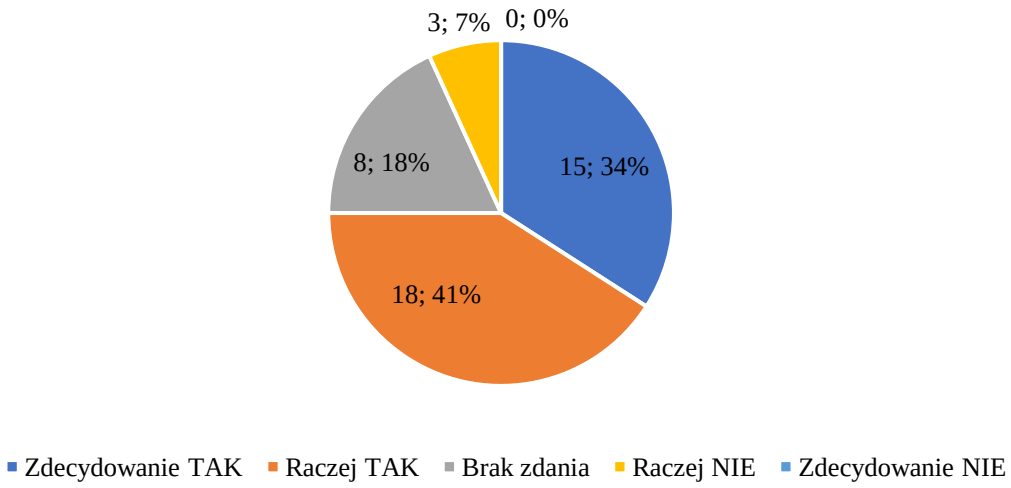
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 41 i na rysunku 31.

Tabela 41. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.2.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	44	33 / 3	15	18	8	3	0
%	100	75,00 / 0,07	34,09	40,91	18,18	6,82	0

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 31. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.2.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie pokazuje, że miażdżąca większość respondentów uważa, że katalog typów podmiotów powinien być znacznie szerszy, niż aktualnie zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w innych regulacjach bezpieczeństwa, a także zawierać szerszy katalog dostawców usług cyfrowych. Wynik badania wskazuje na konieczność zdefiniowania nowego, szerszego katalogu typów podmiotów systemu cyberbezpieczeństwa RP.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Przedstawione przez respondentów argumenty, opinie i komentarze do wskazanych odpowiedzi odnoszą się do ściśle do zagadnienia zakresu podległych sektorów systemu cyberbezpieczeństwa oraz innych obszarów bezpieczeństwa. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających), i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** twierdzili, że zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw i powiązań poszczególnych podmiotów, a w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych powodujących uznanie za OUK. Rozszerzenie katalogu podmio-

tów, a w zasadzie jego doprecyzowanie może pozytywnie wpłynąć na świadomość w obszarze cyberbezpieczeństwa. Zwrócono uwagę, że jeżeli wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa podmioty realizują zadania przy użyciu systemów informacyjnych, to powinny być ujęte we wskazanym katalogu. Podniesiono, że jest to merytorycznie uzasadnione i konieczne ze względu na wciąż poszerzający się zasięg cyfryzacji procesów i sposobu działania podmiotów, aby o cyberbezpieczeństwo dbały wszystkie istotne instytucje. Ważna jest ciągła aktualizacja obszarów IK równolegle z obszarami cyberbezpieczeństwa dla uzyskania niezbędnego efektu synergii. Wskazano, że aktualnie wśród pomiotów KSC brakuje m.in. przedsiębiorstw telekomunikacyjnych/komunikacji elektronicznej, podmiotów odpowiadających za rejestry państwowe, jednostki finansów publicznych i realizujących zadania publiczne, portali społecznościowych, portów lotniczych, miejskich sieci IT, które będąc słabo zabezpieczone narażają gminę lub miasto wraz z podłączonymi jednostkami, także innych sektorów nie scharakteryzowanych w ustawie. Błędnie są wskazywani OUK np. z sektorów energetycznego, wodociągów, szpitali. Sektor DUC również nie jest dobrze zdefiniowany. Zwrócono uwagę, że należy poczekać na wejście w życie dyrektywy unijnej NIS2, która znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC. przyjęcie NIS2 między innymi ma rozwiązać problem z niespójnym definiowaniem OUK przez poszczególne państwa członkowskie. Podejście proponowane w NIS2 są w tym względzie dużo bardziej adekwatne. Rozszerzenie grup podmiotów, które niesie ze sobą dyrektywa NIS2 dodatkowo zwiększy spektrum wyzwań związanych z reorganizacją KSC, ale jednocześnie podniesie potencjalną efektywność systemu, którą będzie trzeba osiągnąć.

Jako argument respondenta **nie zgadzającego się z tezą pytania** przedstawiono stwierdzenie, że nie każdy podmiot, który wykonuje ważne zadania (publiczne itp.) jednocześnie jest wrażliwy w dziedzinie cyberbezpieczeństwa.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 3., ppkt 3.2.

Autor rozprawy również w pełni zgadza się z tezą zawartą w pytaniu. Zdaniem autora system cyberbezpieczeństwa RP powinien obejmować znacznie szerszy katalog typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów

realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych.

Wynik badania w zakresie pytania 3.3.

Wobec tezy pytania 3.3.,

Krajowy system cyberbezpieczeństwa powinien obejmować najszerszy możliwy katalog typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego,

wśród udzielonych przez respondentów odpowiedzi, 28 (62,23%) osób wyraziło zgodę z tezą, przy czym minimalna większość (15) raczej się zgodziła, należy zatem uznać, że rozkład zdecydowanej i raczej zgody jest porównywalny i równomierny, natomiast 11 (24,44%) osób nie zgodziło się z tezą, zdecydowana większość (10) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zdecydowanie zgadzają się (28 głosami zgody, przy 11 głosach braku zgody), z tezą pytania.

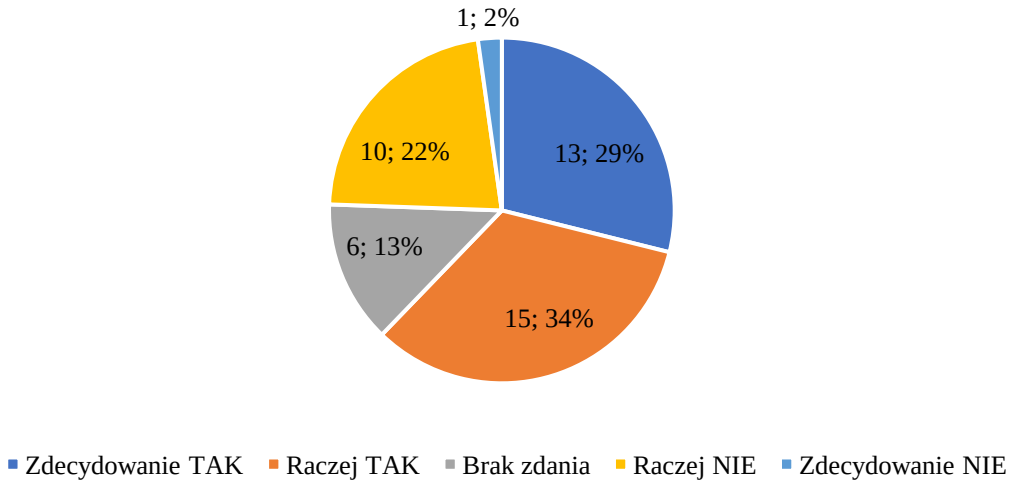
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 42 i na rysunku 32.

Tabela 42. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.3.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	28 / 11	13	15	6	10	1
%	100	62,23 / 24,44	28,90	33,33	13,33	22,22	2,22

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 32. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.3.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie wskazuje, że większość respondentów opowiada się za jak najszerszym katalogiem podmiotów objętych systemem cyberbezieczeństwa, zawierającym podmioty takie jak operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego. Wynik badania wskazuje na konieczność zdefiniowania nowego, możliwie najszerszego katalogu typów podmiotów systemu cyberbezpieczeństwa RP.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Przedstawione przez respondentów argumenty, opinie i komentarze do wskazanych odpowiedzi odnoszą się do ściśle do zagadnienia zakresu podległych sektorów systemu cyberbezpieczeństwa oraz innych obszarów bezpieczeństwa. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających), i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** twierdzili, że jest to merytorycznie uzasadnione i konieczne ze względu na wciąż poszerzający się zasięg cyfryzacji procesów i konieczność ochrony zasobów, aby o cyberbezpieczeństwo dbały wszystkie istotne instytucje. Respondenci uważają, że zakres podmiotów uznanych zwłaszcza za OUK powinien być

znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw i powiązań poszczególnych podmiotów, a w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw. Ważna jest ciągła aktualizacja obszarów IK równolegle z obszarami cyberbezpieczeństwa dla uzyskania niezbędnego efektu synergii. Rozszerzanie zakresu podmiotów systemu jest zasadne, lecz realizowane w wyniku procesu ewolucyjnego, a nie jednorazowej rewolucji. Zwrócono uwagę, że typowanie podmiotów poprzez ich nazwy nie zapewni właściwego poziomu bezpieczeństwa. Istotne są usługi, operatorzy usług i współzależności pomiędzy operatorami i podmiotami niezbędnymi do funkcjonowania operatorów, a cyberbezpieczeństwo to system naczyń połączonych. Podniesiono, że właściwie każdy podmiot na rynku (komercyjny, publiczny, NGO itd.) jest w obecnych czasach obecny w cyberprzestrzeni i narażony na cyberataki. Skuteczny atak nawet na z pozoru nieistotny podmiot może spowodować poważne braki usług, produktów, informacji i innych dóbr na rynku, a w konsekwencji – doprowadzić do dezinformacji, chaosu, przerwania łańcuchów dostaw itd. Skutki incydentu w podmiocie mającym duży wpływ będą odczuwalne dla bezpieczeństwa publicznego. Dlatego grono podmiotów powinno być maksymalnie szerokie. Systemowe monitorowanie możliwie szerokiego katalogu typów podmiotów (jednak opracowanego w oparciu o analizę ryzyka, a co za tym idzie bilans korzyści i kosztów) rozwija zdolności wczesnego wykrycia i analizy anomalii w sieci, a co za tym idzie skutecznego reagowania na incydenty. Zauważono, że cyberbezpieczeństwo z natury rzeczy jest sferą mocno powiązaną z obywatelem. Im głębiej system ochrony cyberbezpieczeństwa wnika w struktury państwa, tym lepiej dla obywatela.

Respondenci **nie zgadzający się z tezą pytania** stwierdzali, że powinny być jasne kryteria doboru podmiotów i nie ma potrzeby, aby rozszerzać system na wszystkie możliwe typy podmiotów, bo KSC i NIS dotyczą incydentów dużej skali mających wpływ na duże grono odbiorców. Wszyscy to też nie jest dobra rzecz, bo takie poszerzenie uczestników spowoduje przerost informacyjny. Zbyt szeroki zakres podmiotów mających obowiązek notyfikacji do krajowych CSRIT może doprowadzić do wystąpienia szumu informacyjnego i odwrócenia uwagi od ryzyk faktycznie mogących naruszyć cyberbezpieczeństwo. Zauważono, że katalog podmiotów powinien być poszerzony, ale należałoby zapewnić stopniowanie obowiązków. Musi również być wzięty pod uwagę rachunek ekonomiczny.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 3., ppkt 3.3.

Autor rozprawy w pełni zgadza się z postawioną tezą. Zdaniem autora system cyberbezpieczeństwa RP powinien obejmować najszerszy możliwy katalog typów podmiotów,

klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.

Wynik badania w zakresie pytania 3.4.

Wobec pytania 3.4. podejmującego problem zdefiniowania sektorów czy typów podmiotów, które miałyby być objęte systemem cyberbezpieczeństwa RP w przypadku ewentualnego ponownego ustawowego ich ustanawiania, zdefiniowany w ramach tezy pytania 3.3.:

Proponowany w pkt. 3.3. powyżej najszerszy możliwy katalog typów podmiotów krajowego systemu cyberbezpieczeństwa, jako mających odpowiednio duży wpływ na sferę administracyjno-społeczno-gospodarczą i bezpieczeństwa państwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinien obejmować podmioty typu: jako wariant wyboru,

respondenci udzielili odpowiedzi w stosunku do wszystkich wyszczególnionych kategorii. Analiza zbiorczych wyników udzielonych odpowiedzi wykazała, że w grupach sektorów i typów podmiotów, koniecznych do objęcia systemem cyberbezpieczeństwa RP, z poparciem w przedziałach wartości, znalazły się:

1) w zakresie 95-100% głosów - 10 sektorów: energetyka, **telekomunikacja i sieci teleinformatyczne**, bankowość i infrastruktura rynków finansowych, wodociągi i kanalizacja, ochrona zdrowia, **instytucje urzędów centralnych**, infrastruktura cyfrowa (DNS, IXP, TLD), usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**), środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach**, **dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/ Telekomunikacja)**. Wśród wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a które respondenci wskazali niemal jednogłośnie, w najwyższym stopniu. Jest zatem zdecydowane wskazanie na rozszerzenie zakresu oddziaływania systemu cyberbezpieczeństwa;
2) w zakresie 90-95% głosów - 4 sektory: transport, **ratownictwo**, **sektor chemiczny**, **dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa**. Wśród

wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a które respondenci wskazali w bardzo wysokim stopniu. Jest zatem zdecydowane wskazanie na rozszerzenie zakresu oddziaływania systemu cyberbezpieczeństwa;

3) w zakresie 80-90% głosów - 7 sektorów: **łączność (usługi pocztowe i kurierskie)**, **sektor żywnościowy**, **administracja publiczna (rządowa i samorządowa) – wszystkie jednostki**, **sektor finansów publicznych**, **sektor usług komunalnych**, **sektor usług publicznych**, **usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)**. Wśród wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem) lub są objęte częściowo, a które respondenci wskazali w wysokim stopniu. Jest zatem zdecydowane wskazanie na rozszerzenie zakresu oddziaływania systemu cyberbezpieczeństwa;
4) w zakresie 70-80% głosów - 2 sektory: **przemysł / produkcja** oraz **media (TV, radio, portale informacyjne)**. Wskazane sektory i typy dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a respondenci wskazali je w dość wysokim stopniu. Jest zatem zdecydowane wskazanie na rozszerzenie zakresu oddziaływania systemu cyberbezpieczeństwa;
5) w zakresie 60-70% głosów - 2 sektory: **sektor kosmiczny** oraz kategoria zdefiniowana jako wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego. Jest to kategoria otwarta, wymagająca przeprowadzenia odpowiednich analiz i podejmowania decyzji. Wskazany sektor kosmiczny nie jest objęty krajowym systemem cyberbezpieczeństwa (wyróżniony pogrubieniem), a respondenci wskazali go w znacznym stopniu. Jest to sektor rozwojowy i o znaczeniu strategicznym w każdym kraju. Jest zatem znaczące wskazanie na rozszerzenie zakresu oddziaływania systemu cyberbezpieczeństwa;
6) w zakresie 50-60% głosów - 3 sektory: **handel**, **nauka i szkolnictwo wyższe**, **instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)**. Żaden ze wskazanych sektorów nie jest objęty krajowym systemem cyberbezpieczeństwa (wyróżniony pogrubieniem), a respondenci wskazali go w średnim stopniu. Są to sektory wskazane do objęcia systemem cyberbezpieczeństwa;

7) w zakresie poniżej 50% głosów - 1 sektor: **usług**. Sektor ten nie jest objęty krajowym systemem cyberbezpieczeństwa. Respondenci bez przekonania i większości wskazali go do objęcia systemem cyberbezpieczeństwa, co wymaga przeprowadzenia odpowiednich analiz i podejmowania decyzji.

Wskazane i wyróżnione pogrubieniem sektory i typy dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa.

Warto zwrócić uwagę, że najwyższą pulę głosów (w przedziale 90-100%) za uznaniem, jako podmioty systemu cyberbezpieczeństwa RP uzyskały wszystkie już wskazane w Ustawie KSC sektory i typy podmiotów. W grupie typów podmiotów z najwyższą pulą głosów (w przedziale 90-100%) znalazły się również takie, które Ustawa KSC wprost wskazała jako nią nie objęte – wykluczyła je z krajowego systemu cyberbezpieczeństwa – tzn. sektory telekomunikacja i sieci teleinformatyczne, i środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach. Respondenci uznali, że są to sektory o kluczowym znaczeniu, podobnie jak pozostałe sektory nie uwzględnione w Ustawie KSC, a przez respondentów wskazane tak zdecydowanie: instytucje urzędów centralnych, dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja), ratownictwo, sektor chemiczny, dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa. Pozostałe wskazane sektory i typy podmiotów do włączenia do krajowego systemu cyberbezpieczeństwa, z pulą głosów poniżej 90%, stanowią już tylko sektory i typy podmiotów nie uwzględnione w Ustawie KSC, czyli sektory i typy podmiotów potencjalnie nowe w systemie, po ich uwzględnieniu.

Po 100% głosów uzyskały 4 zgłoszone przez respondentów w badaniu sektory, które otrzymały po jednym głosie, stanowiącym 100%. Niestety inni respondenci nie mogli się odnieść do tych propozycji, a sami też takich samych nie złożyli. Po bliższej analizie należy stwierdzić, że zaproponowane nowe propozycje sektorów i typów podmiotów mogłyby zostać zakwalifikowane do zdefiniowanych wcześniej kategorii.

Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 43 i na rysunku 33.

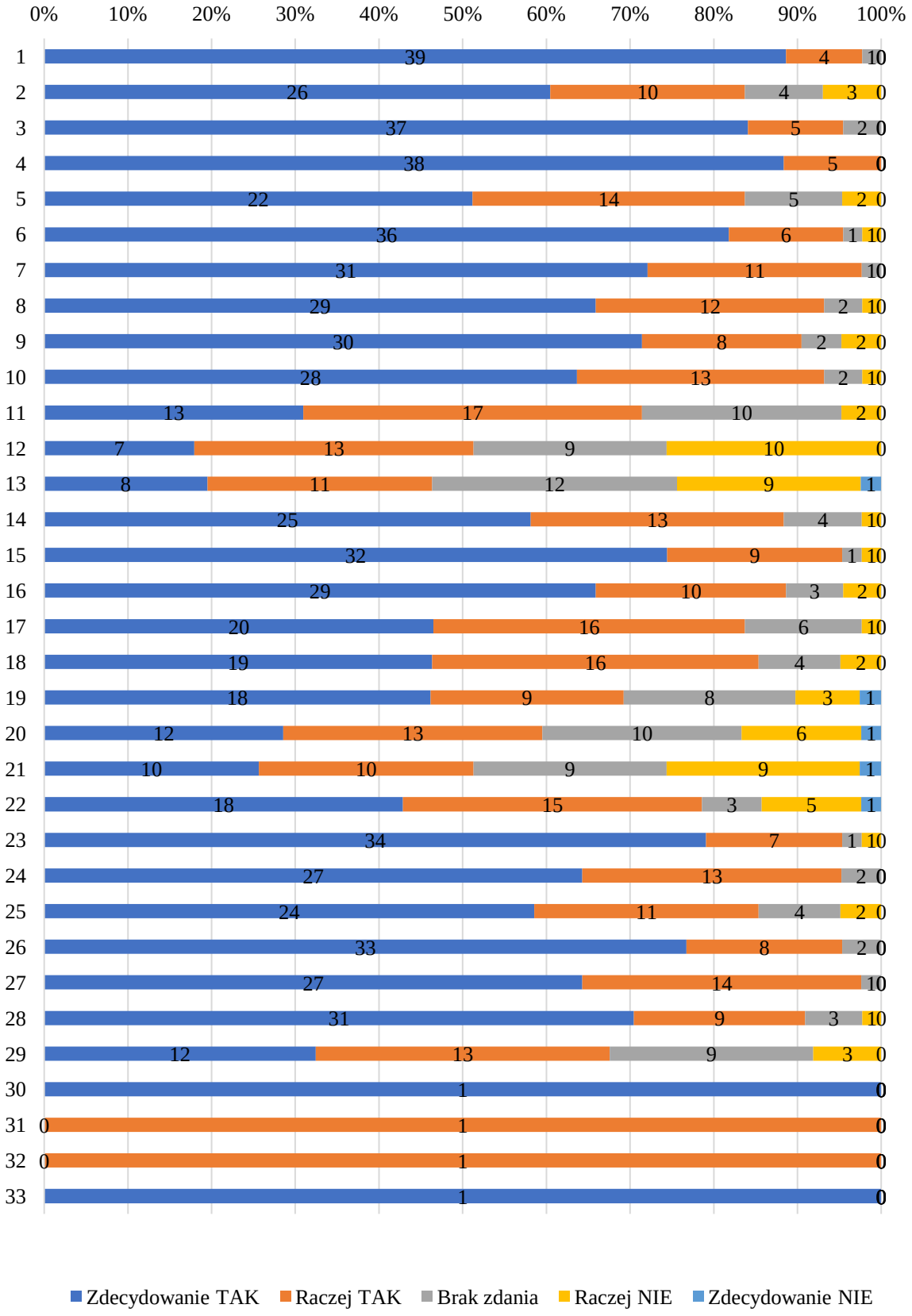
Tabela 43. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.4.

Lp.	Proponowane typy podmiotów krajowego systemu cyberbezpieczeństwa RP	Suma 1228	Wynik T / N Szt./%	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	Energetyka	44	43/0 97,73/ 2,27	39	4	1	0	0
2	Łączność (usługi pocztowe i kurierskie)	43	36/3 83,72/ 6,98	26	10	4	3	0
3	Telekomunikacja i sieci teleinformatyczne	44	42/0 95,45/0	37	5	2	0	0
4	Bankowość i infrastruktura rynków finansowych	43	43/0 100/0	38	5	0	0	0
5	Sektor żywnościowy	43	36/2 83,72/ 4,65	22	14	5	2	0
6	Wodociągi i kanalizacja	44	42/1 95,45/ 2,27	36	6	1	1	0
7	Ochrona zdrowia	43	42/0 97,67/0	31	11	1	0	0
8	Transport	44	41/1 93,18/ 2,27	29	12	2	1	0
9	Ratownictwo	42	38/2 90,48/ 4,76	30	8	2	2	0
10	Sektor chemiczny	44	41/1 93,18/ 2,27	28	13	2	1	0
11	Przemysł / Produkcja	42	30/2 71,43/ 4,76	13	17	10	2	0
12	Handel	39	20/10 51,28/ 25,64	7	13	9	10	0
13	Usługi	41	19/10 46,34/ 24,39	8	11	12	9	1
14	Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki	43	38/1 88,37/ 2,33	25	13	4	1	0
15	Instytucje urzędów centralnych	43	41/1 95,35/ 2,33	32	9	1	1	0
16	Sektor finansów publicznych	44	39/2 88,64/ 4,55	29	10	3	2	0
17	Sektor usług komunalnych	43	36/1 83,72/ 2,33	20	16	6	1	0
18	Sektor usług publicznych	41	35/2 85,37/ 4,88	19	16	4	2	0
19	Sektor kosmiczny	39	27/4 69,23/ 10,26	18	9	8	3	1

20	Nauka i szkolnictwo wyższe	42	25/7 59,52/ 16,67	12	13	10	6	1
21	Instytucje i ośrodki analityczne, doradcze, think-tanki	39	20/10 51,28/ 25,64	10	10	9	9	1
22	Media (TV, radio, portale informacyjne)	42	33/6 78,57/ 14,29	18	15	3	5	1
23	Infrastruktura cyfrowa (DNS, IXP, TLD)	43	41/1 95,35/ 2,33	34	7	1	1	0
24	Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**)**	42	40/0 95,24/0	27	13	2	0	0
25	Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)	41	35/2 85,37/ 4,88	24	11	4	2	0
26	Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach	43	41/0 95,35/0	33	8	2	0	0
27	Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekom.)	42	41/0 97,62/0	27	14	1	0	0
28	Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa	44	40/1 90,91/ 2,27	31	9	3	1	0
29	Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego	37	25/3 67,57/ 8,11	12	13	9	3	0
30	Inny (jaki?) rolnicy wielkoobszarowi	1	1/0 100/0	1	0	0	0	0
31	Inny (jaki?) organizacje/kościoły wspólnotowe i religijne	1	1/0 100/0	0	1	0	0	0
32	Inny (jaki?) NGO wpływające na opinię publiczną	1	1/0 100/0	0	1	0	0	0
33	Inny (jaki?) Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego lub usług kluczowych uczestniczące w łańcuchu dostaw dla nich	1	1/0 100/0	1	0	0	0	0

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 33. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 3.4.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Respondenci udzielili w sumie 1228 odpowiedzi. Z uwagi na tak dużą łączną liczbę uzyskanych głosów wobec od kilku do kilkudziesięciu głosów oddanych na poszczególny sektor czy typ podmiotu, analiza statystyczna nie znajduje racjonalnego uzasadnienia. Istotnym jest fakt, że oddawane głosy na poszczególne sektory czy typy podmiotów nie wykluczają pozostałych, odpowiedzi są komplementarne, uzupełniające się, a nie eliminacyjne, konkurujące. W takim przypadku zasadnym jest rozpatrywanie statystyczne ilości głosów pozytywnych i negatywnych w odniesieniu do każdego badanego sektora.

W odpowiedziach na postawione pytanie 3.4. odniesiono się do udzielonych głosów na tak lub na nie, ponieważ nie wszyscy respondenci zdecydowali się w ogóle udzielić odpowiedzi na to pytania, a spośród udzielających odpowiedzi, część oddała tylko pojedyncze głosy, wskazując wybrane sektory czy typy podmiotów, inni respondenci wskazywali każdy z sektorów czy typów przypisując go do wybranej opcji standardowej odpowiedzi. Stąd pod uwagę nie jest brana liczba respondentów, a liczba oddanych głosów w wyborze sektora czy typu podmiotu, co do ich uznania jako koniecznych do objęcia systemem cyberbezpieczeństwa RP.

Wynik badania w powyższym zakresie wskazuje, że pomimo różnic wśród respondentów, co do tego, które sektory powinny być objęte systemem cyberbezpieczeństwa dla zwiększenia jego zakresu, to finalnie zdecydowana większością respondentów uznała, że należy włączyć do systemu wszystkie wskazane w pytaniu sektory. Wynik badania wskazuje na konieczność zdefiniowania nowego, szerszego katalogu sektorów typów podmiotów systemu cyberbezpieczeństwa RP.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Ze względu na charakter pytania i specyfikę odpowiedzi, polegającej na wskazaniu preferowanych sektorów systemu cyberbezpieczeństwa, przedstawione przez respondentów argumenty, opinie i komentarze należy uznać za uniwersalne, nie odnoszące się do akceptacji lub braku akceptacji dla problemowego zagadnienia, lecz jako odniesienie się do dokonanego wyboru opcji odpowiedzi. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów do udzielonych odpowiedzi.

Respondenci w uzupełnieniu do dokonanego wyboru opcji odpowiedzi w przedstawionych argumentach, opiniach i komentarzach stwierdzają m.in., że większość wymienionych typów podmiotów już obecnie znajduje się w zakresie ustawy lub za chwilę się znajdzie w wyniku wejścia w życie Dyrektywy NIS2. Ponadto niektóre typy podmiotów ustawowo jednoznacznie wykluczono, wskazując na inne regulacje (np. podmioty podlegające prawu

telekomunikacyjnemu lub dostawców tożsamości) z niezbyt jasnych względów. Zaakcentowano, że trzeba mieć też na uwadze, że nadmierne rozszerzanie zakresu podmiotów w tym katalogu nie jest wskazane. Obecnie nawet wielu OUK nie wypełnia wymogów ustawowych, m.in. z powodu wysokich i kosztownych wymagań nałożonych rozporządzeniem ministra cyfryzacji na wewnętrzne zespoły, które powinny być powołane. Podmioty niechętnie sięgają też po usługi zewnętrznych dostawców cyberbezpieczeństwa. W pierwszej kolejności należy zacząć egzekwować obecnie obowiązujący system prawny, w razie potrzeby z zastosowaniem kar przewidzianych w ustawie. Postawiono zdanie, że zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy, jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Trzeba też zdefiniować odpowiednio duży wpływ poprzez katalog incydentów i wpływ skutków na funkcje państwa, a nie tylko specyfikę podmiotu. Podmioty - szczególnie komercyjne, przeliczają wszystko na pieniądze i nie mają obowiązku zwracania uwagi na zaburzenie w świadczeniu usług dla społeczeństwa, a jeśli mają, to weryfikują wielkość kar, jako skutek, a nie skutek dla ogółu, dlatego odpowiedzialność personalna karna z zakazem pracy w tego typu podmiotach dla zarządzających tymi podmiotami może zmienić podejście. Stwierdzono, że warto poszerzać katalog podmiotów, ale jednocześnie dołączać je do KSC w tempie, które uwzględni ich gotowość kompetencyjną oraz zapewni narzędzia potrzebne do współdziałania w KSC. Należy także rozważyć sposoby podnoszenia samoistnej odporności wymienionych podmiotów na potencjalne cyberzagrożenia. Państwo jest systemem naczyń połączonych, w tym przypadku systemami teleinformatycznymi. Zatem dysfunkcja jednego z nich ma oczywisty wpływ na pozostałe. Wielkość tego wpływu jest pochodną wielu czynników, jednakowoż bezwzględnie oddziaływają na siebie. W przypadku, gdy podmioty przetwarzają dane w systemach informacyjnych, to zdecydowanie powinny być włączone w krajowy system cyberbezpieczeństwa. Jednocześnie zwrócono uwagę, że przed wskazaniem sektora należy dokonać starannej analizy, na ile dany sektor jest uzależniony od sprawności systemów IT/OT oraz jakie są możliwości zmiany (tzn. na ile sektor działa lokalnie). Zauważono też, że dla większości podmiotów działających w gospodarce, bezpieczeństwo – niezależnie, czy cyber czy inne – jest kwestią apetytu na ryzyko. Państwo powinno interweniować, kiedy są zagrożone dobra publiczne, takie jak stabilność gospodarki czy dane osobowe obywateli, ale nie powinno to być automatyczne. Wraz ze wzrostem cyfryzacji obszarów życia i budowania cyfrowej tkaniny usług (services fabric), centralna rola państwa i tradycyjne obszary

„infrastruktury krytycznej" przechodzą transformację w system zdecentralizowany, wzajemnie zależny. Zauważono, że właściwie każdy podmiot na rynku (komercyjny, publiczny, NGO itd.) jest w obecnych czasach obecny w cyberprzestrzeni i narażony na cyberataki. Skuteczny atak nawet na z pozoru nieistotny podmiot może spowodować poważne braki usług, produktów, informacji i innych dóbr na rynku, a w konsekwencji – doprowadzić do dezinformacji, chaosu, przerwania łańcuchów dostaw itd. Dlatego grono podmiotów powinno być maksymalnie szerokie. Kluczowy jest łańcuch dostaw z określeniem krytyczności poszczególnych podmiotów. Krytyczne dla zapewnienia cyberbezpieczeństwa jest znajomość łańcucha powiązań poszczególnych podmiotów i w tym względzie w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw. Jedyna droga do najwyższej skuteczności działań i zapewnienia jak najwyższego poziomu bezpieczeństwa Państwa, to jak najpełniejsza synergia i integracja działań przy uwzględnieniu wszelkich możliwych obszarów funkcjonowania organizacji. Nie ma mowy o przeroście czegokolwiek w tych zagadnieniach. Podniesiono także, że cyberbezpieczeństwo to szerokie zagadnienie, którego punktem wyjścia jest budowa świadomości wokół zagrożeń cyberatakami. Obecność wszystkich obszarów państwa i wszystkich jednostek decydująca jest dla ukształtowania myśli obywatela o możliwościach wykorzystania cyberprzestrzeni przez wroga i kształtowania odpowiedniej świadomości i nawyków. Podkreślono, że wzmocnienie ustawowe kwalifikacji do najszerszego zakresu podmiotów systemu pozwoli umieszczą w budżetach instytucji środków na cyberbezpieczeństwo, co z kolei umożliwi realizację zadań z tego zakresu.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 3., ppkt 3.3.

Autor rozprawy w pełni zgadza się z uzyskanymi odpowiedziami respondentów. Zdaniem autora system cyberbezpieczeństwa RP powinien obejmować najszerszy możliwy katalog typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne i inne spośród wszystkich typów podmiotów, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego lub usług kluczowych, uczestniczących w łańcuchu dostaw dla nich.

5.4. Podsumowanie wyników badania

Wyniki przeprowadzonego badania realizowanego w zakresie zagadnienia zbioru sektorów i typów podmiotów systemu cyberbezpieczeństwa RP, stanowiącym przedmiotową problematykę niniejszego rozdziału pozytywnie zweryfikowały postawioną hipotezę stanowiącą, że: *objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.*

Wyniki badania pozwalają na sformułowanie wniosków do zastosowania w opracowaniu proponowanej koncepcji rozwiązań udoskonalenia zbioru sektorów i typów podmiotów systemu cyberbezpieczeństwa RP. Wnioski z wyników badania są następujące:

1. Podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) **nie są właściwie zdefiniowane, co nie zapewnia efektywności** krajowego systemu cyberbezpieczeństwa **i odpowiedniego poziom bezpieczeństwa** państwa.
2. System cyberbezpieczeństwa RP **powinien obejmować znacznie szerszy katalog** sektorów, systemów i typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych.
3. System cyberbezpieczeństwa RP **powinien obejmować najszerszy możliwy katalog** sektorów, systemów i typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.

4. Proponowany w pkt. 3 powyżej najszerszy możliwy katalog sektorów, systemów i typów podmiotów typów podmiotów systemu cyberbezpieczeństwa RP, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinien obejmować, w kolejności najczęstszych wskazań:
   1) ze zdecydowanym wskazaniem w zakresie 95-100% głosów - 10 sektorów: energetyka, **telekomunikacja i sieci teleinformatyczne**, bankowość i infrastruktura rynków finansowych, wodociągi i kanalizacja, ochrona zdrowia, **instytucje urzędów centralnych**, infrastruktura cyfrowa (DNS, IXP, TLD), usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**), środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach**, **dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/ Telekomunikacja)**. Wśród wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a które respondenci wskazali niemal jednogłośnie, w najwyższym stopniu;
   2) ze zdecydowanym wskazaniem w zakresie 90-95% głosów - 4 sektory: transport, **ratownictwo**, **sektor chemiczny**, **dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa**. Wśród wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a które respondenci wskazali w bardzo wysokim stopniu;
   3) z bardzo silnym wskazaniem w zakresie 80-90% głosów - 7 sektorów: **łączność (usługi pocztowe i kurierskie)**, **sektor żywnościowy**, **administracja publiczna (rządowa i samorządowa) – wszystkie jednostki**, **sektor finansów publicznych**, **sektor usług komunalnych**, **sektor usług publicznych**, **usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)**. Wśród wskazanych sektorów i typów są takie, które dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem) lub są objęte częściowo, a które respondenci wskazali w wysokim stopniu;
   4) z silnym wskazaniem w zakresie 70-80% głosów - 2 sektory: **przemysł / produkcja** oraz **media (TV, radio, portale informacyjne)**. Wskazane sektory i typy dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem), a respondenci wskazali je w dość wysokim stopniu;

5) ze znaczącym wskazaniem w zakresie 60-70% głosów - 2 sektory: **sektor kosmiczny** oraz kategoria zdefiniowana jako **wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego**. Jest to kategoria otwarta, wymagająca przeprowadzenia odpowiednich analiz i podejmowania decyzji. Wskazany sektor kosmiczny nie jest objęty krajowym systemem cyberbezpieczeństwa (wyróżniony pogrubieniem), a respondenci wskazali go w znacznym stopniu. Jest to sektor rozwojowy i o znaczeniu strategicznym w każdym kraju;
6) ze średnim wskazaniem w zakresie 50-60% głosów 3 sektory: **handel, nauka i szkolnictwo wyższe, instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)**. Wskazane sektory i typy dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa (wyróżnione pogrubieniem);
7) **nie powinien obejmować** podmiotów, do których respondenci odnieśli się bez przekonania - ze wskazaniem poniżej 50% głosów - **sektor usług**. Nie jest on objęty krajowym systemem cyberbezpieczeństwa i wymaga przeprowadzenia odpowiednich analiz i podejmowania decyzji, co do objęcia systemem cyberbezpieczeństwa RP.

Wskazane i wyróżnione pogrubieniem sektory i typy dotychczas nie są objęte krajowym systemem cyberbezpieczeństwa.

Definiując katalog sektorów, systemów i typów podmiotów systemu cyberbezpieczeństwa RP warto zwrócić uwagę, że najwyższą pulę głosów (w przedziale 90-100%) za uznaniem, jako podmioty systemu cyberbezpieczeństwa RP uzyskały wszystkie już wskazane w Ustawie KSC sektory i typy podmiotów. W grupie typów podmiotów z najwyższą pulą głosów (w przedziale 90-100%) znalazły się również takie, które Ustawa KSC wprost wskazała jako nią nie objęte – wykluczyła je z krajowego systemu cyberbezpieczeństwa – tzn. sektory telekomunikacja i sieci teleinformatyczne oraz środki tożsamości elektronicznej i rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach. Respondenci uznali, że są to sektory o kluczowym znaczeniu, podobnie jak pozostałe sektory nie uwzględnione w Ustawie KSC, a przez respondentów wskazane tak zdecydowanie: instytucje urzędów centralnych, dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja), ratownictwo, sektor chemiczny, dostawa usług i syste-

mów teleinformatycznych cyberbezpieczeństwa. Pozostałe wskazane sektory i typy podmiotów do włączenia do systemu cyberbezpieczeństwa RP, z pulą głosów poniżej 90%, stanowią już tylko sektory i typy podmiotów nie uwzględnione dotychczas w Ustawie KSC, czyli sektory i typy podmiotów potencjalnie nowe w systemie, po ich uwzględnieniu. Wśród nowych sektorów i typów podmiotów powinny się znaleźć: łączność (usługi pocztowe i kurierskie), sektor żywnościowy, administracja publiczna (rządowa i samorządowa) – wszystkie jednostki, sektor finansów publicznych, sektor usług komunalnych, sektor usług publicznych, usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.), przemysł / produkcja oraz media (TV, radio, portale informacyjne), sektor kosmiczny, handel, nauka i szkolnictwo wyższe, instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe) oraz kategoria zdefiniowana jako wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.

Kolejną istotną kwestią, niezbędną do uwzględnienia jest to, że aktualnie jako podmioty krajowego systemu cyberbezpieczeństwa w kategorii podmiotów publicznych, jest tylko mała część polskich urzędów centralnych, administracji publicznej, podmiotów użyteczności publicznej i finansów publicznych. Katalog typów podmiotów systemu cyberbezpieczeństwa RP powinien zawierać wszystkie systemy zdefiniowane w zarządzaniu kryzysowym i podmioty uznane za operatorów infrastruktury krytycznej oraz sektor publiczny i wszystkie podmioty tego sektora, w tym szczególnie wskazanych w ustawie o informatyzacji podmiotów realizujących zadania publiczne. Ustawa o informatyzacji podmiotów realizujących zadania publiczne (Ustawa IPP) obejmuje szerszą pulę podmiotów z tej kategorii, przy czym należy zaznaczyć, że są to inne podmioty, niż te w systemie cyberbezpieczeństwa. Ustawa IPP nakłada na objęte nią podmioty znacznie większe wymagania w zakresie zarządzania usługami systemów teleinformatycznymi i ich bezpieczeństwa teleinformatycznego niż Ustawa KSC na podmioty publiczne, a nawet na operatorów usług kluczowych. Instytucje i podmioty tego typu są niezmiernie ważne dla bezpieczeństwa państwa i usług publicznych, jest błędem nieuwzględnienie w systemie cyberbezpieczeństwa wszystkich podmiotów z kategorii podmiotów publicznych, urzędów centralnych, administracji publicznej, podmiotów użyteczności publicznej i finansów publicznych. Definiując katalog typów podmiotów systemu cyberbezpieczeństwa RP należy bezwzględnie wskazać wszystkie rodzaje podmiotów publicznych - urzędy centralne, administrację publiczną wszystkich poziomów, podmioty użyteczności publicznej i finansów publicznych itp. Takie zdanie mają również

respondenci typując podmioty w kategorii: instytucje urzędów centralnych ze zdecydowanym wskazaniem w zakresie 95-110% głosów, a administracja publiczna (rządowa i samorządowa) – wszystkie jednostki, sektor finansów publicznych, sektor usług komunalnych, sektor usług publicznych z bardzo silnym wskazaniem w zakresie 80-90% głosów.

Szczególnie istotne dla bezpieczeństwa RP jest, zdaniem autora, ujednolicenie systemów infrastruktury krytycznej i sektorów cyberbezpieczeństwa oraz sektora publicznego, tzn. włączenie wszystkich sektorów określonych w systemie zarządzania kryzysowego oraz podmiotów sektora publicznego i prywatnego realizujących zadania publiczne, do systemu cyberbezpieczeństwa RP oraz włączenie do systemów infrastruktury krytycznej nieuwzględnionego tam sektora infrastruktury cyfrowej z systemu cyberbezpieczeństwa. Kwalifikacja podmiotów opiera się na konkretnie zdefiniowanych kryteriach, które muszą wykazać odpowiednio duży wpływ braku lub niewłaściwego działania usług i systemów teleinformatycznych na aspekty bezpieczeństwa państwa i porządku publicznego oraz bezpieczeństwa i funkcjonowania krytycznej działalności systemów społeczno-gospodarczych. Każdy podmiot, który po weryfikacji wg takich kryteriów zostaje uznany za kluczowy, tak w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa, jest kluczowy dla państwa. Usługi wszystkich podmiotów są obecnie zależne od systemów teleinformatycznych, więc wszystkie podmioty wytypowane wg kryteriów każdego z systemów i uznane za kluczowe powinny zostać objęte systemem cyberbezpieczeństwa RP. Zastosowanie przedstawionej wyżej sugestii autora spowoduje, że operatorzy infrastruktury krytycznej (realizującej usługi kluczowe dla bezpieczeństwa państwa i porządku publicznego), zdefiniowani w systemie zarządzania kryzysowego będą tożsami z operatorami usług kluczowych (realizującymi usługi kluczowe dla utrzymania krytycznej działalności społecznej lub gospodarczej), zdefiniowanymi w krajowym systemie cyberbezpieczeństwa. Takie podejście zapewni spójne podejście i wysoki poziom cyberbezpieczeństwa państwa.

System cyberbezpieczeństwa RP potrzebuje zbioru sektorów i typów podmiotów gwarantującego odpowiedni poziom bezpieczeństwa systemów teleinformatycznych polskiej cyberprzestrzeni i bezpieczeństwa kraju. System cyberbezpieczeństwa RP powinien obejmować najszerszy możliwy katalog systemów, sektorów i typów podmiotów, obejmujący wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkie inne typy podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego, co zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa.

5.5. Koncepcja wykazu systemów i typów podmiotów systemu cyberbezpieczeństwa RP

W ramach przeprowadzonego procesu badawczego w zakresie zbioru systemów i typów podmiotów systemu cyberbezpieczeństwa RP, stanowiącym przedmiotową problematykę niniejszego rozdziału, na podstawie wyników przeprowadzonego badania zweryfikowano pozytywnie postawioną przez autora hipotezę i sformułowano wnioski, wynikające z uzyskanych od respondentów odpowiedzi na postawione w badaniu pytania, które zostały wykorzystane w proponowanej koncepcji zbioru systemów i podmiotów systemu cyberbezpieczeństwa RP.

Koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP, po uwzględnieniu sformułowanych wniosków z badania, stanowi, że:

System cyberbezpieczeństwa RP powinien obejmować wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego, a mianowicie: energetyka, **łączność (usługi pocztowe i kurierskie), telekomunikacja i sieci teleinformatyczne**, bankowość i infrastruktura rynków finansowych, **sektor żywnościowy i rolniczy**, wodociągi i kanalizacja, ochrona zdrowia, transport, **ratownictwo, sektor chemiczny, przemysł/produkcja, handel, administracja publiczna (rządowa i samorządowa) – wszystkie jednostki, instytucje urzędów centralnych, sektor finansów publicznych, sektor usług komunalnych, sektor usług publicznych, sektor kosmiczny, nauka i szkolnictwo wyższe, instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe), media (TV, radio, portale informacyjne)**, infrastruktura cyfrowa (DNS, IXP, TLD), usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej), **usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.),** środki **tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach, dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja), dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa, wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego lub usług kluczowych oraz uczestniczące w łańcuchu dostaw dla nich.**

Sektory, systemy i typów podmiotów cyberbezpieczeństwa dotychczas nie objęte krajowym systemem cyberbezpieczeństwa zostały zaznaczone przez pogrubienie.

Opracowana koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP stanowi nowum pracy, wypełnia zdiagnozowaną lukę, brak i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwego wykazu sektorów i typów podmiotów. W ramach koncepcji zaproponowano znaczne rozszerzenie sektorów i typów podmiotów w stosunku do aktualnie zdefiniowanego. Wg koncepcji system cyberbezpieczeństwa RP powinien obejmować wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego. Implementacja tak sformułowanej koncepcji objęłaby systemem cyberbezpieczeństwa wielokrotnie więcej podmiotów, a przez to przyczyniłaby się do zwiększenia poziomu cyberbezpieczeństwa i bezpieczeństwa państwa.

Szczegółowe zestawienie porównawcze sektorów, systemów i typów podmiotów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa, systemu informatyzacji podmiotów publicznych i koncepcji systemu cyberbezpieczeństwa RP zostało przedstawione w tabeli 44.

Sektory, systemy i typy podmiotów cyberbezpieczeństwa dotychczas nie objętych krajowym systemem cyberbezpieczeństwa zostały zaznaczone przez pogrubienie.

Tabela 44. Systemy i sektory podmiotów systemów zarządzania kryzysowego, cyberbezpieczeństwa, informatyzacji podmiotów publicznych i koncepcji systemu cyberbezpieczeństwa RP – ujęcie porównawcze

Systemy i sektory podmiotów systemów zarządzania kryzysowego, cyberbezpieczeństwa, informatyzacji podmiotów publicznych i koncepcji systemu cyberbezpieczeństwa RP			
Rozwiązania aktualne			**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**System informatyzacji podmiotów publicznych (SIPP)**	**System cyberbezpieceństwa RP (SCRP) - Koncepcja**
Zaopatrzenie w energię, surowce energetyczne i paliwa	Energia		Energetyka

Łączność			Łączność (usługi pocztowe i kurierskie)
Sieci teleinformatyczne			Telekomunikacja i sieci teleinformatyczne
Finanse	Bankowość i infrastruktury rynków finansowych		Bankowość i infrastruktura rynków finansowych
Zaopatrzenie w żywność			Sektor żywnościowy i rolniczy
Zaopatrzenie w wodę	Zaopatrzenie w wodę		Wodociągi i kanalizacja
Ochrona zdrowia	Ochrona zdrowia		Ochrona zdrowia
Transport	Transport		Transport
Ratownictwo			Ratownictwo
Zapewniający ciągłość działania administracji publicznej	Podmioty publiczne i urzędy centralne Podmioty realizujące zadania publiczne	Podmioty publiczne i urzędy centralne Podmioty realizujące zadania publiczne	Sektor chemiczny
Produkcja, składowanie, przechowywanie i stosowanie substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych			Przemysł / Produkcja
			Handel
			Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki
			Instytucje urzędów centralnych - wszystkie jednostki
			Sektor finansów publicznych
			Sektor usług komunalnych
			Sektor usług publicznych
			Sektor kosmiczny
			Nauka i szkolnictwo wyższe

			Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)
			Media (TV, radio, portale informacyjne)
	Infrastruktura cyfrowa		Infrastruktura cyfrowa (DNS, IXP, TLD)
	Usługi cyfrowe		Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej)
			Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)
			Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach
			Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja)
	Usługi cyberbezpieczeństwa		Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa
			Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego lub usług kluczowych oraz uczestniczące w łańcuchu dostaw dla nich

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565, wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Systemy, sektory i typy podmiotów wskazane w ramach opracowanej koncepcji systemu cyberbezpieczeństwa RP zawierają najszerszy możliwy ich katalog, obejmujący wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania

publiczne oraz wszystkie inne typy podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego, co zapewni efektywność systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa RP.

5.6. Podsumowanie i wnioski

W rozdziale piątym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa RP, sformułowanego jako pytanie badawcze: *jakie sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP i jakie powinny zostać nim objęte, aby zapewnić jego efektywność i odpowiedni poziom bezpieczeństwa kraju?* Rozstrzygnięcie problemu zostało przeprowadzone poprzez weryfikację w procesie badawczym przyjętej hipotezy pomocniczej stwierdzającej, że: *objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa*.

W celu weryfikacji hipotezy przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu systemów, sektorów i typów podmiotów w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych. Przedstawiono i omówiono zagadnienia doboru sektorów i typów podmiotów objętych systemem cyberbezpieczeństwa państwa w ujęciu regulacji prawnych trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych. Dokonano analizy porównawczej wykazu podmiotów objętych ww. regulacjami w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego obejmuje podmioty zdefiniowane jako operatorzy infrastruktury krytycznej wskazywane w ramach zdefiniowanych 11 systemów, krajowy system cyberbezpieczeństwa obejmuje podmioty zdefiniowane jako operatorzy usług kluczowych, dostawcy usług cyfrowych, wybrane typy podmiotów publicznych i podmioty świadczące usługi w zakresie cyberbezpieczeństwa wskazywane w ramach zdefiniowanych 9 sektorów, natomiast system informatyzacji podmiotów publicznych obejmuje wybrane typy podmiotów publicznych z sektora publicznego. Typy podmiotów włączone do podsystemów bezpieczeństwa

w ramach systemów i sektorów tylko częściowo się pokrywają, są niespójne, nie są ze sobą powiązane i zintegrowane. Jedynie podmioty sektora publicznego objęte są każdym z systemów, ale w innym zakresie, tak, że tylko częściowo się pokrywają. Przedstawiono w ujęciu porównawczym, w formie tabelarycznej i opisowej zestawienie podmiotów oraz zestawienie systemów i sektorów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów publicznych.

Przeprowadzono badania własne autora w zakresie doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i dokonano ich analizy. Wyniki badania wykazały, że sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP nie są właściwie zdefiniowane. Uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań i uzyskanych opinii od respondentów sformułowana została koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP wskazująca zakres sektorów i typów podmiotów koniecznych do objęcia tym systemem. Koncepcja adresuje wyniki i wnioski z badania, i jest oparta na hipotezie badawczej. Opracowano tabelaryczne zestawienie porównawcze dotychczasowych sektorów i systemów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa, systemu informatyzacji podmiotów publicznych z koncepcyjnym wykazem sektorów i typów podmiotów systemu cyberbezpieczeństwa RP.

W wyniku przeprowadzonego procesu badawczego sformułowana hipoteza pomocnicza została pozytywnie zweryfikowana. Na podstawie przyjętej hipotezy, wyników badań, sformułowanych konkluzji i wniosków opracowano koncepcję wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP.

W ramach realizacji celu głównego rozprawy, którym jest: *opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa*, w ramach niniejszego rozdziału został zrealizowany cel szczegółowy rozprawy, którym jest: *opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP.*

Na podstawie przyjętej hipotezy, wyników badań, sformułowanych konkluzji i wniosków opracowano koncepcję wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP. Przyjęty cel szczegółowy został osiągnięty, przez co przyczynił się do osiągnięcia celu głównego rozprawy.

Rozdział VI. BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH PODMIOTÓW SYSTEMU CYBERBEZPIECZEŃSTWA RP

Podmioty systemu cyberbezpieczeństwa realizują zadania w zakresie zapewnienia bezpieczeństwa usług publicznych i społecznych oraz infrastruktury tych usług poprzez zapewnienie bezpieczeństwa infrastruktury systemów teleinformatycznych oraz reagowanie i zarządzanie incydentami cyberbezpieczeństwa i sytuacjami kryzysowymi wynikającymi z materializacji cyberzagrożeń. W zakresie problematyki bezpieczeństwa teleinformatycznego, bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych jest dostępnych wiele rozwiązań technicznych i organizacyjnych. Rozwiązania te obejmują szeroki zakres zagadnień bezpieczeństwa teleinformatycznego, m.in. zabezpieczania i ochrony informacji i przetwarzających je systemów teleinformatycznych, zapewnienia poufności, dostępności, integralności i rozliczalności informacji w systemach teleinformatycznych, a także metody i rozwiązania techniczne i technologiczne bezpieczeństwa teleinformatycznego, zasady budowy architektury bezpiecznych systemów oraz procesy bezpośrednio z nimi związane. Pula takich rozwiązań jest domeną tzw. dobrej praktyki inżynierskiej i kompetencji poszczególnych zespołów odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych. Dla zapewnienia kompletnego i kompleksowego podejścia do zarządzania i zapewniania bezpieczeństwa informacji i systemów teleinformatycznych powstało wiele branżowych standardów i metodyk oraz norm międzynarodowych. Regulacje systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych zawierają wymagania dla wdrożenia rozwiązań organizacyjnych i technicznych bezpieczeństwa teleinformatycznego podmiotów i systemów teleinformatycznych oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa w oparciu o wskazane normy, metodyki i standardy. Wytyczne ww. regulacji w tym zakresie są niespójne, nie są ze sobą powiązane i zintegrowane, w dużej części się nie pokrywają, przez co nie adresują

pełnego, powtarzalnego i referencyjnego dla wszystkich podmiotów zakresu zagadnień bezpieczeństwa teleinformatycznego, dzięki zastosowaniu których podmioty operujące w cyberprzestrzeni mogłyby zaprojektować i zbudować w sposób spójny i kompleksowy architekturę bezpiecznych systemów i system bezpieczeństwa stosowanych rozwiązań teleinformatycznych, a przez to przyczynić się do zapewnienia odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni. Taki stan skutkuje tym, że nie może być zapewniony odpowiedni poziom cyberbezpieczeństwa kraju na najniższym, operacyjnym poziomie usług publicznych i społecznych oraz infrastruktury, w tym teleinformatycznej, tych usług. System cyberbezpieczeństwa powinien zapewniać funkcjonalny, spójny, kompleksowy i całościowy model w praktycznym i aplikowalnym ujęciu metodycznym i strukturalnym, wskazując niezbędne w takim systemie normy, metodyki i standardy rozwiązań organizacyjnych i technicznych bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa. Zdaniem autora *ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

Celem niniejszego rozdziału, w kontekście celu rozprawy, jest realizacja jej celu szczegółowego *opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP*. W niniejszym rozdziale dokonano próby rozstrzygnięcia problemu badawczego dotyczącego rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP poprzez weryfikację przyjętej hipotezy pomocniczej. W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych oraz dokonano ich analizy porównawczej. Przedstawiono również wyniki przeprowadzonych badań własnych autora w tym zakresie, prezentujące stanowiska respondentów nt. efektywności dotychczasowych oraz rozważanych w badaniu nowych rozwiązań, adresujących przyjęte założenia ujednolicenia i zharmonizowania wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych dla zapewnienia podobnego i porównywalnego w skali kraju poziomu

odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa oraz dokonano ich analizy. Została opracowana i przedstawiona autorska koncepcja wykazu norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, adresująca wyniki badania.

Kwestia bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i doboru właściwych norm, standardów czy metodyk zarządzania bezpieczeństwem systemów teleinformatycznych, przedstawiona jest w niniejszym rozdziale rozprawy z perspektywy trzech funkcjonujących w Polsce systemów bezpieczeństwa, adresujących kwestie cyberbezpieczeństwa, w ujęciu wybranych aspektów właściwych dla problematyki niniejszego rozdziału, zdefiniowanych przez dokumenty strategiczne i stosowne regulacje prawne dotyczące zarządzania kryzysowego – tworzące system zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa – tworzące krajowy system cyberbezpieczeństwa i dotyczące informatyzacji podmiotów realizujących zadania publiczne – tworzące system informatyzacji podmiotów publicznych.

6.1. Bezpieczeństwo systemów teleinformatycznych

Rozwiązania normatywne bezpieczeństwa teleinformatycznego podmiotów i systemów teleinformatycznych systemu cyberbezpieczeństwa Polski zostaną rozpatrzone w ujęciu trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych. Charakterystyka systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych została przedstawiona w rozdziale 2.6 pracy. Normy, metodyki i standardy zarządzania bezpieczeństwem informacji, bezpieczeństwem teleinformatycznym i cyberbezpieczeństwem oraz rozwiązań organizacyjnych i technicznych bezpieczeństwa teleinformatycznego systemów i podmiotów systemu cyberbezpieczeństwa zostały przedstawione w rozdziale 2.7 pracy. W niniejszym rozdziale zostaną zaprezentowane szczegółowe rozwiązania systemowe tych regulacji w zakresie doboru norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

System zarządzania kryzysowego jest rozpatrywany z perspektywy zagadnienia bezpieczeństwa teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych wspierających funkcjonowanie usług infrastruktury krytycznej, czyli cyberbezpieczeństwa

tej infrastruktury i jej usług. Zarządzanie kryzysowe i planowanie cywilne w tym zakresie są rozumiane i rozpatrywane jako zarządzanie cyberbezpieczeństwem.

6.1.1. Bezpieczeństwo teleinformatyczne w systemie zarządzania kryzysowego

Ustawa o zarządzaniu kryzysowym[341] (Ustawa ZK) wraz z Rozporządzeniem w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[342] oraz Narodowy Program Ochrony Infrastruktury Krytycznej[343] (NPOIK) wraz z Załącznikiem 1 do NPOIK – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje[344] stanowią dokumenty formalne ustanawiające i definiujące wymagania i warunki bezpieczeństwa infrastruktury krytycznej. Celem NPOIK jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w tym teleinformatycznej infrastruktury krytycznej i systemów teleinformatycznych wspierających funkcjonowanie usług infrastruktury krytycznej, i przez to podniesienie bezpieczeństwa Rzeczypospolitej Polskiej[345]. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) obejmuje infrastrukturę krytyczną (IK) umieszczoną w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy[346].

Ochronę infrastruktury krytycznej należy pojmować jako proces zapewnienia jej bezpieczeństwa. Wszelkie działania podejmowane w celu zapewnienia ochrony infrastruktury krytycznej, w tym teleinformatycznej infrastruktury krytycznej cyberprzestrzeni, powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to zarówno przyjętego modelu ochrony infrastruktury krytycznej, jej rodzajów, a także użytych sił i środków. Z punktu widzenia NPOIK jest to element kluczowy, determinujący i uzasadniający działania podejmowane w celu obniżenia ryzyka zakłócenia funkcjonowania infrastruktury krytycznej do poziomu akceptowalnego. Ocena ryzyka powinna być podstawą określenia standardów ochrony infrastruktury krytycznej cyberprzestrzeni i ustalenia priorytetów działań. Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno

[341] Ustawa o zarządzaniu kryzysowym, wyd. cyt.
[342] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. 2010 Nr 83 poz. 541
[343] Opracowany w 2015 r. i aktualizowany co ok. 2 lata przez Rządowe Centrum Bezpieczeństwa. Uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej z uwzględnieniem Uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej
[344] Opracowany i aktualizowany wraz z Narodowym Programem Ochrony Infrastruktury Krytycznej
[345] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 5b
[346] NPOIK, wyd. cyt., pkt. 2.1, s. 8

być ściśle związane z oceną ryzyka zakłócenia funkcjonowania infrastruktury krytycznej[347], w tym infrastruktury krytycznej cyberprzestrzeni.

Ustawa ZK nakłada na właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej (operatorów infrastruktury krytycznej, OIK) obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia[348]. Wg rozporządzenia w sprawie planów ochrony infrastruktury krytycznej[349] elementami planu są:

1) dane ogólne charakteryzujące operatora infrastruktury krytycznej;
2) dane infrastruktury krytycznej obejmujące charakterystykę i podstawowe parametry techniczne, plan (mapę) z naniesieniem lokalizacji obiektów, instalacji lub systemu, funkcjonalne połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami, charakterystyka zagrożeń dla infrastruktury krytycznej oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń, zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej, zasobów własnych możliwych do wykorzystania w celu ochrony infrastruktury krytycznej, zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej;
3) zasadnicze warianty działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienia ciągłości funkcjonowania infrastruktury krytycznej, odtwarzania infrastruktury krytycznej;
4) zasady współpracy z właściwymi miejscowo centrami zarządzania kryzysowego i organami administracji publicznej.

Operatorzy infrastruktury krytycznej, będący jednocześnie operatorami usług kluczowych, w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, uwzględniają w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, zgodnie

[347] tamże, s. 28, 31
[348] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 6, pkt. 5
[349] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. Nr 83 poz. 542

z zakresem informacji określonym w przepisach związanych z ustawą o krajowym systemie cyberbezpieczeństwa[350].

Działania podejmowane przez operatorów infrastruktury krytycznej na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez zmniejszenie prawdopodobieństwa wystąpienia zagrożenia, zmniejszanie podatności lub minimalizowanie skutków wystąpienia zagrożenia. Na działania na rzecz zapewnienia bezpieczeństwa IK składają się[351]:

1) zapewnienie bezpieczeństwa fizycznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – jest to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

W kręgu zainteresowania rozprawy, a w szczególności niniejszego jej rozdziału, są zagadnienia zapewnienia bezpieczeństwa teleinformatycznego infrastruktury krytycznej.

Przywołany NPOIK Załącznik 1 - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej dobre praktyki i rekomendacje, definiuje zapewnienie

[350] Ustawa o zarządzaniu kryzysowym, wyd. cyt., art. 5b
[351] NPOIK, wyd. cyt., s. 30

bezpieczeństwa teleinformatycznego jako zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne, włączając w to akty szeroko rozumianej cyberprzestępczości i cyberterroryzmu a także przypadkowych (niecelowych) działań użytkowników[352]. Dokument wskazuje, że najistotniejszymi elementami zapewnienie bezpieczeństwa teleinformatycznego IK są[353]:

1) współpraca sektorowa,
2) plany awaryjne i ciągłości działania,
3) bezpieczeństwo oprogramowania,
4) kontrola dostępu,
5) ochrona stacji roboczych,
6) bezpieczeństwo sieci bezprzewodowych,
7) monitoring zagrożeń,
8) reakcja na incydenty.

Dokument wskazuje normy i standardy bezpieczeństwa teleinformatycznego możliwe do zastosowania przez operatorów infrastruktury krytycznej do ochrony systemów teleinformatycznych stanowiących i wspierających ich IK, takie jak[354]: ISO/IEC 27002, IEC62443/ISA62443, NIST 800-82, NERC-CIP, TIA 942, ISO/IEC24762 oraz standardy bezpieczeństwa opracowywane przez ENISA[355]. Charakterystyka wskazanych norm i standardów bezpieczeństwa teleinformatycznego jest następująca:

- PN-EN ISO 27002 – Technika informatyczna - Techniki bezpieczeństwa - Zasady zabezpieczenia informacji. Norma definiująca i opisująca najlepsze praktyki i zasady w zakresie rozwiązań organizacyjnych i technicznych bezpieczeństwa, tzw. Zabezpieczeń;
- IEC 62443 / ISA 62433 – zbiór standardów zawierających rekomendacje co do zakresu i realizacji programów poprawy bezpieczeństwa w przedsiębiorstwach będących operatorami przemysłowych systemów sterowania, wskaźników dla oceny stanu bezpieczeństwa w organizacji, definicji pojęć z zakresu bezpieczeństwa;

[352] NPOIK Załącznik 1, wyd. cyt., s. 67
[353] tamże, s. 67, 76
[354] tamże, s. 74-75
[355] ENISA (ang. – European Agency for Network and Information Security) Europejska Agencja Bezpieczeństwa Sieci i Informacji, zajmująca się kwestiami bezpieczeństwa teleinformatycznego

- NIST 800-82 – zawiera wiele rekomendacji z zakresu bezpieczeństwa teleinformatycznego systemów automatyki, w tym w szczególności w obszarze architektury sieci i separacji sieci IK od pozostałych sieci przedsiębiorstwa;
- NERC CIP – amerykański standard poświęcony bezpieczeństwu teleinformatycznemu infrastruktury krytycznej w segmencie energetyki;
- API-1164 Pipeline SCADA Security – zbiór zasad dla bezpieczeństwa systemów ICS opracowany przez American Petroleum Institute specjalnie dla sektora rafineryjnego. Wytyczne w nim zawarte mogą być z powodzeniem zastosowane w systemach przemysłowych innych sektorów;
- TIA-942 – amerykański standard opisujący minimalne wymagania dla infrastruktury telekomunikacyjnej i centrów przetwarzania;
- ISO/IEC 24762[356] – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie;
- Protecting Industrial Control Systems – Recommendations for Europe and Member States (ENISA), dokument, który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz 7 głównych kroków jak podnieść poziom bezpieczeństwa w takim środowisku.

Regulacje wynikające z ustawy o zarządzaniu kryzysowym - Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje – wymagają wdrożenia rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo systemów teleinformatycznych stanowiących teleinformatyczną infrastrukturę krytyczną i systemów wspierających usługi kluczowe infrastruktury krytycznej, jednakże wskazują normy międzynarodowe i krajowe tylko jako zalecenie czy sugestię. Oznacza to, że operatorzy infrastruktury krytycznej mogę wdrożyć również dowolne inne normy, standardy czy metodyki definiujące bezpieczeństwo wykorzystywanych systemów teleinformatycznych.

[356] Norma została wycofana w 2014 r., źródło: iso.org [dostęp 10.03.2020]

6.1.2. Bezpieczeństwo teleinformatyczne w krajowym systemie cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa KSC) wraz z towarzyszącymi rozporządzeniami zobowiązują operatorów usług kluczowych, dostawców usług cyfrowych i podmioty świadczące usługi w zakresie cyberbezpieczeństwa do wdrożenia systemu zarządzania bezpieczeństwem w oparciu wskazane międzynarodowe i krajowe normy ISO. Należy zwrócić uwagę, że tylko wybrane typy podmiotów objętych ustawą muszą zrealizować ten obowiązek. Nie dotyczy on podmiotów publicznych i urzędów centralnych wymienionych w Ustawie KSC, co jest rzeczą niezrozumiałą ze względu na to, że podmioty takie są częścią systemu administracji państwa, a ich bezpieczeństwo, a przez to również bezpieczeństwo ich systemów teleinformatycznych jest uwarunkowaniem cyberbezpieczeństwa państwa. Podmioty publiczne objęte regulacjami ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, które stanowią odrębną, nie pokrywającą się grupę względem podmiotów publicznych krajowego systemu cyberbezpieczeństwa, zostały zobligowane do wdrożenia rozwiązań bezpieczeństwa systemów teleinformatycznych w oparciu o wskazaną grupę norm ISO, co zostało omówione w dedykowanych podrozdziale.

Ustawa KSC nakłada na operatorów usług kluczowych obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. System zarządzania ma zapewnić[357]:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: utrzymanie i bezpieczną eksploatację systemu informacyjnego, bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

[357] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 8

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Operatorzy usług kluczowych mają obowiązek opracować, stosować i aktualizować dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[358]. Zgodnie z rozporządzeniem w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[359] do tej dokumentacji zalicza się:

1) dokumentację normatywną, którą stanowi:
   a. dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami normy PN-EN ISO/IEC 27001[360],
   b. dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa,
   c. dokumentacja systemu zarządzania ciągłością działania usługi kluczowej wytworzona zgodnie z wymaganiami normy PN-EN ISO 22301[361],
   d. dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
   e. dokumentacja wynikająca ze specyfiki świadczonej usługi kluczowej w danym sektorze lub podsektorze,
2) dokumentację operacyjną (dokumentację dotyczącą procedur oraz instrukcji wynikających z dokumentacji normatywnej, opisy sposobów dokumentowania wykonania czynności w ramach ustalonych procedur, dokumentację poświadczającą każdorazowe wykonanie procedury).

[358] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 10
[359] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz. U. poz. 2080
[360] PN-EN ISO/IEC 27001 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji
[361] PN-EN ISO 22301 – Bezpieczeństwo publiczne - System zarządzania ciągłością działania

Operatorzy usług kluczowych, będący jednocześnie operatorami infrastruktury krytycznej, którzy posiadają zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie mają obowiązku opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych[362].

Struktury cyberbezpieczeństwa operatorów usług kluczowych oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa operatorom usług kluczowych, w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji, zobowiązani są[363]:

1) posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001;
2) zapewnić ciągłość działania usłudze reagowania na incydenty, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów informacyjnych zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
3) zapewnić wsparcie operatorowi usługi kluczowej w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej;
4) dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:
   a) identyfikowania zagrożeń w odniesieniu do systemów informacyjnych,
   b) analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,
   c) zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

Ustawa KSC nakłada na dostawców usług cyfrowych zobowiązanie do podjęcia właściwych i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej oraz do podejmowania środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi. Środki te mają zapewniać cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniać[364]:

[362] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 10
[363] Rozporządzenie ministra cyfryzacji z dnia 10 września 2018 r, w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. 2018 poz. 1780, art. 1
[364] Ustawa o krajowym systemie cyberbezpieczeństwa, wyd. cyt., art. 17

1) bezpieczeństwo systemów informacyjnych i obiektów,
2) postępowanie w przypadku obsługi incydentu,
3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej,
4) monitorowanie, audyt i testowanie,
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi.

Ustawa KSC nie wskazuje dostawcom usług cyfrowych konkretnych norm, standardów czy metodyk do zastosowania, co oznacza, że mogą oni zastosować normę obejmującą swoim zakresem wszystkie wskazane aspekty bezpieczeństwa lub też zbiór norm, które pokrywają ten zakres wymaganych aspektów bezpieczeństwa systemów teleinformatycznych, np. zbiór norm z rodziny ISO 270xx, adresujący kwestie bezpieczeństwa informacji i systemów teleinformatycznych.

Ustawa KSC wskazuje jako podmioty krajowego systemu cyberbezpieczeństwa, podmioty publiczne – administrację publiczną i urzędy centralne, jednakże nie zobowiązuje tych podmiotów do wdrożenia systemu zarządzania bezpieczeństwem systemów teleinformatycznych, stosowanych do realizacji zadań publicznych. Ustawa KSC nakłada na podmioty publiczne nią objęte tylko obowiązki wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i obsługi incydentów, zgodnie ze zdefiniowanymi warunkami.

6.1.3. Bezpieczeństwo teleinformatyczne w systemie informatyzacji podmiotów realizujących zadania publiczne

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[365] (Ustawa IPP) wraz z Rozporządzeniem w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[366] (Rozporządzenie KRI) stanowią dokumenty formalne, ustanawiające i definiujące wymagania i warunki bezpieczeństwa dla systemów teleinformatycznych podmiotów realizujących zadania publiczne. Ustawa IPP nie jest dokumentem bezpośrednio adresującym kwestie bezpieczeń-

[365] Ustawa o informatyzacji, wyd. cyt.
[366] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526 z późn. zmianami (Dz.U. 2017 poz. 2247) (Rozporządzenie KRI)

stwa państwa czy bezpieczeństwa teleinformatycznego, odnosi się jednak do kwestii informatyzacji podmiotów publicznych i definiuje wymagania bezpieczeństwa ich systemów teleinformatycznych

Ustawa IPP definiuje system teleinformatyczny jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Ustawa IPP określa zasady m.in. ustalania minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i dla rejestrów publicznych oraz ustalania Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji oraz dostosowania systemów teleinformatycznych używanych do realizacji zadań publicznych i rejestrów publicznych do tych wymagań w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji w celu ochrony interesu publicznego, w tym zachowania przez państwo możliwości swobody wyboru technologii w procesach informatyzacji realizacji zadań publicznych. Podmiot publiczny zobowiązany jest do używania do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności[367]. Przywołane Rozporządzenie KRI określa m.in: Krajowe Ramy Interoperacyjności oraz minimalne wymagania dla systemów teleinformatycznych, w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji. Krajowe Ramy Interoperacyjności określają sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych oraz sposoby postępowania podmiotu realizującego zadania publiczne w zakresie przejrzystego wyboru norm, standardów i rekomendacji w zakresie interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z zapewnieniem zasady neutralności technologicznej[368].

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności na poziomie organizacyjnym, semantycznym i technologicz-

[367] Ustawa o informatyzacji, wyd. cyt., art. 1, 3, 13
[368] Rozporządzenie RKRI, wyd. cyt., art. 1, 3

nym. Interoperacyjność na poziomie technologicznym osiągana jest przez stosowanie zdefiniowanych w Rozporządzeniu minimalnych wymagań dla systemów teleinformatycznych i stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku uwzględnienia postanowień odpowiednich Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe[369].

Podmioty realizujące zadania publiczne zobowiązane są do projektowania, wdrażania oraz eksploatacji systemów teleinformatycznych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w standardów i metodyk branżowych. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne powinno odbywać się w oparciu o udokumentowane procedury w celu dostarczania tych usług na deklarowanym poziomie dostępności. Tak zdefiniowane wymagania mogą być uznane za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2[370].

Podmiot realizujący zadania publiczne zobowiązany jest do opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie warunków umożliwiających realizację i egzekwowanie następujących działań[371]:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie

[369] tamże, art. 5
[370] tamże, art. 15
[371] tamże, art. 20

w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Zdefiniowane wymagania wobec systemu zarządzania bezpieczeństwem informacji mogą zostać uznane za spełnione, jeżeli został on opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym[372]:

1) PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń,
2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem,
3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Niezależnie od wdrożenia zabezpieczeń na podstawie ww. norm, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia[373]. Jest to standardowe podejście stosowane w systemach zarządzania bezpieczeństwem, opartych na normach ISO.

Ustawa IPP i Rozporządzenie KRI wskazują wprost wymagania wdrożenia systemu zarządzania usługami informatycznymi, realizowanymi przez systemy teleinformatyczne, i systemu zarządzania bezpieczeństwem informacji, odnoszącego się do bezpieczeństwa przetwarzanych informacji i bezpieczeństwa systemu teleinformatycznego, wskazując wprost dedykowane międzynarodowe i krajowe normy ISO.

[372] tamże, art. 20
[373] Rozporządzenie RKRI, wyd. cyt., art. 20

6.2. Analiza porównawcza rozwiązań bezpieczeństwa systemów teleinformatycznych

Kwestie bezpieczeństwa krajowych systemów teleinformatycznych, z racji swojego znaczenia dla bezpieczeństwa państwa, są przedmiotem zainteresowania i wpływu regulacji prawnych, w tym w szczególności ustawy o zarządzaniu kryzysowym, ustawy o krajowym systemie cyberbezpieczeństwa i ustawy o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącymi im aktami wykonawczymi i pomocniczymi (rozporządzeniami i dokumentami powstałymi na ich mocy). Regulacje systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych zawierają wymagania dla rozwiązań bezpieczeństwa teleinformatycznego podmiotów i systemów teleinformatycznych. W/w regulacje prawne definiują m.in. wymagania wobec podmiotów nimi objętych dotyczące wdrożenia odpowiednich normatywnych rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa.

Regulacje wynikające z ustawy o zarządzaniu kryzysowym - Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje – wymagają wdrożenia rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo systemów teleinformatycznych stanowiących teleinformatyczną infrastrukturę krytyczną i systemów wspierających usługi kluczowe infrastruktury krytycznej, jednakże wskazują normy międzynarodowe i krajowe tylko jako zalecenie czy sugestię. W związku z regulacjami systemu zarządzania kryzysowego operatory infrastruktury krytycznej, w ramach zapewnienia bezpieczeństwa teleinformatycznego, mogą wdrożyć system zarządzania bezpieczeństwem z dobrowolnym wykorzystaniem następujących norm, wskazanych w NPOIK:

- PN-EN ISO 27002 – zbiór dobrych praktyk i zasad zapewnienia bezpieczeństwa informacji,
- IEC 62443 / ISA 62433 – zbiór standardów zawierających rekomendacje co do zakresu i realizacji programów poprawy bezpieczeństwa w przedsiębiorstwach będących operatorami przemysłowych systemów sterowania, wskaźników dla oceny stanu bezpieczeństwa w organizacji, definicji pojęć z zakresu bezpieczeństwa,

- NIST 800-82 – zawiera wiele rekomendacji z zakresu bezpieczeństwa teleinformatycznego systemów automatyki, w tym w szczególności w obszarze architektury sieci i separacji sieci IK od pozostałych sieci przedsiębiorstwa,
- NERC CIP – amerykański standard poświęcony bezpieczeństwu teleinformatycznemu infrastruktury krytycznej w segmencie energetyki,
- API-1164 Pipeline SCADA Security – zbiór zasad dla bezpieczeństwa systemów ICS opracowany przez American Petroleum Institute specjalnie dla sektora rafineryjnego. Wytyczne w nim zawarte mogą być z powodzeniem zastosowane w systemach przemysłowych innych sektorów,
- TIA-942 – amerykański standard opisujący minimalne wymagania dla infrastruktury telekomunikacyjnej i centrów przetwarzania,
- ISO/IEC 24762 – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie,
- Protecting Industrial Control Systems – Recommendations for Europe and Member States (ENISA), dokument, który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz 7 głównych kroków jak podnieść poziom bezpieczeństwa w takim środowisku.

Ustawa o krajowym systemie cyberbezpieczeństwa wraz z towarzyszącymi rozporządzeniami zobowiązują operatorów usług kluczowych oraz ich wewnętrzne struktury cyberbezpieczeństwa i podmioty świadczące usługi w zakresie cyberbezpieczeństwa do wdrożenia systemu zarządzania bezpieczeństwem w oparciu wskazane międzynarodowe i krajowe normy ISO. Rozporządzenia do Ustawy KSC wskazują wprost normy ISO konieczne do wdrożenia w zakresie systemu zarządzania bezpieczeństwem informacji ich systemów teleinformatycznych. Operatorzy muszą wdrożyć ISO/IEC 27001 w zakresie systemu zarządzania bezpieczeństwem informacji systemu teleinformatycznego oraz ISO 22301 w zakresie zarządzania ciągłością działania usługi kluczowej, wewnętrzne struktury cyberbezpieczeństwa operatorów i podmioty świadczące usługi w zakresie cyberbezpieczeństwa musza wdrożyć ISO/IEC 27001 w zakresie systemu zarządzania bezpieczeństwem informacji systemu teleinformatycznego oraz ISO 22301 w zakresie zarządzania ciągłością działania usługi reagowania na incydenty, czyli ich usługi podstawowej, do której realizacji zostały powołane. Należy zwrócić uwagę, że tylko wybrane typy podmiotów objętych ustawą muszą

zrealizować ten obowiązek. Dostawcy usług cyfrowych są zobowiązani do wdrożenia rozwiązań bezpieczeństwa usług i systemów teleinformatycznych, ale bez konieczności stosowania norm ISO, natomiast urzędy centralne, podmioty publiczne i realizujące zadania publiczne nie mają w ogóle wymagania wdrożenia systemu zarządzania bezpieczeństwem informacji i systemów teleinformatycznych.

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych wskazuje wprost wymagania wdrożenia systemu zarządzania usługami informatycznymi realizowanymi przez systemy teleinformatyczne i systemu zarządzania bezpieczeństwem informacji dla systemów teleinformatycznych, wskazując wprost dedykowane międzynarodowe i krajowe normy ISO. Jest to sytuacja zgoła odmienna od wymagań zdefiniowanych dla podmiotów publicznych w krajowym systemie cyberbezpieczeństwa, dla których nie ma żadnych wymagań w tym zakresie. Należy zwrócić uwagę, że regulacjami tymi objęte są różne grupy podmiotów publicznych, nie pokrywających się, co oznacza, że część z nich musi wdrożyć rozwiązania bezpieczeństwa systemów teleinformatycznych, a inna nie musi ich zabezpieczać. Jest to sytuacja niezrozumiała i generująca luki w cyberbezpieczeństwie państwa. Do realizacji wymaganych przez przepisy Ustawy IPP systemów zarządzania usługami informatycznymi i systemów zarządzania bezpieczeństwem systemów teleinformatycznych podmioty powinny zastosować najnowsze normy międzynarodowe w tym zakresie, w szczególności europejskie i krajowe normy ISO. W związku z wymaganiami regulacji systemu informatyzacji podmiotów publicznych podmioty te powinny wdrożyć systemy zarządzania usługami informatycznymi i systemu zarządzania bezpieczeństwem informacji z zastosowaniem norm ISO wskazanych w Rozporządzeniu KRI, a mianowicie:

- PN-EN ISO/IEC 27001 - system zarządzania bezpieczeństwem informacji,
- PN-EN ISO/IEC 27002 – zbiór dobrych praktyk i zasad zapewnienia bezpieczeństwa informacji,
- ISO/IEC 27005 – zarządzanie ryzykiem w bezpieczeństwie informacji,
- ISO/IEC 24762 – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie,
- ISO 20000-1 – system zarządzania usługami IT,

– ISO 20000-2 – wytyczne wdrażania systemu zarządzania usługami IT.

Szczegółowe zestawienie norm i standardów bezpieczeństwa systemów teleinformatycznych zalecanych lub wymaganych do wdrożenia przez podmioty objęte regulacjami systemów bezpieczeństwa – zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych zostały przedstawione w tabeli 45.

Tabela 45. Normy ISO i standardy zarządzania bezpieczeństwem systemów teleinformatycznych systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych – ujęcie porównawcze

Normy zarządzania bezpieczeństwem systemów teleinformatycznych		
Zarządzanie kryzysowe	**Krajowy system cyberbezpieczeństwa**	**Informatyzacja podmiotów publicznych**
ISO 27002	ISO 27001	ISO 27001
IEC 62443 / ISA 62433	ISO 22301	ISO 27002
NIST 800-82		ISO 27005
NERC CIP		ISO 24762
API-1164 Pipeline SCADA Security		ISO 20000-1, 20000-2
TIA-942		
ISO 24762[374]		
Protecting Industrial Control Systems		

Źródło: Opracowanie własne na podstawie: 1. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 poz. 590; Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) Załącznik 1 - Standardy służących zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje; 2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Rozporządzenie w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych; 3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565, Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Na uwagę zasługuje fakt, że, w ramach regulacji zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje, choć wskazują normy

[374] Norma została wycofana w 2014 r., źródło: iso.org [dostęp 10.03.2020]

międzynarodowe i krajowe jako podstawę wdrożenia systemu zarządzania bezpieczeństwem, tylko jako zalecenie czy sugestię, to jest to lista najobszerniejsza i otwarta na nowe pozycje standardów. Należy zwrócić uwagę, że wskazane standardy są alternatywne względem siebie. Takie podejście z jednej strony jest dobre, ponieważ daje podmiotom możliwość rozwoju swoich rozwiązań implementowania nowych standardów, z drugiej strony brak obowiązkowego stosowania konkretnych norm powoduje brak ustandaryzowanego podejścia podmiotów do zarządzania bezpieczeństwem.

Regulacje krajowego systemu cyberbezpieczeństwa, choć wymagają od wskazanych podmiotów wdrożenia systemu zarządzania bezpieczeństwem opartego na normach międzynarodowych i krajowych, to spośród szerokiej palety takich rozwiązań, jako wymagane wskazano tylko dwie normy. Regulacje krajowego systemu cyberbezpieczeństwa zostały ustanowione jako te, które mają porządkować i wznieść na wysoki poziom cyberbezpieczeństwo, co nie jest w pełni odzwierciedlone w postawionych wymaganiach, co do rozwiązań bezpieczeństwa systemów teleinformatycznych.

Regulacje systemu informatyzacji podmiotów publicznych wskazują wprost wykaz sześciu norm, które należy zastosować do opracowania i wdrożenia systemu zarządzania usługami i bezpieczeństwem systemów teleinformatycznych. Takie podejście stwarza podstawę i warunki do zbudowania kompletnego i skutecznego systemu zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów publicznych.

Regulacje prawne, omówione powyżej, formułują wymagania wobec podmiotów nimi objętych dotyczące wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa. Do realizacji tego celu w/w regulacje wskazują na konieczność zastosowania międzynarodowych i krajowych norm ISO, jednakże każda z regulacji wskazuje inny ich zbiór, co w połączeniu z niespójnością rozwiązań bezpieczeństwa teleinformatycznego zawartego w tych regulacjach tworzy nieprecyzyjne i niedostateczne podstawy do budowy wysokiego poziomu bezpieczeństwa krajowych systemów teleinformatycznych.

Zastosowanie jednorodnego i spójnego zbioru norm ISO kompleksowo adresujących kwestie zarządzania bezpieczeństwem informacji i systemów teleinformatycznych do wdrożenia wymaganego przez regulacje prawne systemu zarządzania bezpieczeństwem, szczególnie w formie zintegrowanego systemu zarządzania bezpieczeństwem, zdaniem autora,

byłoby najbardziej efektywnym rozwiązaniem realizującym zamierzone cele bezpieczeństwa[375]. System zarządzania bezpieczeństwem systemów teleinformatycznych powinien być wdrażany we wszystkich podmiotach objętych regulacjami adresującymi kwestie cyberbezpieczeństwa jako zbiór jednakowych wytycznych, opartych na normach międzynarodowych i krajowych ISO. Należy opracować zestaw odpowiednich do problematyki cyberbezpieczeństwa najaktualniejszych norm ISO i zawrzeć w odpowiednich regulacjach do zastosowania przez podmioty objęte regulacjami cyberbezpieczenstwa[376]. Optymalnym rozwiązaniem dla efektywnego zarządzania bezpieczeństwem systemów teleinformatycznych zdaje się być uspójnienie i integracja rozwiązań zarządczych i organizacyjnych w tym zakresie, co wymagałoby nadania nowej formuły prawnej i instytucjonalnej dokumentom strategicznym i operacyjnych oraz regulacjom prawnym. Zdaniem autora takie rozwiązanie wpłynęłoby na poprawę skuteczności wdrażanych rozwiązań i zwiększenie cyberbezpieczeństwa państwa.

Zdaniem autora zasadnym jest, zgodnie ze zdefiniowaną hipotezą, dotyczącą przedmiotowych zagadnień niniejszego rozdziału, ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych, co zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.

6.3. Wyniki przeprowadzonych badań

W ramach procesu badawczego, realizowanego w zakresie zagadnienia doboru norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP, stanowiącym przedmiotową problematykę niniejszego rozdziału, poddano weryfikacji hipotezę autora brzmiącą:

Ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa,

sformułowaną jako odpowiedź na postawione pytanie badawcze:

[375] Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów,* wyd. cyt., s. 144
[376] Mąkosa G., *Cyberbezpieczeństwo,* wyd. cyt., s. 116

Jakie międzynarodowe i krajowe normy, metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych są aktualnie wymagane i jakie powinny zostać wskazane do stosowania, aby zapewnić odpowiedni poziom bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP?

W celu znalezienia odpowiedzi na postawione pytanie badawcze oraz zweryfikowania sformułowanej hipotezy, w procesie badawczym zostały postawione respondentom – ekspertom pytania, jak niżej:

4. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?
   4.1. *Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.*
   4.2. *Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa.*
   4.3. *Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinny być oparte o:*
      1) *Normy ISO wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301);*
      2) *Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762);*
      3) *Normy ISO wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762);*

4) *Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.);*
5) *Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301;*
6) *Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania;*
7) *Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST);*
8) *Standardy ITIL, RESILIA;*
9) *Dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania;*
10) *Inne (jakie?).*

W wyniku przeprowadzonego badania uzyskano od respondentów – ekspertów szereg odpowiedzi na postawione pytania. Analiza uzyskanych odpowiedzi na poszczególne pytania, wyrażone w tezach w nich zawartych, została przestawiona i omówiona poniżej tekście niniejszego podrozdziału.

Szczegółowe zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 4.

Wynik badania w zakresie pytania 4.1.

Wobec tezy pytania 4.1.,

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa,

wśród udzielonych przez respondentów odpowiedzi, 15 (33,33%) osób wyraziło zgodę z tezą, przy czym wszystkie (15) raczej się zgodziły, natomiast 25 (57,78%) osób nie zgodziło się z tezą, przy czym zdecydowana większość (23) raczej się nie zgodziła, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zdecydowanie nie zgadzają się (26 głosami braku zgody, przy 15 głosach zgody), z tezą zawartą w pytaniu.

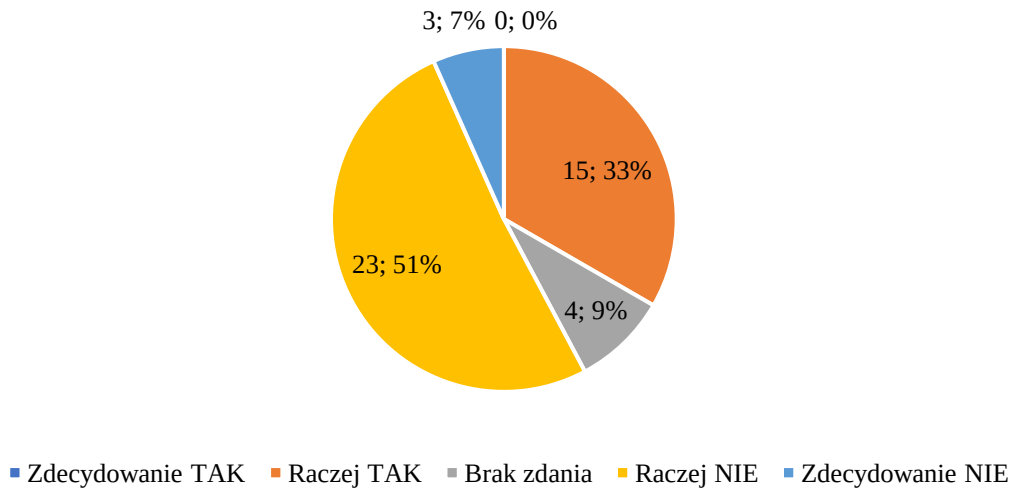
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 46 i na rysunku 34.

Tabela 46. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.1.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	15 / 26	0	15	4	23	3
%	100	33,33 / 57,78	0	33,33	8,89	51,11	6,67

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 34. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.1.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w powyższym zakresie wskazuje, że respondenci uważają za niewłaściwie sformułowane aktualnie wymagania względem bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa. Wskazuje to na konieczność opracowania nowych, bardziej efektywnych wymagań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego opartych na normach.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Przedstawione przez respondentów jako uzupełnienie do wybranej opcji odpowiedzi, argumenty, opinie i komentarze, zdecydowanie odnoszą się bezpośrednio do rozwiązań normatywnych cyberbezpieczeństwa dedykowanych podmiotom systemu. Zdarzają się także wątki odnoszące się do krajowych rozwiązań organizacyjnych bezpieczeństwa i zagadnień technicznych. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających), i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** stwierdzili, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane. Oparcie przepisów UKSC na uznanych standardach w zakresie bezpieczeństwa, takich jak ISO 27001, ISO 22301 powoduje, że zastosowane rozwiązania zarządcze, organizacyjne i techniczne podmiotów krajowego systemu cyberbezpieczeństwa zapewniają efektywność krajowego systemu cyberbezpieczeństwa oraz odpowiedni poziom bezpieczeństwa państwa w stosunku do oszacowanych zagrożeń (analiza ryzyka prowadzona na poziomie podmiotu i świadczonych usług). Zauważono, że bezpieczeństwo jest odpowiedzialnością każdego kierownika danego podmiotu, a mechanizmy ustawowe strukturyzują rozwiązania, które ułatwiają realizację obowiązków. Respondenci zwrócili uwagę, że problemem pozostaje ich właściwe wdrożenie.

Respondenci **nie zgadzający się z tezą pytania** w swoich argumentach, opiniach i komentarzach zauważali, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów KSC wymagają doskonalenia. Na obecnym etapie Ustawa KSC wprowadza pewne zadania, nie do końca możemy powiedzieć o zbudowaniu „systemu". Wszystko wygląda dobrze w teorii, ale w praktyce wygląda to wciąż słabo. Rozwiązania te dopiero teraz są budowane i ich obecna efektywność nie jest adekwatna. Przyjęte kierunki należy ocenić pozytywnie, ale wymagany jest jeszcze znaczny rozwój tych działań. Zwrócono uwagę, że obecna Ustawa KSC nie przewiduje żadnych katalogów proponowanych zabezpieczeń, zakres wymagań jest bardzo ogólnie zdefiniowany, zdecydowana większość firm nie radzi sobie z monitorowaniem środowiska OT, zarządzaniem podatnościami i analizą ryzyka, wiele obszarów jest pominiętych, jak choćby odkrywanie/wyszukiwanie podatności w sprzęcie ICT.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 4., ppkt 4.1.

Autor rozprawy w pełni zgadza się z wynikiem ustalonym przez respondentów, przez co zdecydowanie nie zgadza się z tezą postawioną w pytaniu. Zdaniem autora rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa nie są właściwie zdefiniowane i nie zapewniają efektywności krajowego systemu cyberbezpieczeństwa i odpowiedniego poziomu bezpieczeństwa państwa.

Wynik badania w zakresie pytania 4.2.

Wobec tezy pytania 4.2.,

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa,

wśród udzielonych przez respondentów odpowiedzi, 31 (68,89%) osób wyraziło zgodę z tezą, przy czym rozkład zdecydowanej i raczej zgody jest porównywalny i równomierny, natomiast 9 (20,00%) osób nie zgodziło się z tezą, prz czym wszystkie osoby (9) raczej się nie zgodziły, nie jest to więc twardy, zdecydowany brak zgody.

Wnioskować należy, wobec uzyskanych odpowiedzi, że respondenci zdecydowanie zgadzają się (31 głosami zgody, przy 9 głosach braku zgody), z tezą pytania.

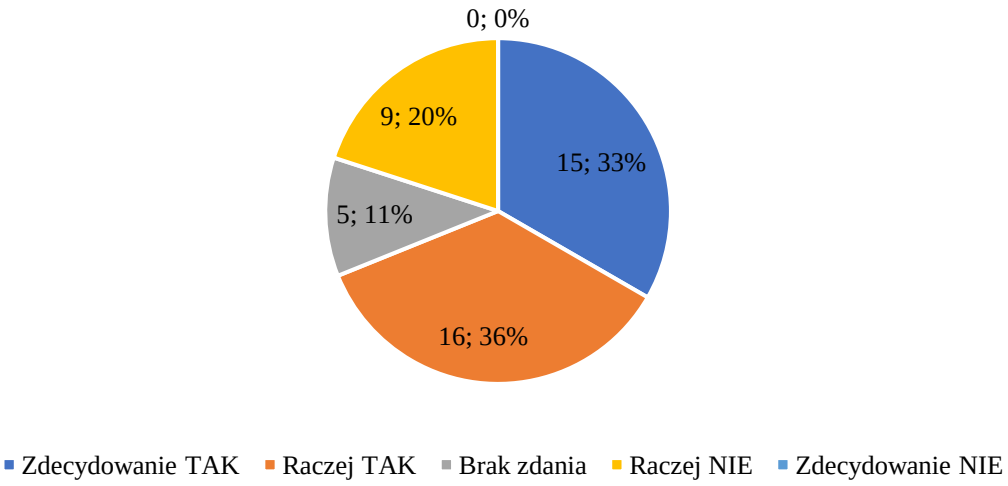
Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 47 i na rysunku 35.

Tabela 47. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.2.

WYNIK	Suma	Wynik T / N	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
Szt.	45	31 / 9	15	16	5	9	0
%	100	68,89 / 20,00	33,33	35,56	11,11	20,00	0

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 35. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.2.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Wynik badania w zakresie powyższego pytania zdecydowanie wskazuje, że respondenci podzielają zdanie, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa tych systemów i podmiotów. Respondenci oczekują zdefiniowania zbioru norm zapewniającego efektywne zarządzania bezpieczeństwem, adresowanego do wszystkich podmiotów systemu cyberbezpieczeństwa.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Przedstawione przez respondentów, argumenty, opinie i komentarze uzupełniające odpowiedzi, zdecydowanie odnoszą się bezpośrednio do rozwiązań normatywnych cyberbezpieczeństwa dedykowanych podmiotom systemu. Zdarzają się także wątki odnoszące się do krajowych rozwiązań organizacyjnych bezpieczeństwa i rozwiązań technicznych. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów, zarówno zgadzających się (zdecydowanie i raczej się zgadzających), i nie zgadzających się (zdecydowanie i raczej się nie zgadzających) z tezą postawionego pytania.

Respondenci **zgadzający się z tezą pytania** w uzupełnieniu odpowiedzi przedstawili swoje argumenty, opinie i komentarze, w których stwierdzają, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów

krajowego systemu cyberbezpieczeństwa powinny być jednolite, budowanie systemów cyberbezpieczeństwa w oparciu o normy i standardy jest uzasadnione. Jak najpełniejsza synergia i integracja działań przy uwzględnieniu wszelkich możliwych obszarów funkcjonowania organizacji to jedyna droga do najwyższej skuteczności działań i zapewnienia jak najwyższego poziomu bezpieczeństwa państwa. Standardy, chociażby prowadzenia dokumentacji czy organizacja poszczególnych obszarów systemu cyberbezpieczeństwa (jak monitoring, response, detection itp.), powinny być zdefiniowane i wymagane. Spójne wzorce są konieczne do zorganizowanego i jednolitego sposobu zarządzania w kontekście zagrożeń cyberbezpieczeństwa. Zwrócono również uwagę, że ujednolicanie rozwiązań w oparciu o jednolitą analizę ryzyka jest najlepszym podejściem, jednolity powinien być katalog i metodologie zarządzania ryzykiem, jednak powinien być on otwarty na kontrole (zabezpieczenia) i ryzyka specyficzne dla danego sektora lub charakterystyki operacyjnych podmiotów działających w systemie. Rozwiązania techniczne nie powinny być ujednolicane z uwagi na słabości technologiczne, jednak wskazane jest ustalenie minimalnego wymaganego poziomu funkcjonalności wraz z ośrodkiem certyfikacji/testów niezależnie potwierdzających spełnienie wymogów. Ujednoliceniu wymagań mają służyć programy certyfikacji wprowadzane w oparciu o rozporządzenie o cyberbezpieczeństwie. Podniesiono jednak konieczność zachowania adekwatnych wymogów dla podmiotów o różnej wielkości, z uwzględnieniem różnic w sektorach i organizacjach. Ważne jest postawienie racjonalnych wymagań możliwych do spełnienia i osiągalnych dla wszystkich podmiotów oraz określenie wymaganych poziomów dojrzałości i wdrożenia elementów dodatkowych ponad standard w uzależnieniu od wagi/typu danej organizacji. Stwierdzono także, że powinien być wprowadzony ustawowy obowiązek wdrożenia przez podmioty krajowego systemu cyberbezpieczeństwa norm, np. ISO 27001, a w Ustawie KSC powinien znaleźć się przepis, że jeśli dla danego sektora lub podsektora obowiązują rozwiązania i standardy branżowe związane z cyberbezpieczeństwem, to również mogą być stosowane. Zwrócono uwagę, że normy takie jak ISO27001, ISO220301 czy ISO27032 są uniwersalne i jeśli przepisy UKSC będą się do nich odwoływać, nie będzie problemów z ich stosowaniem w różnych podmiotach i sektorach. Podniesiono, że należy zwiększać dostępność wiedzy i kształcenia oraz podnoszenie kompetencji kadr, które odpowiadają w podmiotach KSC na różnych poziomach odpowiedzialności za rozwiązania zarządcze, organizacyjne i techniczne. W związku z brakiem specjalistów w zakresie cyberbezpieczeństwa, należy w miarę ujednolicać kompetencje i rozwiązania, by umożliwiać przepływ pomiędzy sektorami specjalistów oraz łatwiejszą ich adaptację

w pracy. Jednocześnie należy zachować konieczną elastyczność zastosowań dla wskazywanych norm, wytycznych i standardów w poszczególnych podmiotach. Wskazano również korzyści wynikające z ujednolicenia norm, wytycznych i standardów, którymi mogą być: jeden punkt odniesienia i jasność oceny odporności, mitygacja ryzyka braku kompatybilności, ułatwienie projektowania i budowy również dla mniej doświadczonych podmiotów, szybsze dostosowanie się podmiotów, upowszechnienie świadomości ich istnienia, zminimalizowanie cen i poprawa dostępności wiedzy i narzędzi.

Respondenci **nie zgadzający się z tezą pytania** podnosili głównie kwestie różnorodności sektorów i podmiotów i różnic między nimi, również zdefiniowanych w przepisach prawa i dedykowanych normach i standardach. Respondenci zauważali, że poszczególne sektory znacznie różnią się, co do wymogów prawnych i stosowanych rozwiązań organizacyjnych, a różnice pomiędzy branżami/obszarami (np. kolej, lotnictwo, przemysł chemiczny, administracja), jak też różnice np. środowisk IT/OT, kultur organizacyjnych, zależności (wewnętrznych i zewnętrznych) w różnych podmiotach są tak duże, że definiowanie jednolitych rozwiązań spowoduje, że będą one bezużyteczne. Różne podmioty pełnią różną rolę, więc nie można zastosować tych samych wytycznych, norm itp. Różnorodność branż i ich wpływu na życie społeczeństwa powoduje, że tak silna korelacja nie jest ani potrzebna, ani możliwa. Stwierdzono też, że rozwiązania krajowe powinny być jednolite, co do wyniku, nie, co do środka. Poziom odporności i techniczne środki bezpieczeństwa powinny być oparte o podejście bazujące na ryzyku, różne sektory mają inne profile ryzyka. Zwrócono uwagę, że w wielu branżach obowiązują różne normy sektorowe, jedynym wspólnym mianownikiem jest rodzina norm ISO/IEC 27000, ewentualnie ISO/IEC dotyczące ciągłości działania i tak powinno pozostać. Pozostałe rodziny norm powinny podlegać świadomemu wyborowi przez podmioty danego sektora. Praktyka wskazuje ze nadmiar formalnych regulacji i wymagań powoduje, że nie są one faktycznie przestrzegane.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 4., ppkt 4.2.

Autor rozprawy w pełni zgadza się z tezą postawioną w pytaniu. Zdaniem autora rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa.

Wynik badania w zakresie pytania 4.3.

Wobec pytania 4.3.,

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinny być oparte o wariant wyboru,

respondenci udzielili w sumie 300 odpowiedzi, w tym odnośnie wariantu 1 – 32 głosy, wariantu 2 – 31 głosów, wariantu 3 – 32 głosy, wariantu 4 – 31 głosów, wariantu 5 - 36 głosów, wariantu 6 – 36 głosów, wariantu 7 – 36 głosów, wariantu 8 – 30 głosów, wariantu 9 – 31 głosów, w których:

- wariant 1 przedstawionego rozwiązania uzyskał poparcie 26 (8,67%) głosów, przy czym zdecydowana większość głosów (18) zdecydowanie go poparła, jest to więc twarde, zdecydowane poparcie, natomiast 1 (0,33%) głos nie poparł tego wariantu, przy czym raczej nie poparł;
- wariant 2 przedstawionego rozwiązania uzyskał poparcie 21 (7,00%) głosów, przy czym większość głosów (13) zdecydowanie go poparła, natomiast 5 (1,67%) głosów nie poparła tego wariantu, przy czym zdecydowana większość (4) głosów raczej nie poparła;
- wariant 3 przedstawionego rozwiązania uzyskał poparcie 22 (7,33%) głosów, przy czym większość głosów (13) zdecydowanie go poparła, natomiast 5 (1,67%) głosów nie wyraziło poparcia dla tego wariantu, przy czym zdecydowana większość (4) głosów raczej nie poparła;
- wariant 4 przedstawionego rozwiązania uzyskał poparcie 21 (7,00%) głosów, przy czym większość głosów (13) raczej go poparła, natomiast 2 (0,67%) głosy nie wyraziło poparcia dla tego wariantu;
- wariant 5 przedstawionego rozwiązania uzyskał poparcie 23 (7,67%) głosów, przy czym większość głosów (14) zdecydowanie go poparła, natomiast 4 (1,33%) głosów nie wyraziło poparcia dla tego wariantu, przy czym większość (3) głosów raczej nie poparła;
- wariant 6 przedstawionego rozwiązania uzyskał poparcie 25 (8,33%) głosów, przy czym zdecydowana większość głosów (18) zdecydowanie go poparła, natomiast 4 (1,33%) głosów nie wyraziło poparcia dla tego wariantu;

- wariant 7 przedstawionego rozwiązania uzyskał poparcie 26 (8,67%) głosów, przy czym większość głosów (15) zdecydowanie go poparła, natomiast 3 (1,00%) głosy nie wyraziło poparcia dla tego wariantu, przy czym raczej nie poparła;
- wariant 8 przedstawionego rozwiązania uzyskał poparcie 10 (3,33%) głosów, przy czym zdecydowana większość głosów (8) zdecydowanie go poparła, natomiast 9 (3,00%) głosów nie wyraziło poparcia dla tego wariantu, przy czym zdecydowana większość (8) głosów raczej nie poparła;
- wariant 9 przedstawionego rozwiązania uzyskał poparcie 7 (2,33%) głosów, przy czym większość głosów (5) zdecydowanie go poparła, natomiast 14 (4,67%) głosów nie wyraziło poparcia dla tego wariantu, równomiernie zdecydowanie i raczej nie poparła.

Respondenci zaproponowali 2 dodatkowe standardy bezpieczeństwa systemów teleinformatycznych (Rekomendacje i dobre praktyki ENISA i Model dojrzałości zarządzania incydentami – SIM3 (Security Incident Management Maturity Model)) do zastosowania przez podmioty krajowego systemu cyberbezpieczeństwa, które zyskały po 1 głosie oraz podejście, aby stosować standardy bezpieczeństwa uwzględniające specyfikę sektorów, które zyskało 3 głosy.

Podsumowując uzyskane wyniki, należy stwierdzić, że respondenci, w swojej większości, najbardziej poparli rozwiązanie wariantu 1 (26 głosów na tak, przy 1 głosie na nie), następnie wariant 7 (26 głosów na tak, przy 3 głosach na nie), a następnie wariant 6 (25 głosów na tak, przy 4 głosach na nie). Kolejne były warianty: 5 (24/3 głosów), 4 (21/2 głosów), 3 (22/5 głosów) i 2 (21/5 głosów). Wariant 8 uzyskał równomierne głosy poparcia i braku poparcia, natomiast wariant 9 uzyskał zdecydowany brak poparcia (14 głosów na nie, przy 7 głosach na tak) i został odrzucony przez respondentów.

Zdanie respondentów zostało opracowane, na podstawie i zgodnie ze zagregowanymi danymi uzyskanych w badaniu odpowiedzi. Szczegółowe zestawienie ze zagregowanymi danymi uzyskanych odpowiedzi respondentów zostało przedstawione w tabeli 48 i na rysunku 36.

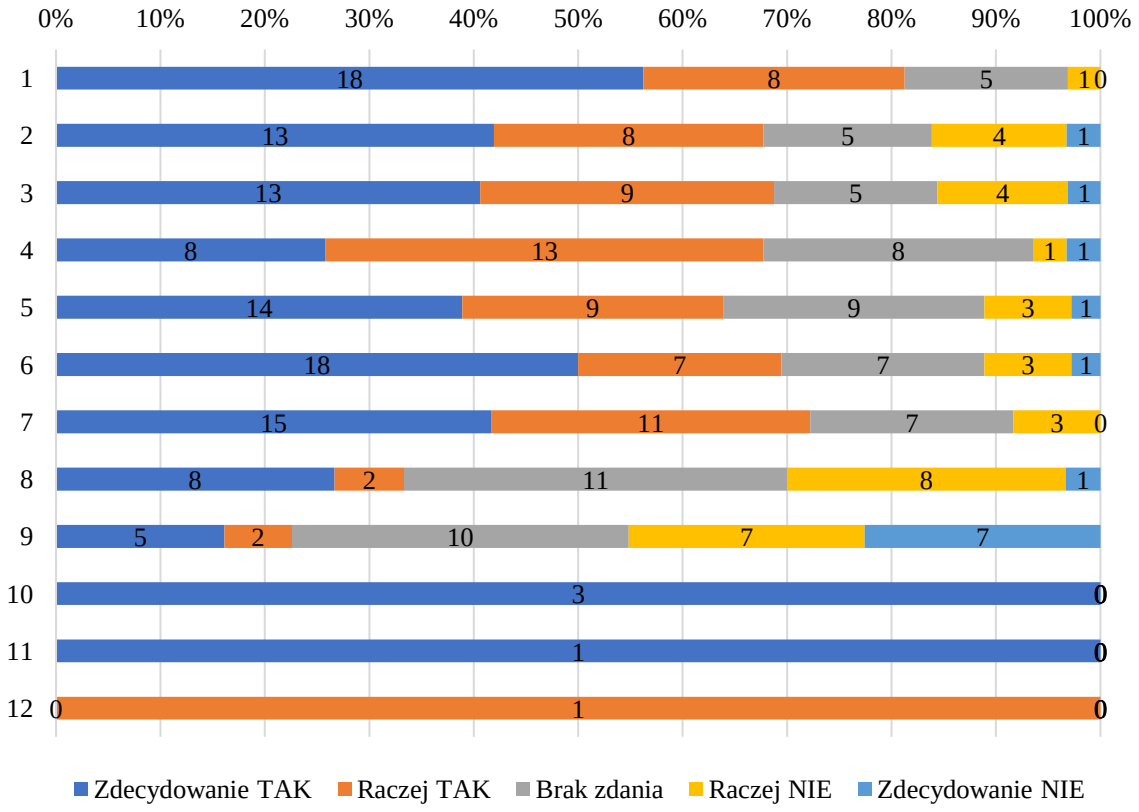
Tabela 48. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.3.

Lp	Standardy bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa	Suma 300	Wynik T / N Szt./%	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301)	32	26 / 1 8,67 / 0,33	18	8	5	1	0
2	Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)	31	21 / 5 7,00 / 1,67	13	8	5	4	1
3	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)	32	22 / 5 7,33 / 1,67	13	9	5	4	1
4	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.)	31	21 / 2 7,00 / 0,67	8	13	8	1	1
5	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301	36	23 / 4 7,67 / 1,33	14	9	9	3	1
6	Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania	36	25 / 4 8,33 / 1,33	18	7	7	3	1
7	Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST)	36	26 / 3 8,67 / 1,00	15	11	7	3	0
8	Standardy ITIL, RESILIA	30	10 / 9 3,33 / 3,00	8	2	11	8	1
9	Dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania	31	7 / 14 2,33 / 4,67	5	2	10	7	7

10	Inne (jakie?) Uwzględniające specyfikę sektorów	3	3 / 0 3,00 / 0	3	0	0	0	0
11	Inne (jakie?) Rekomendacje i dobre praktyki ENISA	1	1 / 0 0,33 / 0	1	0	0	0	0
12	Model dojrzałości zarządzania incydentami – SIM3 (Security Incident Management Maturity Model)	1	1 / 0 0,33 / 0	0	1	0	0	0

Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Rys. 36. Zestawienie zagregowanych odpowiedzi respondentów na pytanie 4.3.



Źródło: opracowanie własne na podstawie przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

W odpowiedziach na postawione pytanie 4.3. odniesiono się do udzielonych głosów na tak lub na nie, ponieważ nie wszyscy respondenci zdecydowali się w ogóle udzielić odpowiedzi na to pytania, a spośród udzielających odpowiedzi, część oddała tylko jeden głos, wskazując wybrany wariant, inni respondenci wskazywali każdy z wariantów przypisując go do wybranej opcji standardowej odpowiedzi. Stąd pod uwagę nie jest brana liczba respondentów, a liczba oddanych głosów w wyborze wariantu rozwiązania.

Wynik badania wykazuje, że respondenci miażdżącą przewagą wskazali na rozwiązania normatywne już istniejące w regulacjach ustawy KSC, tak jakby nie chcieli zmian, co przeczy konkluzji, że jest to rozwiązanie niewłaściwie zdefiniowane. Respondenci przeważającą pulę głosów skierowali na rozwiązania NSC (opracowane jako tłumaczenie NIST) i NIST, które nie są popularne w podmiotach i nie mają uzasadnienia w przepisach prawa. Spośród norm ISO respondenci wskazali szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych oraz norm zarządzania usługami informatycznymi i ciągłości działania. Niezależnie od powyższego i różnic zdań respondentów, wszystkie wskazane rozwiązania uzyskały znaczącą przewagę akceptacji nad odrzuceniem.

Konkludując, należy stwierdzić, że zdaniem większości respondentów (oddanych głosów) rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinny być oparte o, w kolejności:

1) Normy ISO wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) (rozwiązanie pierwszego wyboru - wariant 1 proponowanej odpowiedzi pytania ankietowego);
2) Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST) (rozwiązanie drugiego wyboru - wariant 7 proponowanej odpowiedzi pytania ankietowego);
3) Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania (rozwiązanie trzeciego wyboru - wariant 6 proponowanej odpowiedzi pytania ankietowego);
4) Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301 (rozwiązanie czwartego wyboru - wariant 5 proponowanej odpowiedzi pytania ankietowego);
5) Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/

ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) (rozwiązanie piątego wyboru - wariant 4 proponowanej odpowiedzi pytania ankietowego);

6) Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie szóstego wyboru - wariant 3 proponowanej odpowiedzi pytania ankietowego);
7) Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie siódmego wyboru - wariant 2 proponowanej odpowiedzi pytania ankietowego).

Proponowane jednolite rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, nie powinny być oparte o:

1) wariant 8 - Standardy ITIL, RESILIA;
2) wariant 9 - dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania.

Respondenci biorący udział w badaniu zostali poproszeni o uzasadnienie swoich odpowiedzi. Ze względu na charakter pytania i specyfikę odpowiedzi, polegającej na wskazaniu preferowanych zbiorów norm, metodyk i standardów, jako obowiązujących dla podmiotów systemu cyberbezpieczeństwa, przedstawione przez respondentów argumenty, opinie i komentarze należy uznać za uniwersalne, nie odnoszące się do akceptacji lub braku akceptacji dla problemowego zagadnienia, lecz jako odniesienie się do dokonanego wyboru opcji odpowiedzi. Poniżej przedstawiono zestawienia argumentów, opinii i komentarzy respondentów do udzielonych odpowiedzi.

Respondenci w uzupełnieniu do dokonanego wyboru opcji odpowiedzi w przedstawionych argumentach, opiniach i komentarzach stwierdzają m.in., że kluczowym elementem jest wybranie spójnych standardów i odejście od całkowitej dowolności interpretacji, ponieważ prowadzi to do skrajnych przypadków interpretowania punktów odniesienia do tylko tych, które są wygodne i łatwe do dostosowania. Podmioty KSC należy nie tylko zobowiązywać, ale przede wszystkim zachęcać do wdrażania rozwiązań, które wynikają z przytoczonych standardów, rekomendacji i dobrych praktyk, najlepiej dopasowanych do

ich specyfiki działania. Obowiązują nas normy i prawo międzynarodowe, nie jesteśmy państwem autarchicznym, należymy do organizacji międzynarodowych, których normy są dla Polski obowiązujące. Ujednolicenie standardu znacznie upraszcza kwestie związane z zarządzaniem oraz utrzymaniem systemu bezpieczeństwa oraz rozliczaniem realizacji zadań. Normy ISO są najpowszechniejszym standardem dla określenia szeroko rozumianego bezpieczeństwa informacji oraz są już wskazane w wielu regulacjach prawnych krajowych. Wskazane normy i standardy są uniwersalne i jeśli przepisy UKSC będą się do nich odwoływać nie będzie problemów z ich stosowaniu w różnych podmiotach i sektorach, ponieważ są sprawdzonym sposobem zarządzania w skali podmiotu (firmy). Rozwiązania oparte na wymienionych normach w stopniu bardzo dobrym zapewniałyby bezpieczeństwo organizacyjne i techniczne systemów teleinformatycznych. Wskazane normy, standardy, wytyczne i dobre praktyki powinny zostać określone w dokumentach prawnych (np. rozporządzeniu ministra właściwego ds. informatyzacji) wraz z procedurami związanymi z: akredytacją, certyfikacją i deklaracją zgodności ICT (produktów, usług, procesów). Powinno się uwzględniać także normy i standardy branżowe obowiązujące w danym sektorze lub podsektorze. Standardy powinny być adekwatne do danej branży. Ich dobór powinien też zależeć od danej organizacji, a ich ilość od poziomu dojrzałości. Sporo standardów da się na siebie nawzajem zmapować – są do siebie podobne. Należy zaznaczyć, że nie ma zasady one size fits all. Różne rozwiązania działają dla różnych rodzajów podmiotów. Część międzynarodowych podmiotów (np. banki) mają obowiązek stosowania własnych metodyk i standardów. Podkreślono, że system obowiązków nie może być zbyt sztywny. Respondenci stwierdzili, że jedynym wspólnym mianownikiem w obszarze bezpieczeństwa są normy rodziny 27000, można również uznać za wspólnie wymaganą normę dotyczącą ciągłości działania ISO/IEC 22301. Zauważono, że normy ISO są potężnym narzędziem, ale wymagają dodatkowej pracy – nie są gotowymi rozwiązaniami do wdrożenia. Różne normy ISO się uzupełniają, co jest dobre. Część systemów proponowanych przez normy ma dobre, zgodne z ISO, alternatywy. Nie trzeba np. używać ISO/IEC 27035, aby zbudować skuteczny i bezpieczny system reagowania na incydenty bezpieczeństwa informacji. ISO 20000 bazuje na ITIL, jednak ITIL to katalog dobrych praktyk bez obowiązku wdrażania całości – mniejszy podmiot łatwiej spełni ITILa, niż ISO 20000. Seria 270xx może być obowiązkowa, jednak należy dostosować wymagania do podmiotu i niekoniecznie należy wymagać jednocześnie 27035 i 27001. Tworzenie własnych standardów ma sens tylko, gdy jednocześnie wydana zostanie mapa zgodności z już istniejącymi, np. jeśli masz ISO 27001, to spełniasz całość lub większość, ponieważ istnieje już ich tak dużo i na pewno regulują wystarczająco kwestii, np.

niewymieniony COBIT, IEC 62443 uznawany w przemyśle, wydania SANS i CIS, NIST tworzony na potrzeby US Gov oraz dokumenty CISA, FBI, US-CERT. Normy (NIST) czy dobre praktyki (ITIL) powinny być stosowane z dobrowolnego wyboru danego podmiotu. Standardy NIST mają bardzo pragmatyczne podejście do operacyjnej strony cyberbezpieczeństwa i oczywiście bez kłopotu można ich wymagania zmapować z wymaganiami ISO. Zostały także referencją dla NSC, które są kompilacją ISO i NIST. Stwierdzono, że mix wymagań z ISO i NIST będzie dobrym punktem wyjścia. Zwrócono uwagę, że wymagalność komercyjnych norm może być kontrowersyjna. Zauważono, że normy są ważne, niemniej to jednolitość podejścia do analizy ryzyka jest kluczowa dla efektywności działania KSC. Cała rodzina ISO 27000 jest oparta na ryzyku. Podniesiono także, że koordynacja w zakresie cyberbezpieczeństwa wymaga standaryzacji języka i metod oceny ryzyka na poziomie transgranicznym, a nie krajowym z uwagi na charakter zagrożeń cyber. Normy ISO w tym zakresie nie są wystarczająco precyzyjne, aby spełnić warunki komunikacji wspierające szybką koordynację reakcji na zagrożenia transgraniczne. Podkreślono, że ważne jest ciągłe doskonalenie organizacji, badać poziom jej dojrzałości, aby z czasem sięgać po więcej oraz pozostawienie wyboru organizacjom standardów ze względu na ich branżowe wytyczne.

Szczegółowe i kompletne zestawienie udzielonych przez respondentów odpowiedzi wraz z uzasadnieniami zostało zawarte w Załączniku nr 2, pkt 4., ppkt 4.3.

Autor rozprawy częściowo zgadza się z dominującym wynikiem uzyskanych odpowiedzi respondentów i konkluzją. Zdaniem autora proponowane w tezie pytania 4.2 jednolite rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinny być oparte o, w kolejności:

1. Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301 (rozwiązanie pierwszego wyboru - wariant 5 proponowanej odpowiedzi pytania ankietowego);
2. Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie drugiego wyboru - wariant 3 proponowanej odpowiedzi pytania ankietowego);

3. Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie trzeciego wyboru - wariant 2 proponowanej odpowiedzi pytania ankietowego);
4. Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) (rozwiązanie czwartego wyboru - wariant 4 proponowanej odpowiedzi pytania ankietowego);
5. Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) (rozwiązanie piątego wyboru - wariant 1 proponowanej odpowiedzi pytania ankietowego);
6. Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST) (rozwiązanie szóstego wyboru - wariant 7 proponowanej odpowiedzi pytania ankietowego);
7. Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania (rozwiązanie siódmego wyboru - wariant 6 proponowanej odpowiedzi pytania ankietowego).

Proponowane w tezie pytania 4.2 jednolite rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, nie powinny być oparte o:

1. wariant 8 - Standardy ITIL, RESILIA;
2. wariant 9 - dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania.

6.4. Podsumowanie wyników badania

Wyniki przeprowadzonego badania realizowanego w zakresie rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego podmiotów systemu cyberbezpieczeństwa, stanowiącym przedmiotową problematykę niniejszego rozdziału pozytywnie zweryfikowały postawioną hipotezę stanowiącą, że *ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny*

w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.

Wyniki badania pozwalają na sformułowanie wniosków do zastosowania w opracowaniu proponowanej koncepcji rozwiązań w zakresie *wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP*. Wnioski z wyników badania są następujące:

1. Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa **nie są właściwie zdefiniowane i nie zapewniają efektywności** krajowego systemu cyberbezpieczeństwa **i odpowiedniego poziomu bezpieczeństwa** państwa.
2. Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa **powinny być zdefiniowane jednolicie** dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa.
3. Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinny być oparte o, w kolejności:
    1) Normy ISO wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) (rozwiązanie pierwszego wyboru - wariant 1 proponowanej odpowiedzi pytania ankietowego), co stoi w sprzeczności w wnioskiem z badania w pkt 1;
    2) Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST) (rozwiązanie drugiego wyboru - wariant 7 proponowanej odpowiedzi pytania ankietowego);
    3) Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania (rozwiązanie trzeciego wyboru - wariant 6 proponowanej odpowiedzi pytania ankietowego);
    4) Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1,

-2)) i ciągłości działania ISO 22301 (rozwiązanie czwartego wyboru - wariant 5 proponowanej odpowiedzi pytania ankietowego);

5) Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) (rozwiązanie piątego wyboru - wariant 4 proponowanej odpowiedzi pytania ankietowego);
6) Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie szóstego wyboru - wariant 3 proponowanej odpowiedzi pytania ankietowego);
7) Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762) (rozwiązanie siódmego wyboru - wariant 2 proponowanej odpowiedzi pytania ankietowego).

4. Proponowane jednolite rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, nie powinny być oparte o:
   1) standardy ITIL, RESILIA (wariant 8 proponowanej odpowiedzi pytania ankietowego);
   2) dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania (wariant 9 proponowanej odpowiedzi pytania ankietowego).

System cyberbezpieczeństwa RP potrzebuje ujednoliconego i zharmonizowanego normatywnego rozwiązania bezpieczeństwa systemów teleinformatycznych tworzących polską cyberprzestrzeń, należących do kluczowych podmiotów sfery administracyjno-społeczno-gospodarczej w celu zapewnienia podobnego i porównywalnego w skali kraju poziomu ich odporności i bezpieczeństwa, i przez to bezpieczeństwa kraju. Zasadnym jest opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

6.5. Koncepcja bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP

W ramach przeprowadzonego procesu badawczego w zakresie rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego, czyli norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP, stanowiących przedmiotową problematykę niniejszego rozdziału, na podstawie wyników przeprowadzonego badania zweryfikowano pozytywnie postawioną przez autora hipotezę i sformułowano wnioski, wynikające z uzyskanych od respondentów odpowiedzi na postawione w badaniu pytania, które zostały wykorzystane w proponowanej koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

Formułując koncepcję rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego, należy uwzględnić wymaganie prawne w zakresie stosowania norm, metodyk i standardów. Zgodnie z wymaganiami prawnymi w pierwszej kolejności należy stosować normy krajowe, następnie normy europejskie, a następnie normy międzynarodowe. Gdy w zakresie pożądanego zakresu zagadnienia nie ma norm dopuszcza się stosowanie metodyk oraz standardów branżowych i organizacji krajowych i międzynarodowych[377]. Ustawa o krajowym systemie cyberbezpieczeństwa wraz z rozporządzaniami ustanawiają wymagania wdrożenia systemu zarządzania bezpieczeństwem w oparciu wskazane międzynarodowe i krajowe normy ISO. Operatorzy muszą wdrożyć ISO/IEC 27001 w zakresie systemu zarządzania bezpieczeństwem informacji systemu teleinformatycznego oraz ISO 22301 w zakresie zarządzania ciągłością działania usługi kluczowej, wewnętrzne struktury cyberbezpieczeństwa operatorów i podmioty świadczące usługi w zakresie cyberbezpieczeństwa musza wdrożyć ISO/IEC 27001 w zakresie systemu zarządzania bezpieczeństwem informacji systemu teleinformatycznego oraz ISO 22301 w zakresie zarządzania ciągłością działania usługi reagowania na incydenty. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z Rozporządzenie KRI w zakresie ustanawiania wymagań dla zarządzania usługami systemów teleinformatycznych i ich bezpieczeństwa teleinformatycznego stwierdza, że zdefiniowane wymagania mogą być uznane za spełnione

[377] Ustawa z dnia 12 września 2002 r. o normalizacji, z późn. zmianami, Dz.U. 2015, poz. 1483, Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, z późn. zmianami, Dz.U. 2021, poz. 514, 925

jeśli są realizowane odpowiednio: z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 oraz na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Tak więc, uwzględniając wykładnię przepisów prawa, pierwszeństwo należy dać rozwiązaniom opartym o normy polskie i międzynarodowe ISO, a w następnej kolejności rozwiązaniom nienormatywnym, czyli metodykom i standardom branżowym - polskim standardom NSC i amerykańskim normom NIST.

Należy zwrócić uwagę, że w zakresie rozwiązań opartych o zbiór norm ISO, wyniki badania wskazały jako rozwiązanie pierwszego wyboru - wariant 1 proponowanej odpowiedzi pytania ankietowego, rozwiązanie oparte o normy ISO wskazane w regulacjach ustawy KSC i już obowiązujące (ISO 27001, ISO 22301). Takie rozwiązanie jednak nie powinno być akceptowane, ponieważ stoi w sprzeczności z wynikami odpowiedzi na pierwsze pytanie i wnioskiem z badania w pkt 1., stwierdzającym, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa nie są właściwie zdefiniowane i nie zapewniają efektywności krajowego systemu cyberbezpieczeństwa i odpowiedniego poziomu bezpieczeństwa państwa. W zakresie rozwiązania opartego o normy ISO należy wybrać takie, które agreguje najszersze wymagania oparte o normy ISO, uzyskujące jednocześnie największą liczbę głosów. W takiej sytuacji należy uwzględnić rozwiązanie kolejnego wyboru respondentów, uwzględniającego normy ISO. Jest to rozwiązanie czwartego wyboru respondentów - wariant 5 proponowanej odpowiedzi pytania ankietowego. Rozwiązanie oparte o szeroki katalog norm ISO dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301. Należy zwrócić uwagę, że ten wariant spełnia warunek i wniosek wynikający z odpowiedzi respondentów na drugie pytanie o wnioskiem z badania w pkt 2., stwierdzającym, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy. Spełnienie tego warunku

obliguje do uwzględnienia najszerszego zakresu wymagań dla wszystkich typów podmiotów systemu cyberbezpieczeństwa.

Koncepcja rozwiązania w zakresie wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP, adresująca wyniki i wnioski z badania, stanowi, że:

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa i powinny być oparte o szeroki katalog norm ISO dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301.

Opracowana koncepcja wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP stanowi nowum pracy, wypełnia zdiagnozowaną lukę, brak i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwego wykazu odpowiednich norm bezpieczeństwa teleinformatycznego. W ramach koncepcji zaproponowano znaczne rozszerzenie norm mających być zastosowanymi do wdrożenia rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego, zawierające normy zarządzania, jak i szeroki zestaw norm technicznych.

Zawarty w rozwiązaniu zbiór norm ISO jest to zestaw norm, który po wdrożeniu może gwarantować szerokie, kompleksowe i szczegółowe zaadresowanie aspektów zarządzania ciągłością działania, jakością i bezpieczeństwem systemów teleinformatycznych i ich usług oraz procesów związanych z ich funkcjonowaniem, a także usług publicznych i biznesowych wspieranych przez te systemy teleinformatyczne. Ten wariant jest preferowanym rozwiązaniem koncepcji doskonalenia wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP. Takie rozwiązanie zapewnia zgodność z wykładnią przepisów prawa oraz wynikami przeprowadzonego badania.

Tabela 49. Rozwiązania bezpieczeństwa systemów teleinformatycznych systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa, systemu informatyzacji podmiotów publicznych i koncepcji systemu cyberbezpieczeństwa RP – ujęcie porównawcze

Standardy bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP – ujęcie porównawcze			
Rozwiązania aktualnie obowiązujące			**Rozwiązanie koncepcyjne**
System zarządzania kryzysowego (SZK)	**Krajowy system cyberbezpieczeństwa (KSC)**	**System informatyzacji podmiotów publicznych (SIPP)**	**Rozwiązanie oparte o normy ISO systemu cyberbezpieczeństwa RP (SCRP)**
PN-EN ISO 27002	ISO 27001	ISO 27001	ISO 27001
IEC 62443/ ISA 62443	ISO 22301	ISO 27002	ISO 27002
NIST 800-82		ISO 27005	ISO 27005
NERC-CIP		ISO 24762	ISO 24762/ ISO 27031
TIA 942		ISO 20000 (-1, -2)	ISO 27032
ISO/IEC24762[378]			ISO 27033
PICS (Protecting Industrial Control Systems)			ISO 27034
			ISO 27035
			ISO 27040
			ISO 20000 (-1, -2)
			ISO 22301

Źródło: opracowanie własne na podstawie: wyniki przeprowadzonego badania w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r., Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 Nr 89 poz. 590, NPOIK, Załącznik 1 - Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje, Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Rozporządzenie w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych; 3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565, Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

[378] Norma została wycofana w 2014 r., źródło: iso.org [dostęp 10.03.2020]

Szczegółowe zestawienie porównawcze rozwiązanie bezpieczeństwa systemów teleinformatycznych, wypracowanego jako koncepcja doskonalenia oraz rozwiązań aktualnie obowiązujących w świetle przepisów prawa systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych zostało przedstawione w tabeli 49.

Zastosowanie jednorodnego i spójnego zbioru norm ISO, szczególnie w formie zintegrowanego systemu zarządzania kompleksowo adresującego kwestie zarządzania bezpieczeństwem informacji i systemów teleinformatycznych, zarządzania usługami i infrastrukturą systemów teleinformatycznych oraz ciągłością działania procesów związanych z ich funkcjonowaniem, a także usług publicznych i biznesowych wspieranych przez te systemy teleinformatyczne do wdrożenia wymaganego przez regulacje prawne systemu zarządzania bezpieczeństwem przez zobligowane do tego podmioty, zarówno krajowego systemu cyberbezpieczeństwa, jak i podmioty systemu zarządzani kryzysowego i systemu informatyzacji podmiotów publicznych, a także wszelkie inne podmioty realizujące ważne dla bezpieczeństwa i aspektów społeczno- gospodarczych państwa usługi i działalność, nie zobligowane prawnie do wdrożenia takiego systemu bezpieczeństwa w oparciu o normy lub standardy, zdaniem autora, byłoby najbardziej efektywnym rozwiązaniem realizującym zamierzone cele cyberbezpieczeństwa i bezpieczeństwa państwa.

Projektowanie i wdrażanie systemów zarządzania bezpieczeństwem systemów teleinformatycznych może być skutecznie wsparte uznanymi normami, metodykami i standardami, oferującymi wzorce metodycznego zorganizowania systemu, procesów i działań, a także rozwiązań technicznych. Wykorzystując przedstawione normy ISO bezpośrednio lub pośrednio adresujące kwestie zarządzania bezpieczeństwem systemów teleinformatycznych można zaproponować kilka wariantów zintegrowanego systemu zarządzania szeroko rozumianym bezpieczeństwem systemów teleinformatycznych.

6.6. Podsumowanie i wnioski

W rozdziale szóstym dokonano próby rozstrzygnięcia problemu badawczego dotyczącego rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP, sformułowanego jako pytanie badawcze: *jakie międzynarodowe i krajowe normy, metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych są aktualnie wymagane i jakie powinny zostać wskazane do stosowania, aby zapewnić odpowiedni poziom bezpieczeństwa systemów teleinformatycznych*

podmiotów systemu cyberbezpieczeństwa RP? Rozstrzygnięcie problemu zostało przeprowadzone poprzez weryfikację w procesie badawczym przyjętej hipotezy pomocniczej stwierdzającej, że: *ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.*

W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego dokonano przeglądu rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych. Przedstawiono i omówiono zagadnienia doboru norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa w ujęciu regulacji prawnych trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych. Dokonano analizy porównawczej wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów objętych ww. regulacjami w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego wskazuje, jako zalecenie czy sugestię, obszerną listę alternatywnych względem siebie branżowych norm międzynarodowych i krajowych, krajowy system cyberbezpieczeństwa wymaga wdrożenia bezpieczeństwa w oparciu o 2 normy ISO przez wybrane typy podmiotów, natomiast system informatyzacji podmiotów publicznych wymaga wdrożenia zarządzania systemami teleinformatycznymi i ich bezpieczeństwem w oparciu o 5 norm ISO przez podmioty publiczne. Poszczególne regulacje wskazują na konieczność zastosowania międzynarodowych i krajowych norm ISO, jednakże każda z regulacji wskazuje inny ich zbiór, nie pokrywający się, co generuje niespójność rozwiązań bezpieczeństwa teleinformatycznego podmiotów systemu cyberbezpieczeństwa. Przedstawiono w ujęciu porównawczym, w formie tabelarycznej i opisowej zestawienie norm i standardów bezpieczeństwa systemów teleinformatycznych zalecanych lub wymaganych do wdrożenia przez podmioty objęte regulacjami systemów bezpieczeństwa – zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych.

Przeprowadzono badania własne autora w zakresie doboru rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego, czyli norm, metodyk

i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa i dokonano ich analizy. Wyniki badania wykazały, że aktualnie wymagane metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych nie są właściwie zdefiniowane, uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań i uzyskanych opinii od respondentów sformułowana została koncepcja wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP, wskazująca konieczność ujednolicenia, zapewnienia uznanego wzorca odniesienia i porównywalnego poziomu bezpieczeństwa oraz wskazująca zbiór i zakres wymaganych norm ISO. Koncepcja adresuje wyniki i wnioski z badania oraz jest oparta na hipotezie badawczej. Opracowano tabelaryczne zestawienie porównawcze aktualnie obowiązujących wykazów norm rozwiązań bezpieczeństwa systemów teleinformatycznych wskazanych regulacjami przepisów prawa systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych z opracowanym w ramach koncepcji wykazem norm ISO bezpieczeństwa systemów teleinformatycznych dla podmiotów systemu cyberbezpieczeństwa RP.

W wyniku przeprowadzonego procesu badawczego sformułowana hipoteza pomocnicza została pozytywnie zweryfikowana.

W ramach realizacji celu głównego rozprawy, którym jest: *opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa,* w ramach niniejszego rozdziału został zrealizowany cel szczegółowy rozprawy: *opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.*

Na podstawie przyjętej, pozytywnie zweryfikowanej hipotezy, wyników badań, sformułowanych konkluzji i wniosków opracowano koncepcję wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP. Zaproponowane w ramach koncepcji rozwiązanie zapewnia zgodność z wykładnią przepisów prawa oraz wynikami przeprowadzonego badania. Przyjęty cel szczegółowy został osiągnięty, przez co przyczynił się do osiągnięcia celu głównego rozprawy.

PODSUMOWANIE

Przedmiotem badań rozprawy jest organizacja systemu cyberbezpieczeństwa RP zdefiniowana przez regulacje prawne i dokumenty strategiczne bezpieczeństwa państwa, w zakresie: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem, doboru sektorów i typów podmiotów oraz wskazania norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. Przeprowadzony proces badawczy jest próbą kompleksowego spojrzenia na zagadnienia organizacji systemu cyberbezpieczeństwa państwa, odniesionego do zakresu przedmiotu badań. W rozprawie dokonano próby rozstrzygnięcia problemów badawczych (głównego i szczegółowych) dotyczących wybranych rozwiązań organizacji systemu cyberbezpieczeństwa Polski, określonych jako przedmiot badań, poprzez sformułowanie hipotez (głównej i pomocniczych) i poddanie ich weryfikacji i falsyfikacji w przeprowadzonym przez autora procesie badawczym.

Główny problem badawczy został sformułowany w następujący sposób:

Czy organizacja systemu cyberbezpieczeństwa RP zapewnia odpowiedni poziom bezpieczeństwa państwa i jakie są możliwości poprawy organizacji tego systemu dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa?

Główny problem badawczy został rozwinięty w formie problemów szczegółowych.

W odpowiedzi na postawiony problem sformułowano hipotezę główną, brzmiącą:

Organizacja systemu cyberbezpieczeństwa RP nie jest optymalnie zdefiniowana, co w praktyce przyczynia się do braku skoordynowanych zadań różnych organów państwa. Obecnie obowiązujące rozwiązania podsystemów bezpieczeństwa są niekompletne, niespójne, niejednorodne i rozdzielne, i nie mogą tym samym zapewnić odpowiedniego poziomu bezpieczeństwa państwa, a ich ujednolicenie, zharmonizowanie i usprawnienie może przyczynić się do poprawy efektywności systemu cyberbezpieczeństwa RP i tym samym zwiększenia poziomu bezpieczeństwa państwa

oraz wynikające z niej hipotezy pomocnicze, które w toku procesu badawczego zostały poddane weryfikacji i falsyfikacji. Hipotezy pomocnicze i hipoteza główna zostały pozytywnie

zweryfikowane w toku przeprowadzonego procesu badawczego, w wyniku czego zostały przeprowadzone stosowne działania i opracowane koncepcyjne rozwiązania organizacji systemu cyberbezpieczeństwa RP, realizujące poszczególne cele szczątkowe i cel główny rozprawy.

W przeprowadzonym procesie badawczym sformułowane problemy badawcze – główny i szczegółowe zostały poddane weryfikacji i falsyfikacji poprzez weryfikację i falsyfikację przyjętych hipotez głównej i pomocniczych. W tym celu przeprowadzono kompleksowy, metodologiczny proces badawczy, w ramach którego przeprowadzono rozważania nad istotą i pojęciami bezpieczeństwa narodowego i cyberbezpieczeństwa, dokonano analizy aktualnego stanu bezpieczeństwa polskiej cyberprzestrzeni, dokonano także analizy regulacji prawnych i dokumentów strategicznych bezpieczeństwa państwa w kontekście cyberbezpieczeństwa oraz dokonano przeglądu rozwiązań organizacji systemu cyberbezpieczeństwa RP w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych, zgodnie z zakresem problemowym, zdefiniowanym jako przedmiot badań, tzn. zagadnień: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa oraz dokonano ich analizy porównawczej. W celu rozstrzygnięcia problemów badawczych i weryfikacji odpowiadających im hipotez odnoszących się bezpośrednio do rozwiązań organizacyjnych systemu cyberbezpieczeństwa RP, autor przeprowadził badania własne w formie wywiadu eksperckiego z zastosowaniem standaryzowanego arkusza wywiadu eksperckiego opartego na pytaniach uszczegóławiających i rozwijających sformułowane w rozprawie problemy i hipotezy badawcze. W każdym rozdziale rozprawy, dedykowanym problemowemu zagadnieniu przedstawiono wyniki przeprowadzonych badań i dokonano ich szczegółowej analizy. W wyniku przeprowadzonego procesu badawczego wszystkie sformułowane hipotezy pomocnicze zostały pozytywnie zweryfikowane, co jednocześnie pozytywnie weryfikuje hipotezę główną rozprawy. Na podstawie pozytywnie zweryfikowanych hipotez, wyników badań i sformułowanych wniosków z badań opracowano szereg koncepcji szczegółowych rozwiązań doskonalących organizację systemu cyberbezpieczeństwa RP, realizujących przyjęte cele szczegółowe rozprawy.

W rozdziale drugim rozprawy dokonano próby rozstrzygnięcia problemu badawczego: *Jakie są aktualne kontekst, warunki i środowisko prawne, strategiczne i normatywno-*

standaryzacyjne systemu cyberbezpieczeństwa RP i czy ich rozpoznanie umożliwi opracowanie koncepcji doskonalenia systemu cyberbezpieczeństwa RP? poprzez weryfikację hipotezy pomocniczej: *Rozpoznanie aktualnych kontekstu, warunków i środowiska prawnego, strategicznego i normatywno-standaryzacyjnego systemu cyberbezpieczeństwa umożliwi opracowanie koncepcji doskonalenia rozwiązań organizacji systemu cyberbezpieczeństwa RP i zapewni jego efektywność i odpowiedni poziom bezpieczeństwa państwa.* Zostały przeprowadzone rozważania nad istotą i pojęciami bezpieczeństwa narodowego oraz współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą w bezpieczeństwie narodowym. Omówiono i przedstawiono pojęcia, istotę i definicje bezpieczeństwa w ujęciu bezpieczeństwa narodowego, bezpieczeństwa państwa, bezpieczeństwa międzynarodowego, bezpieczeństwa wewnętrznego, podając różne definicje, ujęcia, rodzaje i konteksty bezpieczeństwa. Poruszono zagadnienie bezpieczeństwa w zależności od polityki bezpieczeństwa państwa i strategii bezpieczeństwa oraz jako zależne od i funkcjonujące w ramach środowiska bezpieczeństwa i jego szczególnej formy – strategicznego środowiska bezpieczeństwa. Podniesiono zapewnianie bezpieczeństwa państwa w ramach i przez system bezpieczeństwa narodowego. Omówiono strukturę system bezpieczeństwa i jego składowe komponenty oraz zakres obejmowanych dziedzin na podstawie literatury przedmiotu oraz treści sformułowanych w dokumentach strategicznych bezpieczeństwa Polski. Przedstawiono bezpieczeństwo narodowe w ujęciu koncepcji sektorów bezpieczeństwa, przedstawiając sektory bezpieczeństwa i transsektorowe obszary bezpieczeństwa. Przedstawiono i omówiono pojęcia, istotę i definicje cyberbezpieczeństwa i zagadnień z nim związanych, scharakteryzowano wymiar, zakres i skalę oddziaływania cyberbezpieczeństwa na bezpieczeństwo narodowe zawarte w literaturze, normach i w dokumentach strategicznych bezpieczeństwa Polski. Przywołano powiązania cyberbepieczeństwa z bezpieczeństwem teleinformatycznym i informacyjnym oraz jego transsektorowy charakter w bezpieczeństwie państwa. Autor przedstawił własne pojmowanie i charakterystykę cyberbezpieczeństwa i cyberprzestrzeni oraz ich powiązań i zależności z bezpieczeństwem teleinformatycznym. Przedstawiono wyzwania, zagrożenia i incydenty cyberbezpieczeństwa w kontekście rozwoju i powszechnego wykorzystywania technologii i systemów teleinformatycznych w ujęciu zagadnień teoretycznych oraz działań i zdarzeń faktycznych. Szeroko scharakteryzowano cyberzagrożenia, przedstawiono występujące cyberataki, omówiono i scharakteryzowano działania o charakterze agresywnym podejmowane w cyberprzestrzeni, takie jak cyberwalka i cyberwojna. Przedstawiono i omówiono stan bezpieczeństwa polskiej cyberprzestrzeni i działania w tym zakresie dedykowanych organów. Przedstawiono i omówiono w kilkuletnim przedziale czasowym skalę

i trendy występowania incydentów, ich typy, atakowane sektory i typy instytucji wskazano zagraniczne kierunki, z których wrogie działania są prowadzone. Przeprowadzono rekonstrukcję regulacji prawnych i strategicznych dokumentów normatywnych i ich analizę w zakresie zagadnień systemu cyberbezpieczeństwa oraz omówiono szereg norm, metodyk i standardów zarządzania bezpieczeństwem informacji i bezpieczeństwa systemów teleinformatycznych. Omówiono zagadnienia cyberbezpieczeństwa ujęte w dokumentach strategicznych bezpieczeństwa państwa. Przedstawiono podejście do cyberbezpieczeństwa, strategiczne cele bezpieczeństwa państwa i cele cyberbezpieczeństwa oraz działania, programy i strategie ich realizacji. Wskazano ich powiązania z problematyką podjętą w niniejszej rozprawie. Przedstawiono i omówiono ujęcie problematyki cyberbezpieczeństwa, systemu cyberbezpieczeństwa i działań w tym zakresie w dedykowanych tym zagadnieniom i zagadnieniom pokrewnym regulacjach prawnych. Scharakteryzowano zagadnienia cyberbezpieczeństwa w kontekście podjętych problemów badawczych. Przedstawiono i omówiono normy, standardy i metodyki zarządzania bezpieczeństwem informacji, systemów teleinformatycznych i zarządzania systemami teleinformatycznymi, takie jak normy ISO, NIST, Narodowe Standardy Bezpieczeństwa i inne standardy branżowe.

Zgromadzenie i poddanie analizie zebranego materiału pozwoliło na zrealizowanie celu szczegółowego rozprawy: *Przybliżenie kontekstu, warunków i środowiska systemu cyberbezpieczeństwa RP, poprzez przedstawienie istoty i roli cyberbezpieczeństwa w systemie bezpieczeństwa narodowego, zrekonstruowanie obowiązujących przepisów prawnych i strategicznych dokumentów normatywnych w sposób formalny definiujących organizację systemu cyberbezpieczeństwa RP oraz poprzez rozpoznanie międzynarodowych i krajowych norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych, możliwych do zastosowania w systemie cyberbezpieczeństwa RP*.

Przedstawienie ww. informacji stanowi realizację celu poznawczego rozprawy. Cel poznawczy jest również realizowany w rozdziałach trzecim, czwartym, piątym i szóstym, gdzie przeprowadzone zostało dalsze przybliżanie przedmiotowego zakresu informacyjnego w kontekście i w odniesieniu do podejmowanych szczegółowych celów, problemów i hipotez badawczych. Cel poznawczy jest realizowany także poprzez przedstawienie stanowisk i opinii ekspertów, będących respondentami badania, w wyżej zdefiniowanym zakresie. Pozyskane informacje stanowią gruntowną bazę umożliwiają opracowanie koncepcji doskonalenia rozwiązań organizacji systemu cyberbezpieczeństwa RP.

W rozdziałach trzecim, czwartym, piątym i szóstym przeprowadzono dalsze działania procesu badawczego, dotyczące zagadnień odnoszących się bezpośrednio do rozwiązań

organizacyjnych systemu cyberbezpieczeństwa RP, tzn. zagadnień: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, zdefiniowanych przez kształtujące system cyberbezpieczeństwa dokumenty strategiczne i stosowne regulacje prawne dotyczące zarządzania kryzysowego – tworzące system zarządzania kryzysowego, dotyczące krajowego systemu cyberbezpieczeństwa – tworzące krajowy system cyberbezpieczeństwa i dotyczące informatyzacji podmiotów realizujących zadania publiczne – tworzące system informatyzacji podmiotów publicznych.

W zakresie rozpoznania i diagnozy aktualnych rozwiązań organizacyjnych systemu cyberbezpieczeństwa Polski dokonano ich przeglądu i analizy w kontekście zdefiniowanych pytań badawczych, celów i hipotez podejmowanych w każdym z rozdziałów - trzecim, czwartym, piątym i szóstym.

W rozdziale trzecim przedstawiono i omówiono rozwiązania organizacji (zorganizowania) zarządzania cyberbezpieczeństwem na poziomie krajowym w zakresie struktury procesów i dokumentów planistycznych i wykonawczych w ujęciu regulacji prawnych dwóch systemów bezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Dokonano analizy porównawczej tych rozwiązań w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego posiada kompleksowe rozwiązanie planistyczne i zarządcze w zakresie zarządzania bezpieczeństwem, w tym cyberbezpieczeństwem, na poziomie krajowym, w ramach którego została zbudowana struktura odpowiedzialności i struktura dokumentów zarządczych poziomu krajowego oraz, że krajowy system cyberbezpieczeństwa nie posiada wyrażonego w procesach i powiązanych dokumentach rozwiązania planowania i zarządzania cyberbezpieczeństwem na poziomie krajowym, natomiast koncentruje się na zapewnieniu operacyjnego, funkcjonalnego bezpieczeństwa systemów teleinformatycznych podmiotów tego systemu oraz na ustanowieniu rozwiązań zarządzania incydentami cyberbezpieczeństwa.

W rozdziale czwartym przedstawiono i omówiono zorganizowanie struktur i relacji operacyjnych zarządzania w systemie cyberbezpieczeństwa na poziomie krajowym w zakresie całościowych zaangażowanych struktur i relacji operacyjnych oraz struktur i relacji zarządzania bezpieczeństwem na poziomie krajowym, i struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa w ujęciu dokumentów strategicz-

nych i właściwych regulacji prawnych dwóch systemów bezpieczeństwa – systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa. Dla każdego z systemów – zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa: zidentyfikowano zaangażowane organy i podmioty struktur operacyjnych oraz opracowano dedykowane tym strukturom autorskie modele relacji, zidentyfikowano organy i podmioty struktur zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym oraz opracowano dedykowane nim mapowanie tych struktur na aktualne dokumenty procesów organizacji zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego, zidentyfikowano organy i podmioty struktur zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa oraz opracowano dedykowane tym strukturom autorskie modele relacji. Dokonano analizy porównawczej rozwiązań struktur i relacji zarządzania na poziomie krajowym oraz zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego ustanawia struktury i ich relacje - m.in. organy i instytucje, odpowiedzialne za realizację procesów i dokumentacji planowania i zarządzania bezpieczeństwem na poziomie krajowym oraz za zarządzanie sytuacjami kryzysowymi, w tym wynikającymi z incydentów cyberbezpieczeństwa oraz, że krajowy system cyberbezpieczeństwa, w związku z tym, że nie definiuje zagadnień zarządzania cyberbezpieczeństwem na poziomie krajowym w odniesieniu do procesów i dokumentów zarządczych (co zostało wywiedzione w rozdziale 2 i 3), nie ustanawia takich struktur i relacji zarządzania, natomiast ustanawia dedykowane struktury odpowiedzialnych organów i instytucji, i ich relacje w zakresie zarządzania incydentami cyberbezpieczeństwa. Przedstawiono w ujęciu porównawczym struktury i relacje operacyjne organów i podmiotów zarządzania bezpieczeństwem w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa. Przedstawiono w ujęciu porównawczym obu systemów bezpieczeństwa struktury i relacje organów i podmiotów zarządzania cyberbezpieczeństwem na poziomie krajowym wraz z mapowaniem tych struktur na dokumenty procesów zarządzania bezpieczeństwem i cyberbezpieczeństwem na poziomie krajowym. Przedstawiono także w ujęciu porównawczym struktury i relacje organów i podmiotów zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa każdego z systemów.

W rozdziale piątym przedstawiono i omówiono zagadnienia doboru sektorów i typów podmiotów objętych systemem cyberbezpieczeństwa państwa w ujęciu regulacji prawnych trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji

podmiotów publicznych. Dokonano analizy porównawczej wykazu podmiotów objętych ww. regulacjami w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego obejmuje podmioty zdefiniowane jako operatorzy infrastruktury krytycznej wskazywane w ramach zdefiniowanych 11 systemów, krajowy system cyberbezpieczeństwa obejmuje podmioty zdefiniowane jako operatorzy usług kluczowych, dostawcy usług cyfrowych, wybrane typy podmiotów publicznych i podmioty świadczące usługi w zakresie cyberbezpieczeństwa wskazywane w ramach zdefiniowanych 9 sektorów, natomiast system informatyzacji podmiotów publicznych obejmuje wybrane typy podmiotów publicznych z sektora publicznego. Typy podmiotów włączone do podsystemów bezpieczeństwa w ramach systemów i sektorów tylko częściowo się pokrywają, są niespójne, nie są ze sobą powiązane i zintegrowane. Jedynie podmioty sektora publicznego objęte są każdym z systemów, ale w innym zakresie, tak, że tylko częściowo się pokrywają. Przedstawiono w ujęciu porównawczym, w formie tabelarycznej i opisowej zestawienie podmiotów oraz zestawienie systemów i sektorów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów publicznych.

W rozdziale szóstym przedstawiono i omówiono zagadnienia doboru norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa w ujęciu regulacji prawnych trzech systemów bezpieczeństwa analizowanych w niniejszej rozprawie – systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych. Dokonano analizy porównawczej wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów objętych ww. regulacjami w formie opisowej i tabelarycznej, wykazując, że system zarządzania kryzysowego wskazuje, jako zalecenie czy sugestię, obszerną listę alternatywnych względem siebie branżowych norm międzynarodowych i krajowych, krajowy system cyberbezpieczeństwa wymaga wdrożenia bezpieczeństwa w oparciu o 2 normy ISO przez wybrane typy podmiotów, natomiast system informatyzacji podmiotów publicznych wymaga wdrożenia zarządzania systemami teleinformatycznymi i ich bezpieczeństwem w oparciu o 5 norm ISO przez podmioty publiczne. Poszczególne regulacje wskazują na konieczność zastosowania międzynarodowych i krajowych norm ISO, jednakże każda z regulacji wskazuje inny ich zbiór, nie pokrywający się, co generuje niespójność rozwiązań bezpieczeństwa teleinformatycznego podmiotów systemu cyberbezpieczeństwa. Przedstawiono w ujęciu porównawczym, w formie tabelarycznej i opisowej zestawienie norm i standardów bezpieczeństwa systemów teleinformatycz-

nych zalecanych lub wymaganych do wdrożenia przez podmioty objęte regulacjami systemów bezpieczeństwa – zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych.

W wyniku przeprowadzonych rozpoznania, analiz i diagnozy aktualnych rozwiązań organizacyjnych krajowego systemu cyberbezpieczeństwa Polski i ich zagregowania można przedstawić jego aktualną strukturę w odniesieniu do poszczególnych zagadnień problemowych rozprawy, tzn. zagadnień: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Aktualna struktura krajowego systemu cyberbezpieczeństwa RP w zakresie zagadnień problemowych rozprawy została przedstawiona w tabeli 50.

Tabela 50. Struktura krajowego systemu cyberbezpieczeństwa RP w zakresie zagadnień problemowych rozprawy

Struktura krajowego systemu cyberbezpieczeństwa RP w zakresie zagadnień problemowych rozprawy					
Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym	**Struktury i relacje operacyjne zarządzania systemu cyberbezpieczeństwa**			**Sektory krajowego systemu cyberbezpieczeństwa**	**Normy zarządzania bezpieczeństwem systemów teleinformatycznych**
	Zarządzanie cyberbezpieczeństwem na poziomie krajowym	**Zarządzanie incydentami cyberbezpieczeństwa**	**Struktury operacyjne (całkowite)**		
-	-	Zespół ds. Incydentów Krytycznych	Zespół ds. Incydentów Krytycznych	Energia	ISO 27001
		Pełnomocnik Rządu ds. Cyberbezpieczeństwa	Pełnomocnik Rządu ds. Cyberbezpieczeństwa	Transport	ISO 22301
		Pojedynczy Punkt Kontaktowy	Pojedynczy Punkt Kontaktowy	Bankowość i infrastruktury rynków finansowych	
		Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Ochrona zdrowia	
		Rządowe Centrum Bezpieczeństwa (RCB)	Rządowe Centrum Bezpieczeństwa (RCB)	Zaopatrzenie w wodę pitną i jej dystrybucja	
		Organ właściwy ds. cyberbezpieczeństwa Minister właściwy ds. informatyzacji Minister obrony narodowej MON	Organ właściwy ds. cyberbezpieczeństwa Minister właściwy ds. informatyzacji Minister obrony narodowej MON	Infrastruktura cyfrowa	
		CSIRT MON, CSIRT NASK, CSIRT GOV	CSIRT MON, CSIRT NASK, CSIRT GOV	Usługi cyfrowe	
		Sektorowy zespół cyberbezpieczeństwa	Sektorowy zespół cyberbezpieczeństwa	Podmioty publiczne (finansów publicznych, użyteczności publicznej) i urzędy centralne - wybrane	

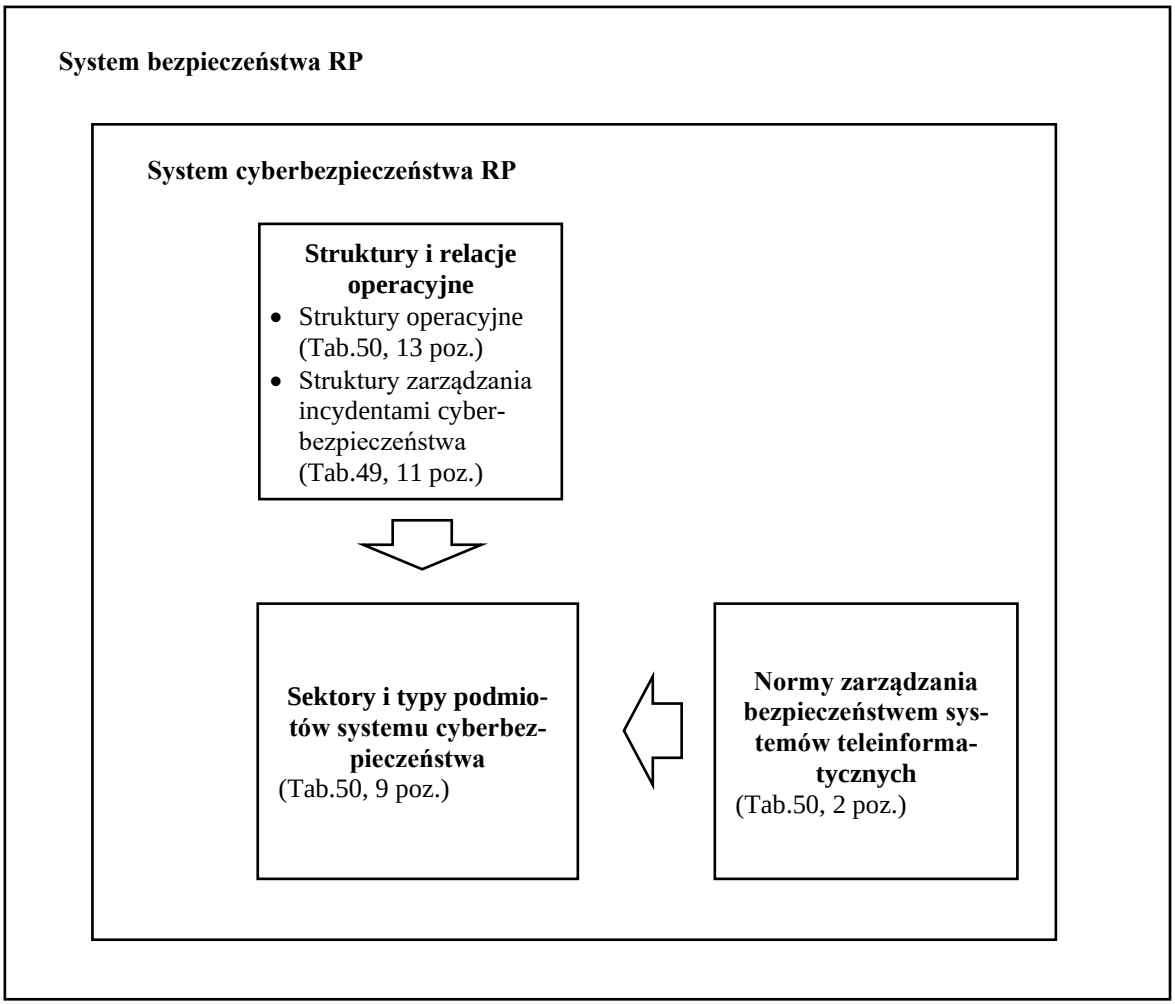
		Szef Agencji Bezpieczeństwa Wewnętrznego	*Szef Agencji Bezpieczeństwa Wewnętrznego*	Usługi cyberbezpieczeństwa	
		Podmiot świadczący usługi z zakresu cyberbezpieczeństwa	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa		
		Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny	Operator usługi kluczowej Dostawca usługi cyfrowej Podmiot publiczny		
			Kolegium do Spraw Cyberbezpieczeństwa		
			Narodowy Punkt Kontaktowy do współpracy z NATO		

Źródło: opracowanie własne na podstawie wyników badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.; Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Rozporządzenie w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

Na podstawie przeprowadzonych rozpoznania, analiz i diagnozy aktualnych rozwiązań organizacyjnych krajowego systemu cyberbezpieczeństwa i jego odwzorowanej struktury w odniesieniu do poszczególnych zagadnień zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa można przedstawić jego aktualny model w ujęciu komponentowym i relacyjnym.

Aktualny model krajowego systemu cyberbezpieczeństwa RP w zakresie zagadnień problemowych rozprawy w ujęciu komponentowym i relacyjnym przedstawia rys. 37.

Rys. 37. Model krajowego systemu cyberbezpieczeństwa RP



Źródło: opracowanie własne na podstawie wyników badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Model aktualnego stanu krajowego systemu cyberbezpieczeństwa przedstawia w ujęciu komponentowym i relacyjnym ulokowany w ramach systemu bezpieczeństwa kraju system cyberbezpieczeństwa, składający się z trzech komponentów: struktury i relacje operacyjne, sektory i typy podmiotów systemu cyberbezpieczeństwa i normy zarządzania bezpieczeństwem systemów teleinformatycznych. W systemie cyberbezpieczeństwa nie zawiera komponentu zarządzanie cyberbezpieczeństwem na poziomie krajowym.

W zakresie realizacji celu rozprawy ***opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa***, w rozdziałach trzecim, czwartym, piątym i szóstym przeprowadzono dla każdego zagadnienia problemowego oraz dedykowanych im szczątkowych celów, pytań i hipotez badawczych realizację metodycznych procesów badawczych, w ramach których pozyskano informacje o stanowiskach respondentów w przedmiotowych kwestiach, dokonano ich oceny i analizy oraz wnioskowania, w wyniku których opracowano koncepcje cząstkowe, jako realizację zdefiniowanych celów cząstkowych, składających się na osiągnięcie celu głównego rozprawy.

W rozdziale trzecim w ramach realizacji celu ***opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym*** przeprowadzono badania własne autora w tym zakresie i dokonano ich analizy. Wyniki badania wykazały, że aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowy nie jest **właściwie** zdefiniowana. Uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań, na podstawie uzyskanych wyników i wniosków z badań oraz opinii respondentów opracowano koncepcję rozwiązania uwzględniającą pozytywną weryfikację hipotezy pomocniczej: *ujednolicenie i zharmonizowanie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami określonymi w systemie zarządzania kryzysowego zapewnieni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa*. Sformułowana koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym wskazuje wytyczne dla jego struktury i dedykowane krajowemu cyberbezpieczeństwu dokumenty zarządcze. W ramach realizacji celu szczątkowego powstała koncepcja oparta na hipotezie badawczej, przedstawiająca się następująco:

Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania

kryzysowego (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej, i powinna funkcjonować równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo być z nim połączona.

Organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym powinna obejmować funkcjonującą równolegle, dedykowaną, tożsamą strukturę procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP (SCRP), jak w systemie zarządzania kryzysowego, punktowo/problemowo wzajemnie powiązanych i odwołujących się do siebie. System cyberbezpieczeństwa RP (SCRP) powinien obejmować dedykowane i skoncentrowane na kwestiach cyberbezpieczeństwa procesy oraz dokumenty zarządcze poziomu krajowego, jako odpowiedniki dokumentów systemu zarządzania kryzysowego, np.: **Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC)**, ministerialne, sektorowe i regionalne **Plany Zarządzania Cyberbezpieczeństwem (PZC)**, **Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT)** oraz **Raport o zagrożeniach cyberbezpieczeństwa** (opcjonalnie może być wykorzystywany aktualnie opracowywany **Raport o zagrożeniach bezpieczeństwa narodowego** w części dotyczącej zagrożeń cyberbezpieczeństwa).

Opracowana koncepcja zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym stanowi nowum pracy, wypełnia zdiagnozowaną lukę i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwej struktury procesów i dokumentów zarządczych systemu cyberbezpieczeństwa RP zsynchronizowanych z i wzorowanych na systemie zarządzania kryzysowego, jednakże odnoszących się do cyberbezpieczeństwa. Implementacja sformułowanej koncepcji w porządku prawnym, w dokumentach strategicznych i operacyjnych bezpieczeństwa pozwoli zarządzać cyberbezpieczeństwem kraju i zapewnić efektywność systemu cyberbezpieczeństwa RP i przez to odpowiedni poziom bezpieczeństwa państwa. Aktualnie funkcjonujący krajowy system cyberbezpieczeństwa nie posiada żadnych procesów i dokumentów planowania i zarządzania cyberbebezpieczeństwem na poziomie krajowym i niższych poziomach

strukturalnych i sektorowych, w przeciwieństwie do systemu zarządzania kryzysowego, dobrze zorganizowanego w tym zakresie.

Opracowano tabelaryczne zestawienie porównawcze dotychczasowych rozwiązań organizacji zarządzania cyberbezpieczeństwem i struktury dokumentów zarządczych na poziomie krajowym w systemie zarządzania kryzysowego (SZK) i krajowym systemie cyberbezpieczeństwa (KSC) oraz koncepcji zorganizowania zarządzania cyberbezpieczeństwem systemu cyberbezpieczeństwa RP (SCRP).

Opracowana na podstawie wskazania wyników badania koncepcja zorganizowania zarządzania cyberbezpieczeństwem RP na poziomie krajowym spełnia założenia przyjętej hipotezy i sformułowane wnioski z badania oraz realizuje cel szczegółowy rozprawy.

W rozdziale czwartym w ramach realizacji celu ***opracowanie koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym*** przeprowadzono badania własne autora w tym zakresie i dokonano ich analizy. Wyniki badania wykazały, że aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem na poziomie krajowym, w tym struktury i relacje operacyjne całościowe, zarządzania systemem i zarządzania incydentami cyberbezpieczeństwa na poziomie krajowy nie są właściwie zdefiniowane. Uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonego procesu badawczego opracowano koncepcję rozwiązania uwzględniającą wyniki i wnioski z badania oraz opinie respondentów pozytywnie weryfikujące hipotezę pomocniczą: *ujednolicenie i zharmonizowanie struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa zapewni efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa.* W ramach rozwiązania powstało trzy cząstkowe rozwiązania koncepcyjne, adresujące odpowiednio zagadnienia organizacji przedmiotowych struktur i relacji systemu cyberbezpieczeństwa RP w zakresie operacyjnym całego systemu oraz wynikających z niej struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym oraz struktur i relacji zarządzania incydentami cyberbezpieczeństwa. Na koncepcję zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym składają się koncepcje cząstkowe, definiujące wytyczne organizacyjne oraz zakres angażowanych organów i podmiotów, które zostały zdefiniowane następująco dla każdego zagadnienia:

1. koncepcja zorganizowania **struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP**, w ramach której:

Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP powinny obejmować zagregowaną listę podmiotów występujących, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

Dla sformułowanej koncepcji zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP opracowano autorski model relacji oraz zestawienie porównawcze z obecnymi strukturami systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

2. koncepcja zorganizowania **struktur i relacji z zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP**, w ramach której:

Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Struktury i relacje zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP powinny obejmować zagregowaną listę podmiotów realizujących procesy i dokumenty zarządcze, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

Dla sformułowanej koncepcji zorganizowania struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP opracowano autorski model relacji, zestawienie porównawcze z obecnymi strukturami obu systemów bezpieczeństwa, opracowano także dedykowane mapowanie tych struktur na koncepcyjną strukturę dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym (wypracowaną w ramach rozdziału 3).

3. koncepcja zorganizowania **struktur i relacji zarządzania incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP**, w ramach której:

Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa na poziomie krajowym systemu cyberbezpieczeństwa RP powinny być ujednolicone i zharmonizowane poprzez zintegrowanie struktur i relacji zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa oraz poprzez m.in. rozszerzenie kompetencji i struktur RCB tj. ulokowanie funkcji i kompetencji przypisanych organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa oraz zapewnienie wiodącej roli i pełnej odpowiedzialności za szeroko zdefiniowane zintegrowane zarządzanie bezpieczeństwem krajowym, w tym zarządzanie kryzysowe i cyberbezpieczeństwo, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Kolegium ds. Cyberbezpieczeństwa i CSIRTy poziomu krajowego. Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami. CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych. Struktury i relacje zarządzania sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP (SCRP) powinny obejmować zagregowaną listę podmiotów realizujących zarządzanie sytuacjami kryzysowymi i incydentami cyberbezpieczeństwa, zarówno w systemie zarządzania kryzysowego, jak i w krajowym systemie cyberbezpieczeństwa.

Opracowana koncepcja zorganizowania struktur i relacji zarządzania cyberbezpieczeństwem na poziomie krajowym stanowi nowum pracy, wypełnia zdiagnozowaną lukę i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwych struktur i relacji operacyjnych.

W zakresie zorganizowania struktur i relacji z zarządzania cyberbezpieczeństwem na poziomie krajowym systemu cyberbezpieczeństwa RP zaproponowano strukturę operacyjną, mogącą realizować procesy i dokumenty zarządcze systemu cyberbezpieczeństwa RP. Aktualnie funkcjonujący krajowy system cyberbezpieczeństwa nie posiada żadnych procesów i dokumentów planowania i zarządzania cyberbebezpieczeństwem na poziomie krajowym, ani żadnych struktur zarządczych, które wypełniałyby takie zadania.

W zakresie zorganizowania struktur i relacji z zarządzania incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP, zaproponowano znaczne rozszerzenie zaangażowanych podmiotów, organów i instytucji względem aktualnie zdefiniowanego zakresu w Ustawie KSC oraz włączenie i zintegrowanie podmiotów systemu zarządzania kryzysowego, dla zapewnienia większej efektywności komunikowania i obsługi incydentów, a przez to zwiększenie poziomu bezpieczeństwa.

Struktury i relacje operacyjne systemu cyberbezpieczeństwa RP skonstruowane są jako łączny zbiór wszystkich aktualnych i nowych podmiotów systemu cyberbezpieczeństwa, zdefiniowanych w koncepcjach struktur zarządzania cyberbezpieczeństwem na poziomie krajowym i zarządzania incydentami cyberbezpieczeństwa, oraz struktur systemu zarządzania kryzysowego, włączonych do realizacji zadań z zakresu cyberbezpieczeństwa.

Dla sformułowanej koncepcji zorganizowania struktur i relacji zarządzania incydentami cyberbezpieczeństwa na poziomie krajowym opracowano autorski model relacji oraz zestawienie porównawcze z obecnymi strukturami systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

Podejście, w ramach którego wypracowano trzy koncepcje cząstkowe struktur i relacje operacyjnych zarządzania systemem cyberbezpieczeństwa na poziomie krajowym, definiujące wytyczne organizacyjne oraz zakres angażowanych organów i podmiotów jest zgodne z zakresem przeprowadzonej analizy zorganizowania struktur i relacji operacyjnych w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa. Opracowane rozwiązania koncepcji struktur i relacji operacyjnych oraz wywodzące się z niej koncepcje struktur i relacji z zarządzania cyberbezpieczeństwem na poziomie krajowym oraz struktur i relacji zarządzania incydentami cyberbezpieczeństwa systemu cyberbezpieczeństwa RP spełniają sformułowane wnioski z badania i realizują cel szczegółowy rozprawy.

W rozdziale piątym w ramach realizacji celu ***opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP*** przeprowadzono badania własne autora w zakresie doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa i dokonano ich analizy. Wyniki badania wykazały, że aktualna organizacja struktur i relacji operacyjnych w zakresie zarządzania cyberbezpieczeństwem i zarządzania incydentami cyberbezpieczeństwa na poziomie krajowy nie jest właściwie zdefiniowana, uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. Uzyskano informacje i stanowiska respondentów dotyczące rozważanych w badaniu rozwiązań, wskazujące kształt możliwych przyszłych rozwiązań w tym zakresie. W wyniku przeprowadzonych badań, na podstawie uzyskanych wyników i wniosków z badań oraz opinii respondentów opracowano koncepcję rozwiązania uwzględniającą pozytywnie zweryfikowaną hipotezę pomocniczą: *objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego zapewni efektywność tego systemu i odpowiedni poziom bezpieczeństwa państwa*. Koncepcja wskazuje zakres sektorów i typów podmiotów koniecznych do objęcia tym systemem. Została zdefiniowana następująco:

System cyberbezpieczeństwa RP powinien obejmować wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego, a mianowicie: energetyka, łączność (usługi pocztowe i kurierskie), telekomunikacja i sieci teleinformatyczne, bankowość i infrastruktura rynków finansowych, sektor żywnościowy i rolniczy, wodociągi i kanalizacja, ochrona zdrowia, transport, ratownictwo, sektor chemiczny, przemysł/produkcja, handel, administracja publiczna (rządowa i samorządowa) – wszystkie jednostki, instytucje urzędów centralnych, sektor finansów publicznych, sektor usług komunalnych, sektor usług publicznych, sektor kosmiczny, nauka i szkolnictwo wyższe, instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe), media (TV, radio, portale informacyjne), infrastruktura cyfrowa (DNS, IXP, TLD), usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej), usługi cyfrowe

(platformy poczty elektronicznej, portale społecznościowe, itp.), środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach, dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja), dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa, wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego lub usług kluczowych oraz uczestniczące w łańcuchu dostaw dla nich.

Opracowana koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP stanowi nowum pracy, wypełnia zdiagnozowaną lukę i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwego wykazu sektorów i typów podmiotów. W ramach koncepcji zaproponowano znaczne rozszerzenie sektorów i typów podmiotów w stosunku do aktualnie zdefiniowanego. Wg koncepcji system cyberbezpieczeństwa RP powinien obejmować wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego. Implementacja tak sformułowanej koncepcji objęłaby systemem cyberbezpieczeństwa wielokrotnie więcej podmiotów, a przez to przyczyniłaby się do zwiększenia poziomu cyberbezpieczeństwa i bezpieczeństwa państwa.

Dla sformułowanej koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa opracowano tabelaryczne zestawienie porównawcze dotychczasowych sektorów i systemów objętych regulacjami zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa, systemu informatyzacji podmiotów publicznych z koncepcyjnym wykazem sektorów i typów podmiotów systemu cyberbezpieczeństwa RP.

Opracowana koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa jest oparta na wynikach i wnioskach z przeprowadzonego badania i opinii respondentów. Realizuje cel szczegółowy rozprawy.

W rozdziale szóstym w ramach realizacji celu ***opracowanie koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP***, w wyniku przeprowadzonego procesu badawczego opracowano koncepcję rozwiązania uwzględniającą wyniki i wnioski z badania oraz

opinie respondentów pozytywnie weryfikujące hipotezę pomocniczą: *ujednolicenie i zharmonizowanie wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych zapewni podobny i porównywalny w skali kraju poziom odporności i bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa*. Opracowana koncepcja rozwiązania wskazuje konieczność ujednolicenia, zapewnienia uznanego wzorca odniesienia i porównywalnego poziomu bezpieczeństwa oraz wskazuje zbiór i zakres wymaganych norm ISO. Koncepcja stanowi:

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa i powinny być oparte o szeroki katalog norm ISO dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301.

Opracowana koncepcja wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP stanowi nowum pracy, wypełnia zdiagnozowaną lukę i dysfunkcyjność krajowego systemu cyberbezpieczenstwa poprzez zdefiniowanie konieczności ustanowienia właściwego wykazu odpowiednich norm bezpieczeństwa teleinformatycznego. W ramach koncepcji zaproponowano znaczne rozszerzenie norm mających być zastosowanymi do wdrożenia rozwiązań zarządczych, organizacyjnych i technicznych bezpieczeństwa teleinformatycznego, zawierające normy zarządzania, jak i szeroki zestaw norm technicznych.

Dla sformułowanej koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP opracowano tabelaryczne zestawienie porównawcze aktualnie obowiązujących wykazów norm rozwiązań bezpieczeństwa systemów teleinformatycznych wskazanych regulacjami przepisów prawa systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów publicznych z opracowanym w ramach koncepcji

wykazem norm ISO bezpieczeństwa systemów teleinformatycznych dla podmiotów systemu cyberbezpieczeństwa RP.

Wypracowane rozwiązanie koncepcyjne wykazy norm zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP zapewnia zgodność z wykładnią przepisów prawa oraz wynikami przeprowadzonego badania. Pozwala też czerpać z najlepszych rozwiązań opartych na szerokich doświadczeniach międzynarodowej społeczności ekspertów.

W wyniku zestawienia i zagregowania opracowanych koncepcji rozwiązań organizacyjnych systemu cyberbezpieczeństwa RP można przedstawić jego koncepcyjną strukturę w odniesieniu do poszczególnych zagadnień problemowych: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Struktura koncepcji systemu cyberbezpieczeństwa RP (SCRP) w zakresie zagadnień problemowych rozprawy została przedstawiona w tabeli 51.

W tabeli poprzez pogrubienie zostały wskazane i wyróżnione te komponenty struktury koncepcyjnego systemu cyberbezpieczeństwa RP (SCRP) i ich elementy, których nie ma w aktualnej strukturze krajowego systemu cyberbezpieczeństwa (KSC), a które zostały zidentyfikowane w ramach opracowanych koncepcji doskonalenia, stanowiących cele cząstkowe rozprawy w zakresie:

- zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym;
- zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym;
- wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa;
- wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Tabela 51. Struktura koncepcji systemu cyberbezpieczeństwa RP (SCRP) w zakresie zagadnień problemowych rozprawy

Struktura koncepcji systemu cyberbezpieczeństwa RP (SCRP) w zakresie zagadnień problemowych rozprawy					
Struktura dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym	**Struktury i relacje operacyjnych zarządzania systemu cyberbezpieczeństwa**			**Sektory krajowego systemu cyberbezpieczeństwa**	**Normy zarządzania bezpieczeństwem systemów teleinformatycznych**
	Zarządzanie cyberbezpieczeństwem na poziomie krajowym	**Zarządzanie incydentami cyberbezpieczeństwa**	**Struktury operacyjne (całkowite)**		
Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC)	**Prezes Rady Ministrów**	**Prezes Rady Ministrów**	**Prezes Rady Ministrów**	Energetyka	ISO 27001
Raport o zagrożeniach cyberbezpieczeństwa	**Rada Ministrów**	**Rada Ministrów**	**Rada Ministrów**	**Łączność (usługi pocztowe i kurierskie)**	**ISO 27002**
Plan Zarządzania Cyberbezpieczeństwem (PZC) ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych, ministrów odpowiedzialnych za systemy infrastruktury krytycznej, sektory krajowego systemu cyberbezpieczeństwa	**Rządowy Zespół Zarządzania Kryzysowego (RZZK)**	**Rządowy Zespół Zarządzania Kryzysowego (RZZK)**	**Rządowy Zespół Zarządzania Kryzysowego (RZZK)**	**Telekomunikacja i sieci teleinformatyczne**	**ISO 27005**
Plany Zarządzania Cyberbezpieczeństwem sektorowe, wojewódzkie, powiatowe, gminne		Zespół ds. Incydentów Krytycznych	Zespół ds. Incydentów Krytycznych	Bankowość i infrastruktura rynków finansowych	**ISO 24762/ ISO 27031**
Narodowy Program Ochrony Infrastruktury Teleinformatycznej (NPOIT)	**Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)**	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	Dyrektor Rządowego Centrum Bezpieczeństwa (RCB)	**Sektor żywnościowy i rolniczy**	**ISO 27032**

	Rządowe Centrum Bezpieczeństwa (RCB), mające w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa	**Rządowe Centrum Bezpieczeństwa (RCB) (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa)**	**Rządowe Centrum Bezpieczeństwa (RCB) (z funkcjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego ds. Cyberbezpieczeństwa)**	Wodociągi i kanalizacja	**ISO 27033**
	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON	organy właściwe ds. cyberbezpieczeństwa, minister właściwy ds. informatyzacji, minister obrony narodowej MON		
	ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych	**ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa, ministrowie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych**	**ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych, ministrowie odpowiedzialni za systemy infrastruktury krytycznej i sektory krajowego systemu cyberbezpieczeństwa oraz ministrowie właściwi w sprawach bezpieczeństwa narodowego, minister właściwy do spraw administracji publicznej, minister właściwy do spraw wewnętrznych**	Ochrona zdrowia	**ISO 27034**
	zespoły zarządzania kryzysowego przy ministrach kierujących działami admi-	**zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących dzia-**	**zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami**	Transport	**ISO 27035**

	nistracji rządowej i kierownikach urzędów centralnych	**łami administracji rządowej i kierownikach urzędów centralnych**	**administracji rządowej i kierownikach urzędów centralnych**		
	Szef Agencji Bezpieczeństwa Wewnętrznego	Szef Agencji Bezpieczeństwa Wewnętrznego	Szef Agencji Bezpieczeństwa Wewnętrznego	**Ratownictwo**	**ISO 27040**
	wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego (WZZK)	CSIRT MON, CSIRT NASK, CSIRT GOV	CSIRT MON, CSIRT NASK, CSIRT GOV	**Sektor chemiczny**	**ISO 20000 (-1, -2)**
	starosta, powiatowy zespół zarządzania kryzysowego (PZZK)	sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektorów)	sektorowe zespoły cyberbezpieczeństwa (dla wszystkich sektorów)	**Przemysł / Produkcja**	ISO 22301
	wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK)	**kierownicy jednostek organizacyjnych planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego**	**kierownicy jednostek organizacyjnych planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planach zarządzania kryzysowego**	**Handel**	
		centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych	**zespoły zarządzania kryzysowego i centra zarządzania kryzysowego przy ministrach kierujących działami administracji rządowej i kierownikach urzędów centralnych**	**Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki**	
		wojewoda, wojewódzkie centrum zarządzania kryzysowego (WCZK)	**wojewoda, komórka organizacyjna właściwa w sprawach zarządzania kryzysowego w urzędzie wojewódzkim, wojewódzki zespół zarządzania kryzysowego**	**Instytucje urzędów centralnych - wszystkie jednostki**	

			(WZZK), wojewódzkie centrum zarządzania kryzysowego (WCZK)		
		starosta, powiatowe centra zarządzania kryzysowego (PCZK)	**starosta, powiatowy zespół zarządzania kryzysowego (PZZK), powiatowe centra zarządzania kryzysowego (PCZK)**	**Sektor finansów publicznych**	
		wójt, burmistrz, prezydent miasta, gminne centrum zarządzania kryzysowego (GCZK)	**wójt, burmistrz, prezydent miasta, gminny zespół zarządzania kryzysowego (GZZK), gminne centrum zarządzania kryzysowego (GCZK)**	**Sektor usług komunalnych**	
		podmioty świadczące usługi z zakresu cyberbezpieczeństwa	podmioty świadczące usługi z zakresu cyberbezpieczeństwa	**Sektor usług publicznych**	
		operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny **(wszystkie)** **operator infrastruktury krytycznej**	operator usługi kluczowej dostawca usługi cyfrowej podmiot publiczny **(wszystkie)** **operator infrastruktury krytycznej**	**Sektor kosmiczny**	
			Kolegium ds. Cyberbezpieczeństwa	**Nauka i szkolnictwo wyższe**	
			Narodowy Punkt Kontaktowy do współpracy z NATO	**Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)**	
				Media (TV, radio, portale informacyjne)	

				Infrastruktura cyfrowa (DNS, IXP, TLD)	
				Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**)**	
				Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)	
				Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach	
				Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja)	
				Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa	
				Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa	

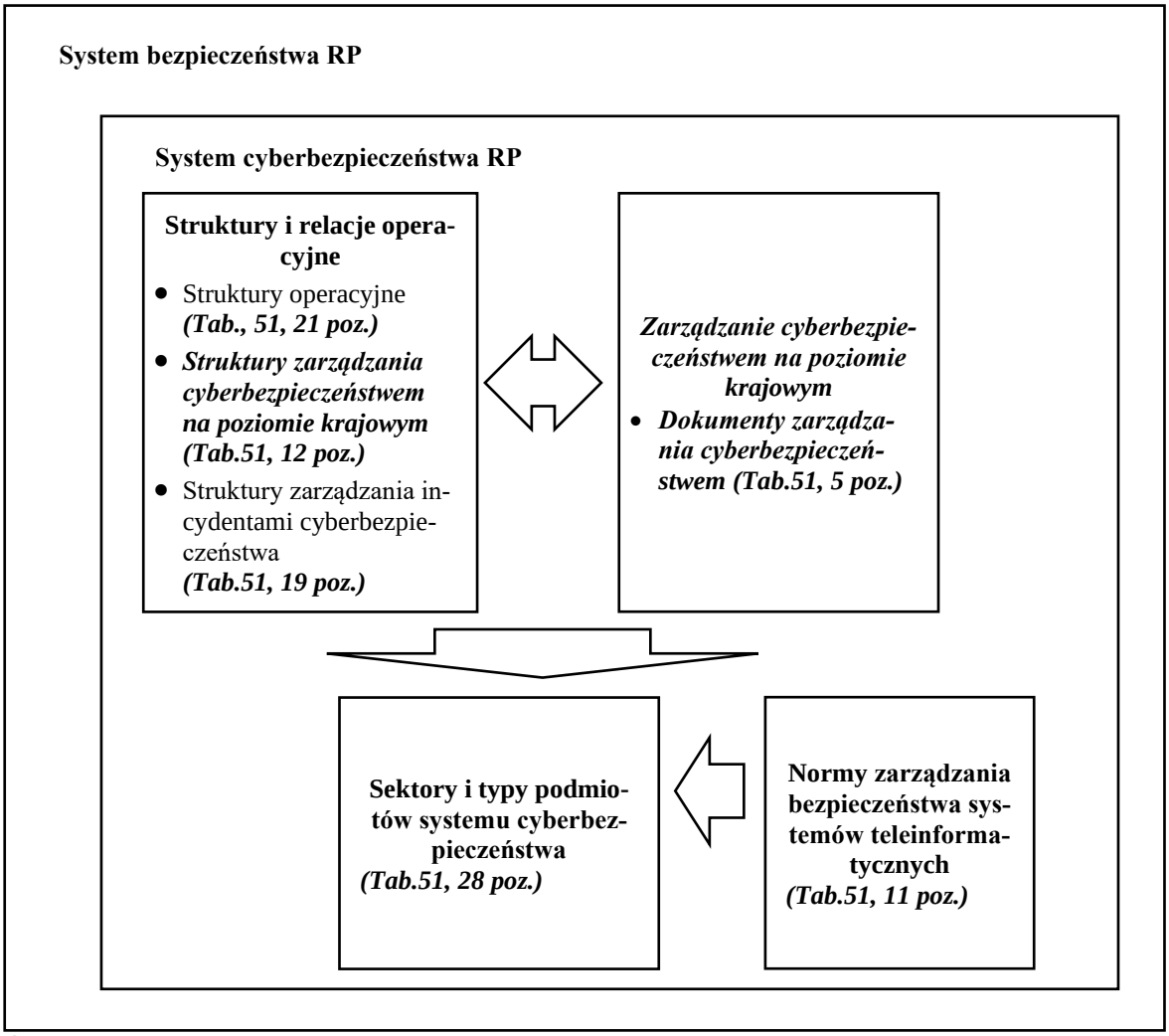
				publicznego lub usług kluczowych oraz uczestniczące w łańcu-chu dostaw dla nich	

Źródło: opracowanie własne na podstawie wyników badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Na podstawie opracowanych koncepcji rozwiązań organizacyjnych systemu cyberbezpieczeństwa RP w zakresie zagadnień problemowych zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa i jego struktury koncepcji systemu cyberbezpieczeństwa RP (SCRP) można przedstawić model koncepcji organizacji systemu cyberbezpieczeństwa RP (SCRP) w ujęciu komponentowym i relacyjnym.

Model koncepcji organizacji systemu cyberbezpieczeństwa RP (SCRP) w ujęciu komponentowym i relacyjnym przedstawia rys. 38.

Rys. 38. Model koncepcji organizacji systemu cyberbezpieczeństwa RP (SCRP)



Źródło: opracowanie własne na podstawie wyników badań w ramach realizacji projektu badawczego rozprawy doktorskiej w okresie 06-07.2022 r.

Uwaga: ***Pogrubieniem i kursywą*** na rys. 38 zaznaczono nowe lub rozbudowane elementy systemu cyberbezpieczeństwa RP zdefiniowane w ramach opracowanych koncepcji doskonalenia względem aktualnych elementów krajowego systemu cyberbezpieczeństwa

Model koncepcji systemu cyberbezpieczeństwa RP przedstawiony w ujęciu komponentowym i relacyjnym zawiera ulokowany w ramach systemu bezpieczeństwa kraju system cyberbezpieczeństwa, składający się z czterech komponentów: zarządzanie cyberbezpieczeństwem na poziomie krajowym, struktury i relacje operacyjne, sektory i typy podmiotów systemu cyberbezpieczeństwa i normy zarządzania bezpieczeństwem systemów teleinformatycznych.

Poprzez zestawienie i porównanie struktury oraz modelu komponentów i relacji aktualnego krajowego systemu cyberbezpieczeństwa ze strukturą i modelem komponentów i relacji koncepcyjnego systemu cyberbezpieczeństwa RP można wyróżnić opracowane w ramach przeprowadzonego procesu badawczego wyniki w postaci zdefiniowanych w ramach koncepcji systemu cyberbezpieczeństwa RP nowych komponentów i nowych elementów względem dotychczasowych komponentów krajowego systemu cyberbezpieczeństwa.

W ramach koncepcji doskonalenia systemu cyberbezpieczeństwa RP zaprojektowano dla tego systemu:

1. dodanie nowego komponentu Zarządzanie cyberbezpieczeństwem na poziomie krajowym, w ramach którego zdefiniowano dedykowane dokumenty procesów planowania i zarządzania cyberbezpieczeństwem na poziomie krajowym – o zawartości 5 pozycji;
2. w ramach komponentu Struktury i relacje operacyjne zarządzania cyberbezpieczeństwem na poziomie krajowym:
   2.1. rozszerzenie zakresu modułu Struktury operacyjne – z 13 do 21 pozycji;
   2.2. dodanie nowego modułu Struktury zarządzania bezpieczeństwem na poziomie krajowym – o zawartości 20 pozycji;
   2.3. rozszerzenie zakresu modułu Struktury zarządzania incydentami cyberbezpieczeństwa – z 11 do 19 pozycji;
3. w ramach komponentu Sektory i typy podmiotów systemu cyberbezpieczeństwa - rozszerzenie jego zakresu – z 9 do 28 pozycji;
4. w ramach komponentu Normy zarządzania bezpieczeństwem systemów teleinformatycznych - rozszerzenie jego zakresu – z 2 do 11 pozycji.

Opracowana w ramach przeprowadzonego procesu badawczego koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa RP, na którą składają się koncepcje cząstkowe w zakresie: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa i wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, jest efektem końcowym dysertacji i realizacją jej celu głównego:

Opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego efektywności i zwiększenia bezpieczeństwa państwa.

Opracowana w ramach realizacji celu głównego i celów szczegółowych rozprawy koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej, składająca się z czterech koncepcji cząstkowych, zgodnie z pierwotnym założeniem przyjętym w rozprawie jest propozycją zbioru kierunkowych, koncepcyjnych rozwiązań w wybranych obszarach problemowych, jest agregacją i kompilacją koncepcji cząstkowych, natomiast nie jest skonstruowaną definitywnie i ostatecznie koncepcją całościowego, kompleksowego modelu zorganizowania systemu cyberbezpieczeństwa RP. Wypracowane koncepcje cząstkowe tworzą w zdefiniowanym zakresie problemowym rozprawy spójne i wzajemnie powiązane merytorycznie rozwiązanie. Rozwiązanie to jest zgodne z przyjętymi założeniami dla realizacji rozprawy oraz adresuje pozytywnie zweryfikowane przyjęte hipotezy dla sformułowanych problemów badawczych.

System cyberbezpieczeństwa RP zbudowany w oparciu o rozwiązania koncepcyjne, opracowane w ramach przeprowadzonego procesu badawczego w ramach niniejszej dysertacji, może przyczynić się do zwiększenia efektywności systemu cyberbezpieczeństwa RP i tym samym zwiększenia poziomu bezpieczeństwa państwa.

ZAKOŃCZENIE

Cyberbezpieczeństwo jest jednym z kluczowych atrybutów bezpieczeństwa państwa ze względu na zależność podmiotów publicznych i gospodarczych, organizacji politycznych i społecznych oraz obywateli od systemów teleinformatycznych współtworzących cyberprzestrzeń. Cyberbezpieczeństwo ma charakter transsektorowy, jest więc jednym z podstawowych i istotnych komponentów bezpieczeństwa narodowego. Bezpieczeństwo w cyberprzestrzeni jako kategoria transsektorowa, łączy wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny. Niezbędne do zapewniania odpowiednio wysokiego poziomu cyberbezpieczeństwa jest podejście systemowe, zintegrowane i kompleksowe. Cyberbezpieczeństwo zapewniane i zarządzane w ramach systemu bezpieczeństwa państwa i będącego jego integralną częścią podsystemu cyberbezpieczeństwa. System bezpieczeństwa jest złożonym systemem, składającym się z podsystemu (systemu) kierowania bezpieczeństwem narodowym oraz podsystemów (systemów) wykonawczych. Podsystem cyberbezpieczeństwa, funkcjonujący w ramach systemu bezpieczeństwa, musi mieć strukturę zgodną ze strukturą systemu bezpieczeństwa, czyli składać się z komponentów podsystemu kierowania cyberbezpieczeństwem i podsystemów wykonawczych. System bezpieczeństwa powinien być kompletny, spójny, funkcjonalny oraz wydolny, sprawny, skuteczny i efektywny, a jego komponenty powinny być wewnętrznie wzajemnie powiązane, skoordynowane i zsynchronizowane w celu działania na rzecz zapewnienia trwałego i niezakłóconego rozwoju kraju i społeczeństwa oraz odpowiedniego poziomu bezpieczeństwa państwa. Sprawny, skuteczny i efektywny system cyberbezpieczeństwa jest niezbędnym warunkiem odpowiedzi na rosnące zagrożenia i wyzwania dla bezpieczeństwa cyberprzestrzeni oraz kluczowej i krytycznej infrastruktury systemów teleinformatycznych, a także dla niezakłóconego świadczenia kluczowych usług administracyjnych, społecznych, gospodarczych i dotyczących bezpieczeństwa publicznego, umożliwiających wielokierunkowy rozwój państwa.

Podjęta w niniejszej dysertacji problematyka badawcza w ramach zdefiniowanego przedmiotowego zakresu, obejmującego zorganizowanie systemu cyberbezpieczeństwa RP, w zakresie: zarządzania cyberbezpieczeństwem na poziomie krajowym, struktur i relacji

operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, jest niezmiernie ważna dla zapewnienia spójności i jednorodności tego systemu z innymi systemami bezpieczeństwa Polski, np. z systemem zarządzania kryzysowego, dla zapewnienia jego wysokiej operatywności i efektywności oraz dla zapewnienia wysokiego poziomu bezpieczeństwa polskiej cyberprzestrzeni i państwa polskiego.

Podjęty przedmiot badań oraz wyznaczone cele i sformułowane hipotezy, a także osiągnięte rezultaty w postaci opracowanych koncepcji rozwiązań doskonalących organizację krajowego systemu cyberbezpieczeństwa RP, znajduje uzasadnienie w konieczności zapewnienia bezpieczeństwa cyberprzestrzeni wobec dynamicznie zachodzących zmian w relacjach międzynarodowych w sferze geostrategicznej, wzrostu intensywności agresywnych i wrogich działaniach podejmowanych przez państwa i zorganizowane grupy cyberprzestępcze oraz wobec wykorzystywania dynamicznie rozwijanych technologii w obszarze rozwiązań teleinformatycznych, wykorzystywanych w przestępczej działalności w cyberprzestrzeni. Potwierdzeniem uzasadniającym podjęcie badań w ramach przedmiotu dysertacji jest również udział w badaniu dużej grupy respondentów – ekspertów z dziedziny cyberbezpieczeństwa i bezpieczeństwa narodowego.

Podjęty przedmiot badań oraz wyznaczone cele i sformułowane hipotezy, a także osiągnięte rezultaty w postaci opracowanych koncepcji rozwiązań doskonalących organizację krajowego systemu cyberbezpieczeństwa RP znajdują potwierdzenie w inicjatywach legislacyjnych UE. W grudniu 2022 r organy UE przyjęły nową wersję Dyrektywy NIS, czyli Dyrektywę NIS2[379], adresującą osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa oraz Dyrektywę CER[380] w sprawie odporności podmiotów krytycznych. Nowe regulacje w swoich zakresach podejmują i adresują zagadnienia podjęte w niniejszej rozprawie, ustanawiając rozwiązania podobne lub zbieżne w rozwiązaniami koncepcyjnymi wypracowanymi przez autora w niniejszej rozprawie w wyniku przeprowadzonych badań.

Polski system cyberbezpieczeństwa jest zbudowany w oparciu o ustawę o krajowym systemie cyberbezpieczeństwa (Ustawę KSC), ustanowioną i wprowadzoną na podstawie

[379] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

[380] Dyrektywa Parlamentu Europejskiego I Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE

unijnej Dyrektywy NIS, definiującej system cyberbezpieczeństwa sieci i systemów informatycznych krajów UE. W grudniu 2022 r. organy UE przyjęły nową wersję wspomnianej dyrektywy, tzw. Dyrektywę NIS2. Podstawowym celem tej regulacji jest osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego. Nowe wydanie Dyrektywy wprowadza szereg istotnych zmian, spośród których część bezpośrednio referuje do zagadnień problemowych podejmowanych w niniejszej rozprawie, tj. zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. W tym zakresie Dyrektywa NIS2 określa m.in. obowiązki państw członkowskich dotyczące przyjęcia krajowej strategii cyberbezpieczeństwa i krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie, wyznaczenia lub powołania właściwych organów ds. cyberbezpieczeństwa oraz organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, definiuje sektory i typy podmiotów objęte regulacją oraz środki zarządzania ryzykiem w cyberbezpieczeństwie – rozwiązania organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów objętych regulacją. Dyrektywa NIS2 zostanie wprowadzona do polskiego porządku prawnego poprzez nowelizację Ustawy KSC kształtującej krajowy system cyberbezpieczeństwa RP, a jej rozwiązania zostaną zaaplikowane w rozwiązania Ustawy. Tym samym nowe rozwiązania zawarte w Dyrektywie NIS2 stają się rozwiązaniami zmieniającymi i doskonalącymi krajowy system cyberbezpieczeństwa RP. Warto zatem przyjrzeć się bliżej zdefiniowanym koncepcjom i odnieść do wypracowanych w ramach procesu badawczego niniejszej rozprawy koncepcji problemowych rozwiązań organizacji krajowego systemu cyberbezpieczeństwa RP.

W zakresie problematyki zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym podjętej w dysertacji Dyrektywa NIS2 wskazuje, że każde państwo członkowskie musi przyjąć krajową strategię cyberbezpieczeństwa i krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie. Zapis dotyczący przyjęcia strategii cyberbezpieczeństwa został sformułowany również poprzedniej wersji Dyrektywy NIS, funkcjonuje także w aktualnie obowiązującej w Polsce Ustawie KSC, na podstawie którego została ustanowiona Strategia cyberbezpieczeństwa RP, omówiona w rozdziale II. Nowum Dyrektywy NIS2, a więc i docelowo przyszłej nowelizacji Ustawy KSC i innych regulacji polskiego systemu cyberbezpieczeństwa, jest to, że został zdefiniowany zakres tej strategii,

który jest bardzo szeroki i wykracza poza dotychczas przyjmowany zakres polskich polityk i strategii cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa ma obejmować cele strategiczne, zasoby kluczowe do osiągnięcia tych celów oraz odpowiednie polityki publiczne i regulacje zapewniające osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa ma zawierać cele i priorytety strategii cyberbezpieczeństwa państwa oraz ramy zarządzania na poziomie krajowym służące ich realizacji oraz definiujące role i obowiązki zaangażowanych organów. Strategia ma definiować mechanizm określania istotnych zasobów i szacowanie ryzyka w państwie oraz wskazywać środki zapewniające gotowość na wypadek incydentów, zdolność reagowania na nie i przywracanie normalnego działania, z uwzględnieniem współpracy pomiędzy sektorami publicznym i prywatnym. Strategia ma zawierać również ramy polityki koordynacji między właściwymi organami systemu cyberbezpieczeństwa i systemu zarządzania kryzysowego (odporności podmiotów krytycznych) w zakresie wymiany informacji na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych. Strategia ma zawierać również zestaw polityk publicznych adresujących kwestie cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług, wymogów cyberbezpieczeństwa i zarządzania podatnościami produktów ICT i usług ICT, utrzymywania dostępności, integralności i poufności infrastruktury publicznego otwartego internetu, rozwoju i integracji zaawansowanych technologii zarządzania ryzykiem w cyberbezpieczeństwie, rozwoju kształcenia i szkolenia w dziedzinie cyberbezpieczeństwa, rozwoju inicjatyw badawczo-rozwojowych i wspierania instytucji akademickich i naukowych w zakresie cyberbezpieczeństwa i bezpiecznej infrastruktury sieciowej, wymiany informacji o cyberbezpieczeństwie oraz wzmacniania poziomu cyberodporności, cyberhigieny i cyberochrony. W zakresie zarządzania incydentami i sytuacjami kryzysowymi cyberbezpieczeństwa, co jest jednym z aspektów zarządzania cyberbezpieczeństwem na poziomie krajowym, Dyrektywa NIS2 wskazuje obowiązek przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie określającego zdolności, zasoby i procedury niezbędne do reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie, również te na dużą skalę – obejmujące minimum 2 kraje członkowskie UE. Krajowy plany reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie ma zawierać cele w zakresie gotowości krajowych środków i działań, zadania i obowiązki organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany

informacji, organy i podmioty publiczne i prywatne oraz infrastrukturę oraz krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia dla tego rodzaju skoordynowanego zarządzania[381].

Zdefiniowana w Dyrektywie NIS2 konieczność przyjęcia przez każdy kraj członkowski UE krajowej strategii cyberbezpieczeństwa i krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie, których wspólny zakres obejmuje szacowanie ryzyka, określanie celów, działań i zasobów dla cyberbezpieczeństwa państwa oraz polityk zabezpieczania, przeciwdziałania i reagowania na incydenty i sytuacje kryzysowe cyberbezpieczeństwa. Tak zdefiniowany zakres i struktura obu przyszłych dokumentów zarządzania cyberbezpieczeństwem poziomu krajowego są bardzo zbliżone we wskazanym zakresie merytorycznym i założeniach stosowania do postulowanego w ramach jednej z hipotez rozprawy ujednolicenia i zharmonizowania zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym. Zgodnie z wypracowanym rozwiązaniem system cyberbezpieczeństwa RP (SCRP) powinien obejmować dedykowane i skoncentrowane na kwestiach cyberbezpieczeństwa procesy oraz dokumenty zarządcze poziomu krajowego, jako odpowiedniki dokumentów systemu zarządzania kryzysowego, np.: Krajowy Plan Zarządzania Cyberbezpieczeństwem (KPZC). Zdefiniowanie dokumentów zarządzania cyberbezpieczeństwem na poziomie krajowym w regulacji unijnej, koniecznej do zaimplementowania w polskim porządku prawnym, kształtującej nowy zakres polskich regulacji systemu cyberbezpieczeństwa, potwierdza zasadność sformułowanych w rozprawie postulatów koncepcji rozwiązań doskonalących polski system cyberbezpieczeństwa w zakresie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym.

W zakresie problematyki zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym podjętej w dysertacji Dyrektywa NIS2 ustanawia i definiuje krajowe ramy zarządzania kryzysowego w cyberbezpieczeństwie zapewniające spójność z istniejącymi krajowymi ramami zarządzania kryzysowego, w których

[381] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, op. cit., art. 7, 9

mają funkcjonować organ właściwy odpowiedzialny za cyberbezpieczeństwo i zadania nadzorcze (organ właściwy), organ właściwy odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę (organ ds. zarządzania kryzysowego w cyberbezpieczeństwie), pojedynczy punkt kontaktowy i CSIRT. Państwa członkowskie zobowiązane są do zapewnienia współpracy i wzajemnej wymiany informacji dotyczących identyfikacji podmiotów krytycznych, ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią mających wpływ na podmioty kluczowe wskazane jako podmioty krytyczne oraz na temat środków podjętych w odpowiedzi na takie ryzyko, zagrożenia i incydenty ww. organów z organami właściwymi systemu zarządzania kryzysowego, systemu usług zaufania, systemu finansowego oraz z organami ścigania, organami ochrony danych[382].

Zapisy Dyrektywy NIS2 obligują do zbudowania systemu zarządzania cyberbezpieczeństwem integrującego struktury i działania organów systemu cyberbezpieczeństwa i systemu zarządzania krajowego oraz innych systemów. Takie rozwiązanie, jest w pełni spójne z przedstawioną przez autora jedną z hipotez rozprawy ujednolicenia i zharmonizowania struktur i relacji operacyjnych systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w zarządzaniu cyberbezpieczeństwem na poziomie krajowym. Rozwiązania Dyrektywy potwierdzają zasadność sformułowanych postulatów rozwiązań doskonalących polski system cyberbezpieczeństwa w zakresie zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.

W zakresie sektorów i typów podmiotów, które powinny być objęte krajowym systemem cyberbezpieczeństwa Dyrektywa NIS2 ustanawia 2 typy podmiotów – podmioty kluczowe i podmioty ważne, wskazywane w sektorach kluczowych i ważnych wg sformułowanych kryteriów, wprowadzone w miejsce dotychczasowych podmiotów typu operator usługi kluczowej i dostawca usługi cyfrowej, wskazywane w zależności od rodzaju działalności. Dyrektywa NIS2 wskazuje wykaz sektorów kluczowych i sektorów ważnych. Jako sektory kluczowe zostały wskazane: energetyka (energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór), transport (lotniczy, kolejowy, wodny, drogowy), bankowość, infrastruktura rynków finansowych, opieka zdrowotna, woda pitna, ścieki, infrastruktura cyfrowa (punkt wymiany ruchu internetowego, usługi DNS, rejestry nazw TLD, usługi chmurowe, usługi przetwarzania danych, sieci dostarczania treści, usługi zaufania,

[382] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, op. cit., art. 8, 9, 10, 13

publiczne sieci i usługi łączności elektronicznej), usługi ICT (usługi ICT, usługi bezpieczeństwa), administracja publiczna (instytucje rządowe na szczeblu centralnym, podmioty na szczeblu regionalnym), przestrzeń kosmiczna. Jako sektory ważne zostały wskazane: usługi pocztowe i kurierskie, gospodarowanie odpadami, chemia, żywność, produkcja (wybrane podsektory), usługi cyfrowe (internetowe platformy handlowe, platformy usług sieci społecznościowych, wyszukiwarki internetowe), badania naukowe. Należy zwrócić uwagę, że zakres sektorów i typów podmiotów objętych Dyrektywą NIS2, a więc i docelowo nową wersją Ustawy KSC wprowadzającej Dyrektywę NIS2, jest znacznie szerszy od dotychczas zdefiniowanego i obejmuje wszystkie sektory i typu podmiotów, które zostały wskazane przez respondentów przeprowadzonego na potrzeby niniejszej rozprawy badania. Kolejnym istotnym aspektem definiowania podmiotów krajowego systemu cyberbezpieczeństwa jest wskazanie na kwalifikację podmiotów średnich i dużych, a w niektórych specyficznych przypadkach podmiotów mających odpowiednio duży wpływ na bezpieczeństwo państwa lub innych podmiotów, kwalifikowanie podmiotów bez względu na wielkość, nawet małych lub mikro. Warto zauważyć, że wszystkie sektory podmiotów krytycznych zdefiniowane w nowej, uchwalonej w grudniu 2022 r., dyrektywie unijnej w sprawie odporności podmiotów krytycznych (Dyrektywie CER) zostały uwzględnione w Dyrektywie NIS2, przy czym wszystkie, poza tylko sektorem żywnościowym, jako sektory kluczowe[383].

W zapisach Dyrektywy NIS2 zachodzi integracja zakresów sektorowych oddziaływania regulacji systemu cyberbezpieczeństwa i systemu zarządzania kryzysowego oraz bardzo istotne rozszerzenie zakresu sektorów i typów podmiotów objętych regulacjami cyberbezpieczeństwa, co jest w pełni spójne z przedstawioną przez autora jedną z hipotez rozprawy proponującą objęcie systemem cyberbezpieczeństwa RP wszystkich sektorów, systemów i typów podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujących zadania publiczne oraz wszystkich innych typów podmiotów mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego. Pozytywnie zweryfikowana hipoteza oraz wypracowany w procesie badawczym wykaz sektorów i typów podmiotów potwierdzają zasadność sformułowanych postulatów rozwiązań doskonalących polski system cyberbezpieczeństwa w zakresie objętych nim sektorów i typów podmiotów.

W zakresie zagadnienia wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP

[383] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, op. cit., art. 2, 3, Załącznik I, Załącznik II

Dyrektywa NIS2 formułuje wymaganie, aby podmioty krajowego systemu cyberbezpieczeństwa (podmioty kluczowe i ważne) wdrażały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Do wdrażania tych rozwiązań wskazane jest stosowanie europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych, tzn. norm i specyfikacji ISO[384].

Wskazanie na stosowanie międzynarodowych i europejskich norm ISO jest w pełni spójne z przedstawioną przez autora jedną z hipotez rozprawy ujednolicenia i zharmonizowania wymagań opartych na międzynarodowych i krajowych normach ISO zarządzania bezpieczeństwem systemów teleinformatycznych. W toku procesu badawczego sformułowano konkluzję, że rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa i powinny być oparte o szeroki katalog norm ISO dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych oraz norm zarządzania usługami informatycznymi i ciągłości działania. Wprowadzone zapisy Dyrektywy NIS2 kształtujące rozwiązania zarządzania ryzykiem w cyberbezpieczeństwie w oparciu o międzynarodowe i europejskie normy ISO potwierdzają zasadność sformułowanych postulatów rozwiązań doskonalących polski system cyberbezpieczeństwa w zakresie wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP.

Dyrektywa NIS2 jako dyrektywa unijna, która musi zostać wprowadzona do krajowych porządków prawnych państw członkowskich, kształtuje charakter i zakres przyszłych zapisów krajowych regulacji systemu cyberbezpieczeństwa – Ustawy KSC i rozporządzeń towarzyszących – formułujących rozwiązania zarządzania cyberbezpieczeństwem na poziomie krajowym, jak również bezpieczeństwa sieci i systemów informatycznych oraz usług społecznych i gospodarczych realizowanych z ich wykorzystaniem. Wprowadzone zapisy

[384] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, op. cit., art. 21, 25

Dyrektywy NIS2 kształtujące rozwiązania dotyczące krajowej strategii cyberbezpieczeństwa i krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie, właściwych organów ds. cyberbezpieczeństwa oraz organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, sektorów i typów podmiotów oraz środków zarządzania ryzykiem w cyberbezpieczeństwie bezpośrednio referują do zagadnień problemowych podejmowanych w niniejszej rozprawie, tj. zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa, wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. Zapisy Dyrektywy NIS2 potwierdzają zasadność sformułowanych szczegółowych problemów badawczych, hipotez i koncepcji rozwiązań doskonalących system cyberbezpieczeństwa RP.

Problematyka niniejszej rozprawy - zdefiniowane przedmiot badań, problemy badawcze, cele i hipotezy - jest zbieżna i adresuje wybrane cele i zadania w zakresie cyberbezpieczeństwa zdefiniowane w dokumentach strategicznych bezpieczeństwa RP, takich jak Strategia Bezpieczeństwa Narodowego RP, Strategia Cyberbezpieczeństwa RP, Doktryna Cyberbezpieczeństwa RP.

Problematyka podjęta przez autora w ramach niniejszej dysertacji adresuje i jest właściwa dla zdefiniowanego w Strategii Bezpieczeństwa Narodowego RP celu podniesienia poziomu odporności na cyberzagrożenia oraz zwiększenia poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Rozprawa adresuje działanie strategiczne „Cyberbezpieczeństwo" w zakresie zadania 1. Zwiększać poziom odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia, poprzez opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych oraz w zakresie zadania 2. Wzmacniać defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa, poprzez realizację wszystkich hipotez i celów szczegółowych rozprawy.

Podjęta problematyka niniejszej dysertacji adresuje i jest właściwa dla zdefiniowanego w Strategii Cyberbezpieczeństwa RP celu szczegółowego 1 – Rozwój krajowego sys-

temu cyberbezpieczeństwa zadania 1.2. Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa poprzez realizację wszystkich hipotez i celów szczegółowych rozprawy. Natomiast poprzez realizację celów opracowania koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych rozprawa adresuje zadanie 1.4. Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej sformułowanych celu szczegółowego 1 – Rozwój krajowego systemu cyberbezpieczeństwa oraz cel szczegółowy 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Niniejsza dysertacji adresuje i jest właściwa dla zdefiniowanego celu Doktryny Cyberbezpieczeństwa RP jakim jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni poprzez realizację wszystkich hipotez i celów szczegółowych rozprawy. Cel zapewnienia adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych jest adresowany poprzez opracowanie koncepcji wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz koncepcji wykazu norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych. Zdefiniowane w Doktrynie zagadnienia i zadania dotyczące zbudowania, utrzymywania i systematycznego doskonalenia (rozwoju) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo systemu cyberbezpieczeństwa RP składającego się z podsystemu kierowania i podsystemów operacyjnych i wsparcia adresowane są w rozprawie poprzez opracowanie koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym i koncepcji zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym.

Wypracowane w toku procesu badawczego szczegółowe, cząstkowe koncepcje doskonalenia systemu cyberbezpieczeństwa w zakresie problemów podjętych w rozprawie, adresujących zagadnienia zorganizowania systemu cyberbezpieczeństwa RP, w zakresie: zarządzania cyberbezpieczeństwem na poziomie krajowym, struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, składające się na

koncepcję główną, stanowią realizację celu praktycznego, utylitarnego rozprawy. Wypracowane koncepcje są rozwiązaniami o charakterze praktycznym, możliwym do zastosowania w systemie cyberbezpieczeństwa i bezpieczeństwa narodowego, w przypadku podjęcia przez właściwe organy państwa inicjatyw doskonalących i aktualizujących regulacje krajowego systemu cyberbezpieczeństwa RP.

Opracowany przez autora zbiór koncepcji szczegółowych, adresujących poszczególne badawcze problemy szczegółowe i hipotezy pomocnicze, sformułowanych w odniesieniu do celów szczegółowych składa się na realizację koncepcji głównej doskonalenia systemu cyberbezpieczeństwa RP na poziomie realizacji celu głównego rozprawy, jakim jest:

opracowanie koncepcji doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej dla poprawy jego funkcjonowania i zwiększenia bezpieczeństwa państwa.

Wypracowane koncepcje cząstkowe doskonalenia wskazanych w rozprawie zagadnień organizacji systemu cyberbezpieczeństwa tworzą w jej zdefiniowanym zakresie problemowym spójne, funkcjonalne, wydolne, operatywnie sprawne, skuteczne i efektywne oraz wewnętrznie wzajemnie powiązane, skoordynowane i zsynchronizowane rozwiązanie. Rozwiązanie to jest zgodne z przyjętymi założeniami dla realizacji procesu badawczego rozprawy oraz adresuje pozytywnie zweryfikowane przyjęte hipotezy dla sformułowanych problemów badawczych.

Opracowane w ramach rozprawy rozwiązania doskonalenia wybranych zagadnień dotyczących organizacji systemu cyberbezpieczeństwa RP nie zamykają tego, tak ważnego tematu, jakim jest zapewnienie efektywnego systemu cyberbezpieczeństwa państwa, raczej jest to przyczynkiem do podejmowania dalszych badań w tym kierunku i zakresie.

Wartym podjęcia i dalszego, indywidualnego pogłębienia jest każdy z poruszonych w niniejszej rozprawie aspektów organizacji systemu cyberbezpieczeństwa – tj. zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym, sektorów i typów podmiotów systemu cyberbezpieczeństwa oraz norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Kwestie zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, w tym zintegrowanego zarządzania cyberbezpieczeństwem w ramach bezpieczeństwa narodowego są niezwykle ważne. Metody zarządzania są wyrażane poprzez strukturę i zakres dokumentów zarządczych – planistycznych i operacyjnych oraz zawarte w nich metody

i techniki zarządcze. Niezwykle ważne jest uspójnienie zorganizowania procesów i dokumentów zarządzania cyberbezpieczeństwem w poszczególnych krajach i na poziomie międzynarodowym, np. w ramach UE i NATO, oraz związanych z tym procesów koordynacji i zarządzania cyberbezpieczeństwem.

Kolejnym niezmiernie ważnym zagadnieniem, które warte jest dalszego pogłębiania jest zorganizowanie struktur i relacji zarządczych i operacyjnych systemu zarządzania cyberbezpieczeństwem na poziomie krajowym. Efektywność systemu zależy nie tylko od struktury i zakresu procesów i dokumentów zarządzania, ale także od struktury organów i podmiotów zaangażowanych jego realizację. System taki powinien odpowiadać koncepcji systemu zbudowanego z podsystemu kierowania i podsystemów wykonawczych i wsparcia, jednakże niezmiernie ważny jest dobór organów i podmiotów każdego z podsystemów oraz zakresu ich kompetencji, a także wzajemnych relacji, powiązań i przepływu informacji oraz struktury procesów decyzyjnych i wykonawczych. Niezwykle ważne jest zdefiniowanie i integracja odpowiednich struktur i relacji zarządzania cyberbezpieczeństwem na poziomie międzynarodowym, np. w ramach UE i NATO.

Poszczególne podsystemy bezpieczeństwa funkcjonują w ramach całościowego systemu bezpieczeństwa, zatem niezmiernie ważne jest wypracowanie rozwiązań procesowych, relacyjnych i strukturalnych kooperacji i współpracy między podsystemami oraz w ramach całościowego systemu bezpieczeństwa w zakresie cyberbezpieczeństwa jako kategorii transsektorowej bezpieczeństwa. Kluczowe także są modele procesów komunikacyjnych i decyzyjnych w zakresie cyberbezpieczeństwa w ramach poszczególnych podsystemów i zintegrowanego, całościowego systemu cyberbezpieczeństwa.

Regulacje prawne, kształtujące poszczególne podsystemy bezpieczeństwa, tj. np. system zarządzania kryzysowego czy system cyberbezpiecześntwa, obejmują zdefiniowany zakres sektorów działalności administracyjnej, społecznej i gospodarczej oraz funkcjonujących w ich ramach instytucji i podmiotów. Skuteczność i efektywność takiego podsystemu bezpieczeństwa jest zależna od zakresu jego oddziaływania, zatem niezmiernie istotne jest wypracowanie odpowiedniego do celów bezpieczeństwa państwa podejścia do definiowania zakresu sektorowego i kryteriów wyboru instytucji i podmiotów nimi obejmowanych w ramach oddziaływania tego typu regulacji. W tym zakresie problemowym warto poddać badaniom rozwiązania prawne zarówno UE, jak i krajowe, powstające jako implementacja prawa europejskiego, jak też z inicjatywy wewnętrznej, ich wzajemne relacje i powiązania oraz procesy i motywy tworzenia poszczególnych regulacji.

Jednym z kluczowych podejść do zarządzania bezpieczeństwem i cyberbezpieczeństwem jest podejście oparte na zarządzaniu ryzykiem. Budowanie systemu cyberbezpieczeństwa opartego na zarządzaniu ryzykiem powinno przejawiać się na poziomie międzynarodowym – unijnym i natowskim, ma poziomie krajowym oraz na poziomie poszczególnych sektorów i podmiotów systemy cyberbezpieczeństwa. Wyzwaniami są opracowanie lub wybór najbardziej odpowiednich podejść, metod i technik szacowania ryzyka i zarządzania ryzykiem właściwych dla każdego z tych poziomów oraz zidentyfikowanie zależności ryzyk i działań odpowiedzi na ryzyka w ramach poszczególnych sektorów, w ujęciu międzysektorowym – krajowym i międzynarodowym, oraz w ujęciu krajowym i międzynarodowym.

Instytucje administracji publicznej i podmioty gospodarcze i społeczne są poddawane stałej presji w zakresie zapewnienia cyberbezpieczeństwa, ochrony danych i systemów teleinformatycznych ze względu na ciągle zmieniające się rozwiązania technologiczne systemów teleinformatycznych oraz powstawanie nowych narzędzi metod cyberzagrożeń. Wyzwaniem jest wypracowanie metodycznego i systemowego podejścia do tego zagadnienia w zakresie zarówno rozwiązań technicznych i technologicznych, jak również w zakresie doboru i stosowania odpowiednich norm, metodyk i standardów oraz technik i metod właściwych dla zarządzania bezpieczeństwem i zapewniania bezpieczeństwa. Istotnym zagadnieniem i wyzwaniem jest stosowanie rozwiązań normatywnych i metodycznych w formie zintegrowanej, co może być podstawą do prowadzenia badań w zakresie metod integracji rozwiązań systemowych i procesowych zdefiniowanych w poszczególnych grupach rozwiązań, jak np. normach ISO, metodykach i standardach branżowych, a także metod integracji rozwiązań normatywnych z rozwiązaniami metodyk i standardów branżowych.

Cyberbezpieczeństwo państwa jest zapewniane w ramach systemu bezpieczeństwa narodowego. Obszarem prac badawczych jest zdefiniowanie modelu systemu zarządzania (kierowania) cyberbezpieczeństwem w systemie zarządzania (kierowania) bezpieczeństwem narodowym. W tym zakresie istotne jest całościowe ujęcie modelu systemu cyberbezpieczeństwa z jego podsystemem kierowania i podsystemami wykonawczymi i wsparcia oraz model relacji i integracji systemu cyberbezpieceństwa i jego podsystemów z systemem bezpieczeństwa narodowego i jego podsystemami. Warto rozważyć i uwzględnić ujęcie sektorowe bezpieczeństwa i transsektorowy charakter cyberbezpieczeństwa oraz aspekty cyberbezpieczeństwa systemów wykonawczych i systemów wsparcia systemu bezpieczeństwa narodowego.

System cyberbezpieczeństwa kraju kształtowany jest w ramach dokumentów strategicznych cyberbezpieczeństwa – doktryn, strategii i polityk. Powstają one w odpowiedzi na

zachodzące zmiany i aktualny stan środowiska bezpieczeństwa i cyberbezpieczeństwa, zarówno krajowego, jak i międzynarodowego. Formowane są i powinny być w relacji do podobnych dokumentów organizacji międzynarodowych, jak UE i NATO. Zakres możliwych badań w tym obszarze jest również szeroki, od analizy i porównania aktualnych dokumentów strategicznych poszczególnych państw, wybranych z kręgu państw sojuszniczych i partnerskich oraz krajów potencjalnie nieprzyjaznych, poprzez analizy w odniesieniu do dokumentów strategicznych cyberbezpieczeństwa poziomu międzynarodowego – UE i NATO, do opracowania wytycznych, koncepcji, kierunków czy modeli takich dokumentów strategicznych poziomu międzynarodowego i krajowego. Warto uwzględnić kształtowanie tego typu regulacji i dokumentów z nimi powiązanych na poziomie UE i NATO. Polskie dokumenty strategiczne adresujące kwestie cyberbezpieczeństwa w dobie zachodzących zmian w środowisku geopolitycznym, trwających konfliktów i gry interesów oraz intensywnością wrogich działań w cyberprzestrzeni, a także zmian regulacyjnych na poziomie UE, zapewne wymagają aktualizacji i redefinicji. Podjęcie badań w tym zakresie jest kluczowe dla dalszego rozwoju nauk o bezpieczeństwie z zakresie cyberbezpieczeństwa.

Proponowana przez autora problematyka przyszłych, kolejnych badań w obszarze powiązanym z problematyką niniejszej rozprawy odnosi się do zagadnień dotyczących rozwiązań systemu cyberbezpieczeństwa Polski, jak również lokuje zagadnienia cyberbezpieczeństwa w ujęciu międzynarodowym, w relacjach z rozwiązaniami Unii Europejskiej i NATO. Szerokie, adresujące aspekty interoperacyjności, rozwijanie rozwiązań cyberbezpieczeństwa poszczególnych krajów w powiązaniu z cyberbezpieczeństwem międzynarodowym, regionalnym, europejskim i notowskim (transatlantyckim) jest koniecznością, jak i wyzwaniem niezbędnym do podjęcia.

Rozwój nauk o bezpieczeństwie w zakresie cyberbezpieczeństwa poza pogłębianiem dotychczas podjętej problematyki może i zapewne będzie wchodził na coraz to nowe obszary integrujące zagadnienia dziedzinowe i sektorowe bezpieczeństwa z cyberbezpieczeństwem. Taki kierunek rozwoju wydaje się naturalny ze względu na bardzo duże i wciąż pogłębiające się zależności sfery polityczno-społeczno-gospodarczej oraz dziedzin i sektorów bezpieczeństwa od rozwoju informatyzacji i zapewniania cyberbezpieczeństwa w stale zmieniających się warunkach i środowisku bezpieczeństwa.

BIBLIOGRAFIA

Pozycje zwarte i artykuły:

1) Abramowicz W., Bukowska E., Filipowska A., *Zapewnienie bezpieczeństwa przez semantyczne monitorowanie cyberprzestrzeni*, e-mentor nr 3 (50), 2013,
2) Aluchna M., *Polityka informacyjna w Polsce. Przypadek spółek giełdowych*, e-mentor nr 2 (9), 2005,
3) Andreasson K.J., *Cybersecurity. Public Sector Threats and Responses*, CRC Press, 2012,
4) Apanowicz J., *Metodologia ogólna*, Gdynia 2002,
5) Batorowska H., Musiał E. (red.), *Bezpieczeństwo informacyjne w dyskursie naukowym*, Uniwersytet Pedagogiczny w Krakowie, Kraków, 2017,
6) Bąk T., Błażejewska B., *Bezpieczeństwo publiczne, współczesne zagrożenia a bezpieczeństwo państwa*, Zeszyt nr 12/2018,
7) Bąk T., Ciekanowski Z., Nowicka J. (red.), *Współczesne zagrożenia bezpieczeństwa państwa*, PWST-E w Jarosławiu, Jarosław 2016,
8) Bąk T., Ciekanowski Z. (red.), *Bezpieczeństwo regionalne gwarantem rozwoju zasobów ludzkich*, PWST-E w Jarosławiu, Jarosław 2015,
9) Będźmirowski J., J*ednostki Obrony Terytorialnej Marynarki Wojennej w systemie bezpieczeństwa morskiego Polski w okresie Zimnej Wojny*, Colloquium 2021 nr 2 (13), Akademia Marynarki Wojennej, Gdynia 2021,
10) Będźmirowski J., Gac M., *Polska Marynarka Wojenna w polityce bezpieczeństwa morskiego państwa w drugiej połowie XX wieku: próba usystematyzowania*, Akademia Marynarki Wojennej, Gdynia 2021,
11) Będźmirowski J., *Bezpieczeństwo polskiej granicy morskiej w początkowym okresie funkcjonowania Układu Warszawskiego*, [w:] Bezpieczeństwo państw Europy Środkowej i Wschodniej: Kwestie społeczne, ekonomiczne, polityczne i militarne, Ziętarski M. (red.), Wydawnictwo Naukowe Silva Rerum, Poznań 2020,

12) Będźmirowski J., *Bezpieczeństwo Europy oraz państw nadbałtyckich w koncepcji Działu Spraw Morskich Ministerstwa Przemysłu, Handlu i Żeglugi, Rządu Emigracyjnego w Londynie*, [w:] Siły morskie Rzeczypospolitej Polskiej w bałtyckim i światowym systemie bezpieczeństwa na morzu: Księga jubileuszowa prof. dr. hab. Andrzeja Makowskiego, Akademia Marynarki Wojennej, Gdynia 2020,
13) Bernacik B., *Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej*, [w:] Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń, Ł. Roman, K. Krassowski, S. Sagan, D. Wróblewski (red.), Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2018,
14) Brysiak K., Elak L., Zygo K., *Geneza hegemoni: implikacja terminu na podstawie Machiavellego oraz analiza hegemoni wybranych państw na przestrzeni wieków*, Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego, 2022, T. XVII, nr 19(2), Lublin 2022,
15) Brzostek A., *Organy władzy publicznej w zakresie ochrony cyberbezpieczeństwa w wybranych strategiach cyberbezpieczeństwa*, Przegląd Prawa Konstytucyjnego, ISSN 2082-1212, DOI 10.15804/ppk.2021.01.18, Nr 1 (59)/2021, Warszawa 2021,
16) Buzan, B., Wæver, O., de Wilde, J., *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers, 1998,
17) Ciekanowski Z., *Podstawy zarządzania bezpieczeństwem państwa*, PWST-E, Jarosław 2019,
18) Ciekanowski Z., *Zagrożenia bezpieczeństwa państwa*, Bezpieczeństwo i Technika Pożarnicza, CNBOP 1/ 2011, Józefów 2011,
19) Ciekanowski Z., Krysiński S., *Zarządzanie kryzysowe w Polsce w sytuacjach zagrożeń niemilitarnych jako sposób umacniania bezpieczeństwa państwa*, PWST-E, Jarosław 2014,
20) Ciekanowski Z., Majkowska J., Załoga W., *Wpływ otoczenia na funkcjonowanie organizacji*, Nowoczesne Systemy Zarządzania, 2018 nr 4 (13), WAT, Warszawa 2018,
21) Ciekanowski Z., Nowicka J., Wyrębek H., *Zarządzanie zasobami ludzkimi w sytuacjach kryzysowych*, CeDeWu Sp. z o.o., Warszawa 2017,
22) Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Pracownia Wydawnicza Wydziału Humanistycznego Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2016,

23) Ciekanowski Z., Ulijasz B., *Zwalczanie terroryzmu w Unii Europejskiej*, PWSTE, Jarosław 2015,
24) Ciekanowski Z., Starczewski J., *Uwarunkowania bezpieczeństwa informacji i systemów teleinformatycznych*, Współczesne Problemy Zarządzania, 6(1(12), PWSTE w Jarosławiu, Jarosław 2018,
25) Ciekanowski Z., Wojciechowska-Filipek S., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki - organizacji – państwa*, CeDeWu Sp. z o.o., Warszawa 2019,
26) Czekaj J., M. Ćwiklicki, *Infonomika jako dyscyplina naukowa*, e-mentor nr 2 (29), 2009,
27) Czupryński A., Elak L., Schreiber H., *Bezpieczeństwo dla rozwoju, Komunikacja międzykulturowa w operacjach reagowania kryzysowego*, AON, Warszawa 2012,
28) Daniluk P., *Wojna informacyjna – złożona przeszłość i niepewna przyszłość***,** Rocznik Bezpieczeństwa Międzynarodowego 2019, vol. 13, nr 2, Akademia Wojsk Lądowych, Wrocław 2019,
29) Dawidczyk A., Gryz J., Koziej S., *Zarządzanie strategiczne bezpieczeństwem. Teoria – praktyka – dydaktyka*. Wyższa Szkoła Humanistyczno-Ekonomiczna w Łodzi, Łódź, 2008,
30) Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002,
31) Dobroczyński M., Stefanowicz J., *Polityka zagraniczna*, PWN, Warszawa 1984,
32) Elak L., *Uwarunkowania bezpieczeństwa Polski na przełomie XX i XXI wieku*, Bezpieczeństwo. Teoria i Praktyka, 2020, No 2 (XXXIX), Oficyna Wydawnicza KA AFM, Kraków 2020,
33) Elak L., *Rola NATO w obszarze bezpieczeństwa europejskiego*, Zeszyty Naukowe, AON, wyd. 3(80), Warszawa 2010,
34) Elak L., Karolewski A., *Przyczyny wojen hybrydowych: wyniki badań empirycznych*, [w:] Zagrożenie wschodniej flanki NATO w aspekcie bezpieczeństwa wewnętrznego obszarów przygranicznych, Elak L., Ciekanowski Z., Dachowicz D. (red.), Wydawnictwo im. Prof. Leszka J. Krzyżanowskiego Wyższej Szkoły Menedżerskiej w Warszawie, Warszawa 2022,
35) Elak L., Karolewski A., *Przyczyny wojen hybrydowych w XXI wieku*, Akademia Sztuki Wojennej, Warszawa 2016,

36) Elak L., Kuranc-Szymczak M. (red.), *Zagrożenia dla bezpieczeństwa Polski*, Wyższa Szkoła Humanistyczno-Ekonomiczna, Zamość 2019,
37) Elak L., Rosłoń P., Iwanowski N., Zygo K., *Wyzwania Sił Zbrojnych Rzeczypospolitej Polskiej w nowych uwarunkowaniach bezpieczeństwa*, Akademia Sztuki Wojennej, Warszawa 2020,
38) Fehler W., *Sektor bezpieczeństwa wewnętrznego – mechanizmy i praktyka zmian*, DOCTRINA, Nr 6 Studia Społeczno-Polityczne, 2009,
39) Flasiński M., *Wstęp do analitycznych metod projektowania systemów informatycznych*, WNT, Warszawa 1997,
40) Fowler B., Maranga K, *Cybersecurity Public Policy. SWOT Analysis Conducted on 43 Countries*, CRC Press, 2022,
41) Frankfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych*, Zysk i S-ka, Poznań 2001,
42) Giemza M., *Zarządzanie bezpieczeństwem informacji w organizacji*, https://www.researchgate.net/publication/292140991, 2016 (28.11.2018),
43) Gradzi D., *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych*, Przegląd Bezpieczeństwa Wewnętrznego 16/17, 2017,
44) Gryz J., *Wzajemny związek między polityką i strategią a bezpieczeństwem państwa*, Rocznik Bezpieczeństwa Międzynarodowego 2, 11-28, 2007,
45) Guiora A.N., *Cybersecurity Geopolitics, Law, and Policy*, Routledge, 2017,
46) Jagusiak B., *Zagrożenia bezpieczeństwa państwa. Geneza i charakter uwarunkowań*, Wojskowa Akademia Techniczna, Warszawa 2015,
47) Jagusiak B. (red.), *Systemy bezpieczeństwa w teorii i praktyce, Wojskowa Akademia Techniczna*, Warszawa 2018,
48) Jagusiak B. (red.), *Zagrożenia bezpieczeństwa państwa – geneza i charakter uwarunkowań*, Wydawnictwo Wojskowej Akademii Technicznej, Warszawa 2015,
49) Jagusiak B. (red.), *Współczesne wyzwania bezpieczeństwa Polski*, Wydawnictwo Wojskowej Akademii Technicznej, Warszawa 2015,
50) Jagusiak B., Żukowski P., *Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa. Zagadnienia wybrane*, Wojskowa Akademia Techniczna, Warszawa 2019,
51) Johnson T.A., *Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Routledge, 2020,

52) Kitler W., *System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne*, Wiedza Obronna Vol. 268 No. 3, 2019, ISSN: 2658-0829 (Online) 0209-0031, Akademia Sztuki Wojennej, Warszawa 2019,
53) Klisz M., Elak L., *The Total Defence 21st Century. COM – Building a Resilient Society: Introduction*, Bezpieczeństwo. Teoria i Praktyka, 2022, No. 3 (XLVIII), Oficyna Wydawnicza KA AFM, Kraków 2022,
54) Kolbusz E., Nowakowski A., *Informatyka dla ekonomistów – Teoria. Systemy. Metody*, Zachodniopomorska Szkoła Biznesu, Szczecin, 1994,
55) Kosowski B., *Bezpieczeństwo informacyjne w zarządzaniu firmą*, Wyższa Szkoła Zarządzania Ochroną Pracy w Katowicach, I Konferencja Naukowa Bezpieczeństwo Pracy – Edukacja – Środowisko,
56) Kostopoulos G., *Cyberspace and Cybersecurity*, Auerbach Publications, 2020,
57) Kotarbiński T., *Elementy teorii poznania, logiki formalnej i metodologii nauk*, Wrocław 1961,
58) Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, Bezpieczeństwo Narodowe II – 2011/18, Polityczno-strategiczne aspekty bezpieczeństwa, Warszawa 2011,
59) Kozielecki, *Rozwiązywanie problemów*, Warszawa 1960,
60) Krawiec J., *System zarządzania bezpieczeństwem informacji – zabezpieczenia*, Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji W Warszawie, T. 15, Z. 1(38) 2017,
61) Kuraś M., *Informatyka a coraz nowsze pojęcia informatyczne*, e-mentor nr 4 (31), 2009,
62) Kulikowski J. L., *Informacja i świat, w którym żyjemy*, 1978,
63) Kulisz M., *Zarządzanie systemem bezpieczeństwa państwa*, Rocznik bezpieczeństwa międzynarodowego 2010/2011,
64) Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012,
65) Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017,
66) Łakomy M., *Cyberwojna – ujęcia definicyjne*, Stosunki Międzynarodowe – International Relations, nr 2 (t. 48), 2013,
67) Łobocki M., *Metody badań pedagogicznych*, Warszawa 1982,

68) Łuczak J., *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, Studia Oeconomica Posnaniensia 2016, vol. 4, no. 12,
69) Manjikian M., *Cybersecurity Ethics. An Introduction*, Routledge, 2022,
70) Materska K., *Audyt informacji - metodologiczne problemy*, e-mentor nr 5 (42), 2011,
71) Mąkosa G., *Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa,* Nowoczesne Systemy Zarządzania, Zeszyt 14, nr 3, WAT, Warszawa 2019,
72) Mąkosa G., *Krajowy system cyberbezpieczeństwa RP*, [w:] Perspektywy bezpieczeństwa w teorii i praktyce, Chabasińska A., Warchał A. (red.), Wojskowa Akademia Techniczna, Warszawa 2019,
73) Mąkosa G., *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020,
74) Mąkosa G., *Zarządzanie kryzysowe a krajowy system cyberbezpieczeństwa*, [w:] Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020,
75) Mąkosa G., *Zarządzanie danymi i systemami IT w Zarządzaniu 4.0*, [w:] Czwarta rewolucja przemysłowa. Mity, paradygmaty i zastosowania. Tom 1 Kompetencje i baza narzędziowa Przemysłu 4.0, Wojciechowski Z. Zaskórski P. (red.), Wojskowa Akademia Techniczna, Warszawa 2020,
76) Mąkosa G., *Bezpieczeństwo cybernetyczne systemów w czwartej rewolucji przemysłowej,* [w:] Czwarta rewolucja przemysłowa. Mity, paradygmaty i zastosowania. Tom 1 Kompetencje i baza narzędziowa Przemysłu 4.0, Wojciechowski Z. Zaskórski P. (red.), Wojskowa Akademia Techniczna, Warszawa 2020,
77) Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, Studia Bezpieczeństwa Narodowego 17(1), Wojskowa Akademia Techniczna, Warszawa 2020,
78) Mąkosa G., *Policja w systemie cyberbezpieczeństwa RP,* [w:] Formacje policyjne w systemie bezpieczeństwa wewnętrznego państwa, Śmiałek K. (red.), WAT, Warszawa 2021,
79) Mąkosa G., *Organizacja systemu cyberbezpieczeństwa RP,* [w:] Świat bez równowagi bezpieczeństwa. Studium wybranych problemów, Lizakowski P. (red.), Wydawnictwo FNCE, Poznań 2021,

80) Mąkosa G., *Zarządzanie ryzykiem w ochronie danych osobowych,* [w:] Ochrona danych osobowych. Perspektywa krajowa i międzynarodowa, Śmiałek K., Kominek A. (red.), Wydawnictwo FNCE, Poznań, 2021,
81) Mąkosa G., *Zarządzanie ryzykiem w ochronie informacji niejawnych,* [w:] Ochrona informacji niejawnych w perspektywie krajowej i międzynarodowej, Śmiałek K., Kominek A. (red.), Wydawnictwo FNCE, Poznań 2021,
82) Mąkosa G., *Strategiczne ujęcie cyberbezpieczeństwa RP*, [w:] Securitologiczna panorama bezpieczeństwa, Lizakowski P. (red.), Wydawnictwo FNCE, Poznań 2022,
83) Mąkosa G., *Realizacja celów biznesowych i poczucie bezpieczeństwa organizacji w aspekcie cyberbezpieczeństwa*, [w:] Odporność organizacji. Cyfryzacja. Bezpieczeństwo. Innowacje, Tarapata J., Woźniak J. (red.), Difin 2022, Warszawa 2022,
84) Mąkosa G., Sołek-Borowska C., *Bezpieczeństwo w organizacji oraz cyberbezpieczeństwo – perspektywa empiryczna,* [w:] Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Gonciarski W., Woźniak J. (red.), Difin, Warszawa 2021,
85) Moallem A., *Understanding Cybersecurity Technologies. A Guide to Selecting the Right Cybersecurity Tools*, CRC Press, 2021,
86) Muliński T., *Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji*, rozprawa doktorska, Wyższa Szkoła Policji w Szczytnie, Szczytno, 2014,
87) Musioł M., *Znaczenie sekurytyzacji i sektorów bezpieczeństwa w ramach krytycznych studiów nad bezpieczeństwem*, Uniwersytet Wrocławski, Historia i Polityka, Nr 23 (30)/2018,
88) Nepelski M., *Zarządzanie w sytuacjach kryzysowych*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2016,
89) Kowalkowski S. (red.), Niemilitarne zagrożenia bezpieczeństwa publicznego, AON, Warszawa 2011,
90) Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin SA, Warszawa 2011,
91) Nowak S., *Metodologia badań socjologicznych*, Warszawa 1970,
92) Olczak S., *Koncepcja obiegu informacji o zagrożeniach i incydentach w systemie bezpieczeństwa państwa*, rozprawa doktorska, Wojskowa Akademia Techniczna, 2019,

93) Oleksiewicz I., *Bezpieczeństwo informacyjne jako wyzwanie XXI wieku*, Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji W Warszawie, T. 15, Z. 4(41) 2017,
94) Oleksiewicz I., *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne rzeczypospolitej polskiej*, Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie, nr 33 (2019), Częstochowa 2019,
95) Olender A., *Proces zarządzania incydentami bezpieczeństwa informacji*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), WAT, Warszawa 2020,
96) Olender A., *Szacowanie i analiza ryzyka ciągłości funkcjonowania organizacji w kontekście incydentów bezpieczeństwa informacji*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), WAT, 2020,
97) Oleński J., *Ekonomika informacji. Podstawy*, PWE, 2001,
98) Oleński J., *Ekonomika informacji – Metody*, PWE, Warszawa 2003,
99) Pałęga M., *Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych*, [w:] Systemy wspomagania w inżynierii produkcji, Prusak R., Kardas E. (red), 2017, vol.6, issue 9,
100) Gwoździewicz S., Tomaszycki K. (red.), *Prawne i społeczne aspekty cyberbezpieczeństwa*, Międzynarodowy Instytut Innowacji „Nauka – Edukacja – Rozwój" w Warszawie, Warszawa 2017,
101) Priyadarshini I., Cotton C., *Cybersecurity. Ethics, Legal, Risks, and Policies*, Apple Academic Press, 2022,
102) Radziejewski K., *Cyberbezpieczeństwo w administracji rządowej w Rzeczypospolitej Polskiej*, Przegląd Bezpieczeństwa Wewnętrznego 16/17, 2017,
103) Rakowski M., *„Nowe wojny" – wybrane aspekty asymetrycznych konfliktów w cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego 17/17, 2017,
104) Santos H., *Cybersecurity. A Practical Engineering Approach*, Chapman&Hall, 2022,
105) Shoemaker D., Kohnke A, Sigler K., *The Cybersecurity Body of Knowledge. The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity*, CRC Press, 2022,
106) Siek M., *Analiza systemowa i prognozowanie stanu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni*, rozprawa doktorska, Wojskowa Akademia Techniczna, 2020,

107) Siek M., *Wojna informacyjna w cyberprzestrzeni*, [w:] Wybrane zagadnienia bezpieczeństwa międzynarodowego, Wiesława Załoga (red.), Wydawnictwo: Wojskowa Akademia Techniczna, Warszawa 2018,

108) Sienkiewicz P., *Wyzwania i zagrożenia bezpiecznego rozwoju społeczeństwa informacyjnego*, Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2,

109) Sienkiewicz P. (red.), *Inżynieria systemów bezpieczeństwa*, PWE, Warszawa, 2014,

110) Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni*, [w:] Metodologia badań bezpieczeństwa narodowego, Sienkiewicz P. (red.), M. Marszałek, H. Świeboda, Tom III, Warszawa, 2012,

111) Sienkiewicz P., *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością*, AON, Warszawa 2008,

112) Sienkiewicz P., *Wizje i modele wojny informacyjnej*, [w:] Społeczeństwo informacyjne – wizja czy rzeczywistość?, Haber L. H. (red.), Biblioteka Główna Akademii Górniczo-Hutniczej, Kraków 2003,

113) Sienkiewicz P., *Analiza systemowa i podstawy zastosowania*, Wydawnictwo Bellona, Warszawa 1994,

114) Sienkiewicz P., Świeboda H., *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa,* Polskie Stowarzyszenie Zarządzania Wiedzą, seria: Studia i materiały, nr 33, 2010,

115) Sienkiewicz P., Świeboda H., Szczepaniuk E. (red.), *Efektywność cyberobrony*, praca naukowo-badawcza, Akademia Obrony Narodowej, 2014,

116) Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa, 2008,

117) Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, PWN, Warszawa–Poznań 2001

118) Sobczak J., *Nowa strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Cybersecurity and Law, Nr 2(4) 2020 Akademia Sztuki Wojennej, Warszawa 2020,

119) Stańczyk J., *Formułowanie kategorii pojęciowej bezpieczeństwa*, Wydawnictwo FNCE sp. z o. o., Poznań 2017,

120) Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Wydawnictwo Instytutu Studiów Politycznych Polskiej Akademii Nauk, Warszawa 1996,

121) Stefanowicz B., *Informacja*, SGH, Warszawa, 2004,

122) Stefanowicz B., *O pojęciach i terminach informatycznych - polemika*, e-mentor nr 5 (32), 2009,

123) Stefanowicz B., *Rola informacji*, e-mentor nr 5 (22), 2007,

124) Jagusiak B., Trejnis Z. (red.), *Studia bezpieczeństwa narodowego*, Wojskowa Akademia Techniczna, 2011,

125) Szeptuch A., *Metody informatyczne jako instrument zarządzania wiedzą*, e-mentor nr 1 (48), 2013,

126) Szleszyński A., *Pomiar bezpieczeństwa informacji w zarządzaniu bezpieczeństwem w systemie teleinformatycznym*, Zeszyty Naukowe Politechniki Śląskiej 2014, seria: Organizacja i Zarządzanie z. 74, nr kol. 1921,

127) Świeboda H., *Zagrożenia informacyjne bezpieczeństwa RP*, rozprawa doktorska, Akademia Obrony Narodowej, 2009,

128) Świniarski J., Chojnacki W., *Filozofia bezpieczeństwa. Podręcznik akademicki*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2004,

129) Świniarski J., *O naturze bezpieczeństwa*, Agencja wydawnicza ULMAK, Warszawa 1997,

130) Terlikowski T., *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów. System cyberbezpieczeństwa w Polsce (w świetle obowiązującego prawa)*, Zeszyty Naukowe SGSP 2019, Nr 71/3/2019, Warszawa 2019,

131) Tikk E., Kerttunen M., *Routledge Handbook of International Cybersecurity*, Routledge, 2022,

132) Tzu S., Pin S., *Sztuka wojny*, Grupa Wydawnicza Helion, Gliwice 2005.

133) Unlod J., Zarządzanie informacją w cyberprzestrzeni, PWN, Warszawa 2015,

134) Wereda W., *Budowanie relacji z interesariuszami w kontekście bezpieczeństwa organizacji – wyzwania gospodarki cyfrowej*, [w:] Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Gonciarski W., Woźniak J. (red.), Difin, Warszawa 2021,

135) Werner J., Szczepaniuk E., *Bezpieczeństwo informacyjne organizacji*, Zeszyty Naukowe AON nr 4 (105) 2016,

136) Więcaszek-Kuczyńska L., Zagrożenia bezpieczeństwa informacyjnego, Obronność. Zeszyty Naukowe 2(10)/2014 ISSN 2299-2316,

137) Williams, P. D., *Security Studies. An Introduction*. London, New York: Routledge, 2008,

138) Witecka M., M*odel systemu bezpieczeństwa cyberprzestrzeni w Rzeczpospolitej Polskiej*, rozprawa doktorska, Akademia Obrony Narodowej, 2016,

139) Wojciechowski Z., *Wyzwania cyberbezpieczeństwa*, [w:] Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Gonciarski W., Woźniak J. (red.), Difin, Warszawa 2021,

140) Wojnowski M., *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*, Przegląd Bezpieczeństwa Wewnętrznego 16/17, 2017,

141) Wołowski F., Zawiła-Niedźwiecki J., *Bezpieczeństwo systemów informacyjnych*, Wydawnictwo edu-Libri, Warszawa, 2013,

142) Woźniak J., *Cyfryzacja gospodarki a zmiany w postrzeganiu i zapewnianiu bezpieczeństwa*, [w:] Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Gonciarski W., Woźniak J. (red.), Difin, Warszawa 2021,

143) Woźniak J., Zaskórski P., *Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej*, Ogólnopolska Konferencja Naukowa, „Nowoczesne koncepcje i metody zarządzania. Teoria i praktyka", WAT, Warszawa 2009,

144) Van Puyvelde D., Brantly A., *US National Cybersecurity International Politics, Concepts and Organization*, Routledge, 2019,

145) Zalewski S., *Strategia jako instrument bezpieczeństwa politycznego państwa*, DOCTRINA Studia Społeczno-Polityczne Nr 6, 2009, Akademia Podlaska, Siedlce 2009,

146) Zaskórski P. (red.), Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania, Wydawnictwo WAT, Warszawa 2011,

147) Zaskórski P., *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, WAT, Warszawa 2005,

148) Zaskórski P., *Systemy informacji menedżerskiej*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, Nr 1, Warszawa 2006,

149) Zaskórski P., *Zarządzanie zasobami informacyjnymi w firmie*, Biuletyn WAT, vol. LVII, nr 4, 2008,

150) Zaskórski P. *Informacyjna ciągłość działania determinantą bezpieczeństwa organizacji*, w: Nie-bezpieczny świat. Systemy. Informacja. Bezpieczeństwo, Akademia Obrony Narodowej, Warszawa 2015,

151) Zaskórski P., *Ewaluacja projektów*, Materiały konferencyjne Zarządzanie Projektami Informatycznymi, Warszawska Wyższa Szkoła Informatyki, Warszawa,

152) Zaskórski P., *Środowisko IT w zapewnianiu bezpieczeństwa organizacji rozproszonych*, [w:] Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej, Gonciarski W., Woźniak J. (red.), Difin, Warszawa 2021,
153) Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, nr 9, rok 7, 2013,
154) Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, Wydawnictwo edu-Libri, Warszawa, 2013,
155) Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013

Dokumenty strategiczne:

1) Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, 2013,
2) Doktryna Cyberbezpieczeństwa RP, BBN, 2015,
3) Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022 (2017),
4) Krajowy Plan Zarządzania Kryzysowego, cz. A, cz. B, RCB, 2017,
5) Narodowy Program Ochrony Infrastruktury Krytycznej, RCB, 2015, 2018, 2020
6) Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1 do Narodowy Program Ochrony Infrastruktury Krytycznej - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, RCB, 2015, 2018, 2020,
7) Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 - 2022 (2017),
8) Plan działań w zakresie zapewniania bezpieczeństwa cyberprzestrzeni RP (2015),
9) Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (2013),
10) Rządowy Program w zakresie Ochrony Cyberprzestrzeni RP na lata 2011-2016 (2010),
11) Strategia Bezpieczeństwa Narodowego RP, Kancelaria Prezydenta/Biuro Bezpieczeństwa Narodowego, BBN, 2014,
12) Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r.,

13) Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, BBN, 2013

Regulacje prawne:

1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. U. UE L 194/1,
2) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148,
3) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE,
4) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),
5) Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. Nr 83 poz. 542,
6) Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. 2010 Nr 83 poz. 541,
7) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2012 poz. 526 z późn. zmianami, Dz.U. 2017 poz. 2247,
8) Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz. U. poz. 1780,
9) Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz.U. poz. 1806,

10) Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz. U. poz. 2080,
11) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. 1997 poz. 883,
12) Ustawa z dnia 12 września 2002 r. o normalizacji, z późn. zmianami, Dz.U. 2015, poz. 1483,
13) Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. 2004 poz. 1800,
14) Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. 2007 poz. 590,
15) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565 z późn. zmianami, Dz.U. z 2020 r. poz. 346, 568, 695, 1517,
16) Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz. U. 2016 poz. 1579,
17) Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, z późn. zmianami, Dz.U. 2021, poz. 514, 925,
18) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018 poz. 1000,
19) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560

Raporty:

1) Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2021, NASK-PIB, 2022,
2) Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2020, NASK-PIB, 2021,
3) Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, NASK-PIB, 2020,
4) Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, NASK-PIB, 2019,
5) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 r., CSIRT-GOV ABW, 2022,
6) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r., CSIRT-GOV ABW, 2021,

7) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r., CSIRT-GOV ABW, 2020,
8) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r., CSIRT-GOV ABW, 2019,
9) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r., CSIRT-GOV ABW, 2018,
10) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r., CSIRT-GOV ABW, 2017,
11) Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r., CSIRT-GOV ABW, 2016,
12) Raport CERT Orange Polska za rok 2020, Orange Polska, 2020,
13) Raport CERT Orange Polska za rok 2019, Orange Polska, 2019,
14) Raport CERT Orange Polska za rok 2018, Orange Polska, 2018,
15) Raport PRC na zlecenie T-mobile, Badanie rynku cyberbezpieczeństwa w Polsce w 2017 roku w dużych i średnich firmach,
16) Raport Barometr cyberbezpieczeństwa. Rozwiązania chmurowe, KPMG, 2020

Normy:

1) PN-ISO/IEC 27000, Technologia informacyjna – Techniki zabezpieczeń – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia,
2) PN-ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji – Wymagania,
3) PN-ISO/IEC 27002 Praktyczne zasady zabezpieczenia informacji,
4) ISO/IEC 27005 Information security risk management,
5) ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications,
6) ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002,
7) ISO/IEC 27014 Governance of information security,
8) ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services,
9) ISO/IEC 27018 Code of practice for protection of personally identifiable information (IIP) in public clouds acting as IPP processors,

10) ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry,
11) ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity,
12) ISO/IEC 27032 Guidelines for cybersecurity,
13) ISO/IEC 27033-1 Network security. Overview and concepts,
14) ISO/IEC 27033-2 Network security. Guidelines for the design and implementation of network security,
15) ISO/IEC 27033-3 Network security. Reference network scenarios — Threats, design techniques and control issues,
16) ISO/IEC 27033-4 Network security. Securing communications between networks using security gateways — Risks, design techniques and control issues,
17) ISO/IEC 27033-5 Network security. Securing virtual private networks — Risks, design techniques and control issues,
18) ISO/IEC 27033-6 Network security, Securing access to IP wireless network,
19) ISO/IEC 27034-1 Application security. Overview and concepts,
20) ISO/IEC 27034-2 Application security. Organization normative Framework,
21) ISO/IEC 27034-3 Application security. Application security management process,
22) ISO/IEC 27034-5 Application security. Protocols and application security control data structure,
23) ISO/IEC 27034-6 Application security. Usecases,
24) ISO/IEC 27034-7 Application security. Certainty forecasting framework,
25) ISO/IEC 27035-1 Information security incident management. Principles of incident management,
26) ISO/IEC 27035-2 Information security incident management. Guidelines to plan and prepare for incident response,
27) ISO/IEC 27036-1 Information security in relations with suppliers. Overview and concepts,
28) ISO/IEC 27036-2 Information security in relations with suppliers. Requiremants,
29) ISO/IEC 27036-3 Information security in relations with suppliers. Information and Communication Technology Supply Chain Security Guidelines,
30) ISO/IEC 27036-4 Information security in relations with suppliers. Cloud service security guidelines,

31) PN-EN ISO/IEC 27037 Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych,
32) PN-EN ISO/IEC 27040 Bezpieczeństwo pamięci masowych / ISO/IEC 27040 Storage security,
33) ISO/IEC 20000-1:2011 Information technology - Service management – Part 1: Service management system requirements,
34) ISO/IEC 20000-1:2018 - Information technology - Service management - Part 1: Service management system requirements,
35) PN-EN ISO 20000-1:2014 Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania usługami,
36) ISO 22301, Societal security — Business continuity management systems — Requirements,
37) PN-EN ISO 22301:2014 Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania – Wymagania,
38) PN-EN ISO 22301:2020 Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania – Wymagania,
39) ISO 22316 Security and resilience — Organizational resilience — Principles and attributes,
40) ISO 28000:2007 Specification for security management systems for the supply chain,
41) ISO 28001:2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance,
42) Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0),
43) Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0),
44) Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0),
45) Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne (NSC 800-30 wer. 1.0),
46) Poradnik Planowania Awaryjnego (NSC 800-34 wer. 1.0),
47) Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0),

48) Zarządzanie ryzykiem bezpieczeństwa informacji (NSC 800-39 wer. 1.0),
49) Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0),
50) Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0),
51) Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0),
52) Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0),
53) Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0),
54) Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część II (NSC 800-60 cz. 2 wer. 1.0),
55) Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer.1.0),
56) Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0),
57) Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (NSC 7298 wer. 1.0),
58) Standardy Cyberbezpieczeństwa Chmur Obliczeniowych,
59) FIPS PUB 199 Standardy Kategoryzacji Bezpieczeństwa,
60) FIPS PUB 200 Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych,
61) NIST SP 800-18 rev. 1 Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych,
62) NIST SP 800-30 rev. 1 Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne,
63) SP 800-37, Rev. 2 Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu,
64) NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View (March 2011) Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informatycznego,
65) NIST SP 800-46 rev. 2 Przewodnik po telepracy w podmiocie publicznym. Zdalny dostęp i bezpieczeństwo używania prywatnych urządzeń (BYOD),

66) NIST SP 800-53, Rev. 5 Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji,
67) NIST SP 800-53B Zabezpieczenia bazowe systemów informatycznych oraz organizacji,
68) NIST SP 800-60 vol. 1, Rev. 1, vol. 2, Rev. 1 Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego,
69) NSC 800-61, Rev. 2 Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego,
70) NIST SP 800-207Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”

Netografia:

1) https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [dostęp 05.02.2018],
2) https://www.cybsecurity.org/pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa,
3) https://www.gov.pl/web/cyfryzacja [dostęp 12.07.2020],
4) https://www.cyberdefence24.pl [dostęp 20.03.2021, 30.10.2022],
5) https://ISO.org [dostęp 10.03.2020],
6) https://www.axelos.com/resilia [dostęp 20.05.2021],
7) https://www.axelos.com/best-practice-solutions/itil [dostęp 20.05.2021],
8) https://www.itgovernanceusa.com/resilia [dostęp 20.05.2021],
9) https://www.itgovernance.eu/en-ie/resilia-ie [dostęp 20.05.2021],
10) https://www.itgovernance.co.uk/itil [dostęp 20.05.2021],
11) https://www.itgovernance.eu/en-ie/shop/product/iso-iec-20000-1-2011-standard [dostęp 20.05.2021],
12) https://www.itgovernance.eu/en-ie/shop/product/iso-iec-20000-1-2018-standard [dostęp 20.05.2021],
13) https://www.itgovernanceusa.com/iso20000 [dostęp 20.05.2021],
14) https://www.itgovernanceusa.com/iso27001 [dostęp 20.05.2021],
15) https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber [dostęp 20.09.2022]

WYKAZ TABEL

WYKAZ RYSUNKÓW

WYKAZ ZAŁĄCZNIKÓW

1. Załącznik nr 1. Arkusz kwestionariusza wywiadu eksperckiego,
2. Załącznik nr 2. Zestawienia zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze

WYKAZ SUPLEMENTÓW

1. Suplement nr 1. Załącznik nr 1. Arkusz kwestionariusza wywiadu eksperckiego,
2. Suplement nr 2. Załącznik nr 2. Zestawienia zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze,
3. Suplement nr 3. Zbiór arkuszy kwestionariusza wywiadu eksperckiego z odpowiedziami respondentów

ZAŁĄCZNIKI

1. Załącznik nr 1. Arkusz kwestionariusza wywiadu eksperckiego

Szanowna Pani/Szanowny Panie,

Realizuję doktorat w Wojskowej Akademii Technicznej, którego przedmiotem jest opracowanie propozycji udoskonalenia krajowego systemu cyberbezpieczeństwa, ustanowionego na mocy ustawy o krajowym systemie cyberbezpieczeństwa. Temat doktoratu brzmi: „Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej".

Niniejszym zwracam się do Pani/Pana, jako eksperta w przedmiotowej problematyce, z prośbą o przedstawienie swojego stanowiska, co do podejmowanych w badaniu kwestii, dotyczących doskonalenia krajowego systemu cyberbezpieczeństwa RP. Pani/Pana zdanie jest niezmiernie ważne dla oceny stanu aktualnego i wypracowania nowych propozycji rozwiązań doskonalących krajowy system cyberbezpieczeństwa RP.

Realizowany doktorat i prowadzone badania dotyczą kilku obszarów, które uznałem za ważne dla skutecznego zarządzania cyberbezpieczeństwem i zapewnienia odpowiedniego poziomu bezpieczeństwa państwa. Problematyka doktoratu obejmuje: rozwiązania organizacji zarządzania cyberbezpieczeństwem na poziomie krajowym, efektywność struktur i relacji operacyjnych w systemie cyberbezpieczeństwa, dobór podmiotów krajowego systemu cyberbezpieczeństwa, bezpieczeństwo teleinformatyczne usług, systemów i podmiotów systemu cyberbezpieczeństwa RP.

Oczywistym jest, że krajowy system cyberbezpieczeństwa może być doskonalony w wielu jego obszarach, jednakże zakres prowadzonego przeze mnie badania obejmuje wyżej zdefiniowane obszary i na nich się koncentruje.

Problematyka projektu badawczego została zdefiniowana w roku 2019, a ostateczny zakres podejmowanych zagadnień i kwestii dotyczących obszarów doskonalenia krajowego systemu cyberbezpieczeństwa RP został zdefiniowany w roku 2020. Z powodu rozpoczęcia w 2020 roku nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która mogłaby istotnie wpłynąć na ustanowione ustawą rozwiązania systemu cyberbezpieczeństwa, jak też na dotychczas zdefiniowaną problematykę doktoratu i propozycje doskonalenia systemu cyberbezpieczeństwa, realizacja badań została odroczona w czasie. Proces nowelizacji ustawy nie został dotychczas zakończony. Badania muszą zostać przeprowadzone w aktualnym czasie, w krótkim terminie – do 30.06.2022 r.

Bardzo proszę o przedstawienie swojego stanowiska, co do podejmowanej w badaniu problematyki.

Arkusz wywiadu eksperckiego składa się z dwóch części – A i B.

W części pierwszej (A) – wywiadzie eksperckim, zawarte zostały pytania badawcze, dotyczące przedmiotu i zakresu badania. Odpowiedzi na postawione pytania zostaną wykorzystane do oceny stanu aktualnego i wypracowania nowych propozycji rozwiązań. Odpowiedzi na pytania będą przetwarzane zbiorczo dla uzyskania uogólnionych wniosków.

W części drugiej (B) – metryce arkusza badania, pozyskiwane są dane dotyczące kompetencji eksperckich i doświadczenia zawodowego w zakresie dotyczącym przedmiotu i zakresu badania.

Badanie jest badaniem eksperckim, jest więc imienne. Przetwarzanie pozyskanych danych będzie anonimowe, żadne dane identyfikujące lub mogące identyfikować Panią/Pana, jako respondenta niniejszego badania, nie będą przetwarzane, ani udostępniane. Wyniki badania – uzyskane odpowiedzi – będą przetwarzane zbiorczo dla uzyskania uogólnionych wniosków.

W przypadku konieczności przeprowadzenia pogłębionych wywiadów z wybranymi ekspertami-respondentami chciałbym mieć możliwość bezpośredniego skontaktowania się z państwem. Jeśli wyraża Pan(i) zgodę na kontakt bezpośredni, proszę o podanie danych kontaktowych wraz z przekazywaniem wypełnionego arkusza badania.

Dziękuję za otwartość, poświęcony czas i przedstawienie swojego stanowiska, co do podejmowanej w badaniu problematyki.

Proszę o przesłanie wypełnionego arkusza badania najpóźniej do 30.06.2022 r. na adres poczty elektronicznej:

1. grzegorz.makosa@wat.edu.pl lub
2. gmakosa@wp.pl

Z poważaniem

mgr Grzegorz Mąkosa

Warszawa, czerwiec 2022 r.

Arkusz wywiadu eksperckiego

PROJEKT BADAWCZY
„Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej”

A. Pytania wywiadu eksperckiego

1. Organizacja cyberbezpieczeństwa na poziomie krajowym

1.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**” w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

1.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

*Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w **systemie zarządzania kryzysowego** (ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.*

Proszę wstawić znak „**x**” w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

1.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowane w pkt. 1.2. powyżej zorganizowanie, planowanie i dokumentowanie zarządzania cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione, jako:

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	**Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**
1	funkcjonujące niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego					
2	funkcjonujące równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim połączone					
3	w pełni zintegrowane z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa					

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2. Efektywność struktur i relacji operacyjnych w systemie cyberbezpieczeństwa

2.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz,

opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2.4. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowane w pkt. 2.3. powyżej zaangażowanie RCB w zarządzanie cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób:

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym					
2	RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego					
3	RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa					

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2.5. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone,

zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Proszę wstawić znak „**x**” w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

2.6. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych.

Proszę wstawić znak „**x**” w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

3. Podmioty krajowego systemu cyberbezpieczeństwa

3.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) są właściwie zdefiniowane, co zapewnia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

3.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Krajowy system cyberbezpieczeństwa powinien obejmować znacznie szerszy katalog typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

3.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Krajowy system cyberbezpieczeństwa powinien obejmować najszerszy możliwy katalog typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

3.4. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowany w pkt. 3.3. powyżej najszerszy możliwy katalog typów podmiotów krajowego systemu cyberbezpieczeństwa, jako mających odpowiednio duży wpływ na sferę administracyjno-społeczno-gospodarczą i bezpieczeństwa państwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinien obejmować podmioty typu:

Proszę wstawić znak „x" w odpowiednim polu.

Lp.	Proponowane typy podmiotów krajowego systemu cyberbezpieczeństwa RP	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	Energetyka					
2	Łączność (usługi pocztowe i kurierskie)					
3	Telekomunikacja i sieci teleinformatyczne					
4	Bankowość i infrastruktura rynków finansowych					
5	Sektor żywnościowy					
6	Wodociągi i kanalizacja					
7	Ochrona zdrowia					
8	Transport					
9	Ratownictwo					
10	Sektor chemiczny					
11	Przemysł / Produkcja					
12	Handel					
13	Usługi					
14	Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki					
15	Instytucje urzędów centralnych					
16	Sektor finansów publicznych					
17	Sektor usług komunalnych					
18	Sektor usług publicznych					
19	Sektor kosmiczny					
20	Nauka i szkolnictwo wyższe					
21	Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)					
22	Media (TV, radio, portale informacyjne)					
23	Infrastruktura cyfrowa (DNS, IXP, TLD)					
24	Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**)**					
25	Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)					
26	Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach					
27	Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja)					
28	Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa					
29	Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego					

30	Inny (jaki?) …					
31	Inny (jaki?) …					
32	Inny (jaki?) …					

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

4. Bezpieczeństwo teleinformatyczne usług, systemów i podmiotów systemu cyberbezpieczeństwa RP

4.1. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

4.2. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

4.3. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób, gdyby miały być na nowo ustawowo ustanowione, to powinny być oparte o:

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Standardy bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa RP	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE
1	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301)					

2	Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)					
3	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)					
4	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.)					
5	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301					
6	Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania					
7	Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST)					
8	Standardy ITIL, RESILIA					
9	Dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania					
10	Inne (jakie?) …					

Proszę o przedstawienie uzasadnienia odpowiedzi i stanowiska wobec przedstawionego zagadnienia:

Uzasadnienie odpowiedzi:

B. Metryka – dane dotyczące respondenta

1. Dane identyfikujące eksperta – respondenta

Proszę podać dane identyfikacyjne:

1.1. Imię i nazwisko: . . . . . .

Badanie eksperckie jest imienne. Dane osobowe w dalszym przetwarzaniu zostaną poddane pseudonimizacji, nie będą przetwarzane ani udostępniane, nie zostaną ujawnione. W opracowywaniu wyników będą stosowane określenia typu: „respondent nr" lub „respondent nr, inicjały".

1.2. Dane kontaktowe (email, nr tel.): . . . . . .

Dla bezpośredniego skontaktowania się w celu przeprowadzenia pogłębionych wywiadów z wybranymi ekspertami-respondentami.

2. Doświadczenie eksperckie i zawodowe na stanowiskach poziomów struktury organizacyjnej

2.1. Proszę wskazać długość łącznego doświadczenia zawodowego na zajmowanych stanowiskach różnych poziomów struktury organizacyjnej w swoim doświadczeniu zawodowym.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze".*

2.2. Proszę wskazać, czy realizacja aktywności na wskazanych stanowiskach jest wykonywana aktualnie.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Wykonywane aktualnie".*

a. Pracownik podmiotów gospodarczych, administracji, organizacji pozarządowych, itp.

Doświadczenie na stanowiskach: pracownik podmiotów gospodarczych, administracji, organizacji pozarządowych, itp.		**Długość łącznego doświadczenia we wskazanym obszarze**				**Wykonywane aktualnie**
Lp	**Zajmowane stanowisko**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	**Aktualne**
1	Menedżer najwyższego szczebla (członek zarządu/ dyrektor generalny/ właściciel)					
2	Menedżer wyższego szczebla (dyrektor komórki organizacyjnej wyższego szczebla - departamentu/działu)					
3	Manager średniego szczebla (kierownik komórki organizacyjnej średniego szczebla)					
4	Ekspert					
5	Specjalista					

b. Pracownik sektora nauki i szkolnictwa wyższego – pracownik naukowy, naukowo-dydaktyczny, dydaktyczny

Tytuł lub stopień naukowy					
Profesor zw.	Profesor uczelni	Doktor hab.	Doktor	Doktorant (Mgr)	Mgr / Mgr inż.

Doświadczenie na stanowiskach: pracownik naukowy, naukowo-dydaktyczny, dydaktyczny		**Długość łącznego doświadczenia we wskazanym obszarze**				**Wykonywane aktualnie**
Lp	**Zajmowane stanowisko**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	**Aktualne**
1	Profesor					
2	Adiunkt					
3	Docent					
4	Asystent					
5	St. Wykładowca, Wykładowca					

3. Doświadczenie zawodowe wg własności podmiotów

3.1. Proszę wskazać dominujące łączne doświadczenie zawodowe w podmiotach, w zależności od ich własności.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze" i kolumny „Wykonywane aktualnie".*

Doświadczenie zawodowe wg własności podmiotów		**Długość łącznego doświadczenia we wskazanym obszarze**				**Wykonywane aktualne**
Lp	**Doświadczenie zawodowe w podmiotach**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	
1	Podmioty z całkowitym lub większościowym kapitałem (właścicielstwem) polskim					
2	Podmioty z całkowitym lub większościowym kapitałem (właścicielstwem) zagranicznym					

4. Status zaangażowania w realizację zapewnienia zgodności z wymaganiami prawa w zakresie zagadnień organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa danych, informacji, systemów teleinformatycznych i podmiotów.

4.1. Proszę wskazać stopień merytorycznego zaangażowania w realizację rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa, wymaganych na mocy przepisów prawa, m.in. ustaw: o krajowym systemie cyberbezpieczeństwa, o zarządzaniu kryzysowym, o informatyzacji podmiotów realizujących zadania publiczne, o działaniach antyterrorystycznych, RODO i innych regulacji, w tym branżowych i sektorowych.

Proszę wstawić odpowiednią cyfrę (1-5) we właściwych polach kolumny „Poziom zaangażowania", gdzie: 5 – bardzo wysoki, 4 – wysoki, 3 – średni, 2 – niski, 1 - bardzo niski lub brak.

4.2. Proszę wskazać długość łącznego doświadczenia w realizacji zagadnień związanych z wdrażaniem, utrzymaniem i zapewnieniem zgodności rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa z ww. przepisami prawa.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze".*

4.3. Proszę wskazać, czy realizacja zagadnień związanych z wdrażaniem, utrzymaniem i zapewnieniem zgodności rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa z ww. przepisami prawa jest wykonywana aktualnie.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Wykonywane aktualnie".*

Zaangażowanie w realizację rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa		**Poziom zaangażowania**	**Długość łącznego doświadczenia we wskazanym obszarze**				**Wykonywane aktualne**
Lp	**Realizacja rozwiązań bezpieczeństwa**	**(1-5)**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	
1	Rozwiązania **techniczne** bezpieczeństwa - systemy teleinformatyczne IT/TI/ICT/OT/Telekomunikacja						
2	Rozwiązania **techniczne** bezpieczeństwa - systemy teleinformatyczne cyberbezpieczeństwa (np. SIEM, SOAR, PIM/PAM, IAM, DLP, AntiAPT, AV, MFA, NetFlow, AntiDoS, itp.)						
3	Rozwiązania **organizacyjne** ochrony i bezpieczeństwa danych, informacji, systemów teleinformatycznych i podmiotów						

5. **Status zaangażowania w realizację zapewnienia zgodności z wymaganiami norm, metodyk, standardów, wytycznych branżowych i administracyjnych w zakresie zagadnień organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa danych, informacji, systemów teleinformatycznych i podmiotów.**

5.1. Proszę wskazać stopień merytorycznego zaangażowania w realizację rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa, wymaganych na mocy norm, metodyk, standardów, wytycznych branżowych i administracyjnych, dot. m.in.: bezpieczeństwa danych, informacji i systemów teleinformatycznych, ciągłości działania, ryzyka, jakości, usług IT, itp.

Proszę wstawić odpowiednią cyfrę (1-5) we właściwych polach kolumny „Poziom zaangażowania", gdzie: 5 – bardzo wysoki, 4 – wysoki, 3 – średni, 2 – niski, 1 - bardzo niski lub brak.

5.2. Proszę wskazać długość łącznego doświadczenia w realizacji zagadnień związanych z wdrażaniem, utrzymaniem i zapewnieniem zgodności rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa z ww. normami, metodykami, standardami, wytycznymi branżowymi i administracyjnymi.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze".*

5.3. Proszę wskazać, czy realizacja zagadnień związanych z wdrażaniem, utrzymaniem i zapewnieniem zgodności rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa z ww. normami, metodykami, standardami, wytycznymi branżowymi i administracyjnymi jest wykonywana aktualnie.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Wykonywane aktualnie".*

Zaangażowanie w realizację rozwiązań organizacyjnych i technicznych bezpieczeństwa i cyberbezpieczeństwa		**Poziom zaangażowania**	**Długość łącznego doświadczenia we wskazanym obszarze**				**Wykonywane aktualne**
Lp	**Realizacja rozwiązań bezpieczeństwa**	**(1-5)**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	
1	Rozwiązania **techniczne** bezpieczeństwa - systemy teleinformatyczne IT/TI/ICT/OT/Telekomunikacja						
2	Rozwiązania **techniczne** bezpieczeństwa - systemy teleinformatyczne cyberbezpieczeństwa (np. SIEM, SOAR, PIM/PAM, IAM, DLP, AntiAPT, AV, MFA, NetFlow, AntiDoS, itp.)						
3	Rozwiązania **organizacyjne** ochrony i bezpieczeństwa danych, informacji, systemów teleinformatycznych i podmiotów						

6. Obszar merytoryczny kompetencji eksperckich i doświadczenie zawodowe

6.1. Proszę wskazać poziom kompetencji w swoich eksperckich obszarach merytorycznych, związanych z bezpieczeństwem i cyberbezpieczeństwem danych, informacji, systemów teleinformatycznych i podmiotów.

Proszę wstawić odpowiednią cyfrę (1-5) we właściwych polach kolumny „Poziom kompetencji", gdzie: 5 – bardzo wysoki, 4 – wysoki, 3 – średni, 2 – niski, 1 - bardzo niski lub brak.

6.2. Proszę wskazać długość łącznego doświadczenia zawodowego we wskazanych eksperckich obszarach merytorycznych.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze".*

6.3. Proszę wskazać, czy realizacja aktywności we wskazanych eksperckich obszarach merytorycznych jest wykonywana aktualnie.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Wykonywane aktualnie".*

Obszar merytoryczny kompetencji eksperckich		Poziom kompetencji	Długość łącznego doświadczenia we wskazanym obszarze				Wykonywane aktualnie
Lp	**Obszar kompetencji eksperckich**	**(1-5)**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	**Aktualne**
1	Systemy teleinformatyczne IT/TI/ICT/Telekomunikacja						
2	Systemy teleinformatyczne OT						
3	Systemy teleinformatyczne cyberbezpieczeństwa (np. SIEM, SOAR, PIM/PAM, IAM, DLP, AntiAPT, AV, MFA, NetFlow, Anti-DoS, itp.)						
4	Ciągłość działania						
5	Zarządzanie kryzysowe						
6	Aspekty organizacyjne ochrony i bezpieczeństwa danych, informacji i systemów teleinformatycznych						
7	Prawo związane z ochroną i bezpieczeństwem danych, informacji i systemów teleinformatycznych, cyberbezpieczeństwem, informatyzacją, zarządzaniem kryzysowym, krajowym systemem cyberbezpieczeństwa, itp.						
8	Normy, standardy, metodyki dot. jakości, bezpieczeństwa, ciągłości działania i ryzyka informacji, procesów i systemów IT/TI/ICT/OT/Telekomunikacji						

7. Obszar branżowy kompetencji eksperckich i doświadczenie zawodowe

7.1. Proszę wskazać poziom kompetencji branżowych (znajomość branży) w swoich eksperckich obszarach branżowych, związanych z bezpieczeństwem i cyberbezpieczeństwem danych, informacji, systemów teleinformatycznych i podmiotów.

Proszę wstawić odpowiednią cyfrę (1-5) we właściwych polach kolumny „Poziom kompetencji", gdzie: 5 – bardzo wysoki, 4 – wysoki, 3 – średni, 2 – niski, 1 - bardzo niski lub brak.

7.2. Proszę wskazać, czy obszar eksperckich kompetencji branżowych obejmuje zagadnienia dotyczące operatorów infrastruktury krytycznej (OIK) i operatorów usług kluczowych (OUK).

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Typ podmiotu".*

7.3. Proszę wskazać długość łącznego doświadczenia zawodowego we wskazanych eksperckich obszarach branżowych.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Długość łącznego doświadczenia we wskazanym obszarze".*

7.4. Proszę wskazać, czy realizacja aktywności we wskazanych eksperckich obszarach branżowych jest wykonywana aktualnie.

*Proszę wstawić znak „**x**" w odpowiednim polu kolumny „Wykonywane aktualnie".*

Obszar branżowy kompetencji eksperckich		Typ podmiotu	Poziom kompetencji	Długość łącznego doświadczenia we wskazanym obszarze				Wykonywane aktualnie
Lp.	**Obszar branżowy kompetencji eksperckich**	**OIK, OUK**	**(1-5))**	**do 3 lat**	**3-5 lat**	**5-10 lat**	**> 10 lat**	**Aktualne**
1	Energetyka							
2	Łączność (usługi pocztowe i kurierskie)							
3	Telekomunikacja i sieci teleinformatyczne							

4	Bankowość i infrastruktura rynków finansowych							
5	Sektor żywnościowy							
6	Wodociągi i kanalizacja							
7	Ochrona zdrowia							
8	Transport							
9	Ratownictwo							
10	Sektor chemiczny							
11	Przemysł / Produkcja							
12	Handel							
13	Usługi							
14	Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki							
15	Instytucje urzędów centralnych							
16	Sektor finansów publicznych							
17	Sektor usług komunalnych							
18	Sektor usług publicznych							
19	Sektor kosmiczny							
20	Nauka i szkolnictwo wyższe							
21	Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)							
22	Media (TV, radio, portale informacyjne)							
23	Infrastruktura cyfrowa (DNS, IXP, TLD)							
24	Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**)**							
25	Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)							
26	Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach							
27	Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja)							
28	Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa							
29	Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego							
30	Inny (jaki?) …							

Szanowna Pani/Szanowny Panie,

Dziękuję za przedstawienie swojego stanowiska, co do podejmowanych w badaniu kwestii.

W przypadku konieczności przeprowadzenia pogłębionych wywiadów z wybranymi ekspertami-respondentami pozwolę sobie na bezpośredni kontakt z Panią/Panem.

Z poważaniem

mgr Grzegorz Mąkosa

2. Załącznik nr 2. Zestawienie zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze

Arkusz wywiadu eksperckiego

PROJEKT BADAWCZY

„Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej”

A. Pytania wywiadu eksperckiego

Legenda - Obszar: A – administracja, B - biznes, I – instytucja, U - uczelnia

1. Organizacja cyberbezpieczeństwa na poziomie krajowym

1.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Zarządzanie cyberbezpieczeństwem RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	Respon-dent	Obszar	Zdecy-dowanie TAK	Raczej TAK	Brak zda-nia	Raczej NIE	Zdecy-dowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Ogólne założenia KSC są słuszne, natomiast wykonanie jest dalekie od ideału. Przede wszystkim brakuje wiedzy po stronie firm świadczących usługi kluczowe, a także zapewnienia budżetu dla rozwiązań w zakresie cyberbezpieczeństwa, zarówno technicznych, jak i usługowych
2	2UM	B				x		Wykonywane przeze mnie audyty w sektorze publicznym wskazują, że z nielicznymi wyjątkami faktyczny stan bezpieczeństwa i świadomość kadry kierowniczej, a w niektórych przypadkach także personelu IT jest niezadawalająca.
3	3BS	B				x		W większości obszarów cyberbezpieczeństwo opiera się na biurokracji, a nie na rzeczywistych zdolnościach cyberobrony.
4	4SK	U			x			W stwierdzeniu powiązano jednocześnie wszystkie szczeble administracji oraz wiele zmiennych warunkujących ocenę efektywności. Nie jestem w stanie odpowiedzieć na to pytanie
5	5MK	B, U				x		Sztywne określenie zakresu kompetencji 3 krajowych zespołów CSIRT, przy braku podmiotu systemowo odpowiedzialnego za przeciwdziałanie dezinformacji i działaniom hybrydowym, powoduje, że system jest dysfunkcyjny. Przykład: podmiana treści na lokalnym mazurskim portalu godzi w dobre imię NATO. Nie może się tym zająć NCBC ani ABW, bo zgodnie z ustawą to domena NASKu. Ale dopóki właściciel portalu tego nie zgłosi, to NASK nie może podjąć działań. I tak dalej...
6	6ST	I, U	x					
7	7KG	B		x				Ustawa o krajowym systemie cyberbezpieczeństwa jest pierwszym aktem prawnym, który w całości skupia się na zagadnieniach dotyczących cyberbezpieczeństwa. Wprowadzenie w tym przepisie kar finansowych i administracyjnych za niestosowanie jej zapisów oraz obowiązkowy proces audytu i kontroli (np. przez organ właściwym) niejako wymusza na pomiotach jej stosowanie. Odesłanie w przepisach wykonawczych do uznanych standardów (ISO27001, ISO22301) powoduje, że organizacja cyberbezpieczeństwa pod względem procesowym, dokumentacyjnym, planistycznym i operacyjnym ma szansę zapewnić, że efektywność tego systemu a tym samym odpowiedni do oszacowanych zagrożeń. poziom bezpieczeństwa państwa.
8	8DP	A	x					Obecnie przyjęte akty prawne pozwalają na zapewnienie efektywnego funkcjonowania krajowego systemu cyberbezpieczeństwa. Należy brać pod uwagę konieczność regularnej weryfikacji, czy przyjęte przepisy we właściwy sposób określają sposób funkcjonowania systemu cyberbezpieczeństwa w dynamicznie zmieniającym się obszarze cyberprzestrzeni.
9	9KM	B					x	KRI funkcjonuje od lat, a prawie nikt go nie ma.

10	10BD	A		x				USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa dostatecznie reguluje powyższe kwestie. Ponadto Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 określiła strategiczne cele oraz odpowiednie środki polityczne i regulacyjne, które trzeba zrealizować, aby systemy informacyjne, operatorzy usług kluczowych, operatorzy infrastruktury krytycznej, dostawcy usług cyfrowych oraz administracja publiczna były odporne na cyberzagrożenia.
11	11KP	B				x		Choć niewątpliwie temat cyberbezpieczeństwa został zauważony w sferze publicznej, to nadal jednak, patrząc chociażby na jego efektywność rozumianą jako stosowanie się do wymogów bezpieczeństwa przez pracowników poszczególnych resortów, a przede wszystkim samych polityków, wydaje się, że poszczególne zapisy i/lub polityki pozostają jedynie w sferze teoretycznej.
12	12PM	B					x	System zarządzania Cyberbezpieczeństwem moim zdaniem przypomina szlacheckie „pospolite ruszenie”. Niby są uznawane certyfikaty, ale w praktyce nie mają żadnego znaczenia w tym systemie. W praktyce każda firma jest pozostawiona sobie sama, a tym bardziej osoby prywatne. Policja w praktyce nie ściga fishingu, wyłudzeń. Nie widać, aby osoby odpowiedzialne za organizację tego systemu rozumiały różnicę między np. specjalistą od testów penetracyjnych, a menadżerem bezpieczeństwa informacji (a to jest odpowiednik roli komandosa i osoby kierującej siłami szybkiego reagowania.
13	13RP	I		x				Zarządzanie cyberbezpieczeństwem RP jest dobrze zorganizowane pod względem procesowym, dokumentacyjnym oraz planistycznym i operacyjnym, i zapewnienia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.
14	14CT	B				x		Można długo pisać na ten temat. Brak świadomości, brak środków, lekceważenie obowiązków, brak pracy „u podstaw” – to wszystko składa się na moją negatywną ocenę.
15	15MB	A			x			Jeszcze nie ma wyników ogólnokrajowych ćwiczeń a dodatkowo Polska nie była poddana pod zmasowany atak hakerów
16	16KR	B				x		<u>Wady systemowe:</u> Niejednolite podejście sektorowe Brak odpowiedzialności osobistej kierowników jednostek OUK Brak skuteczności w egzekwowaniu wymagań wobec OUK Kompletny brak egzekwowania wymagań dla dostawców usług dla OUK Brak jednoznacznych wymagań metodycznych dla audytu systemów informacyjnych
17	17MM	I				x		Zarządzanie cyberbezpieczeństwem jest iluzoryczne.
18	18WM	U	x					Polskie rozwiązania implementują założenia Dyrektywy NIS co jest dobrym kierunkiem w obszarze unifikacji działań cyberprzestrzeni UE.
19	19DJ	A			x			Poziom zorganizowania zarządzania cyberbezpieczeństwem w Polsce różni się w zależności od poziomu organizacyjnego i aspektu działania. Spora część zadań (np. obowiązki

								dokumentacyjne, sprawozdawczość, procesy) jest uregulowana na poziomie ustawy co upraszcza porównywanie wyników. Część zadań (np. planowanie na poziomie centralnym) jest przedmiotem dokumentu o charakterze strategicznym, przyjętego przez Radę Ministrów. Inaczej sprawa wygląda na poziomie samorządu (gdzie podmioty różnią się poziomem sprawności realizacji zadań ustawowych). Podobnie z firmami prywatnymi – ich poziom bezpieczeństwa zależy od działań kierownictwa, środowiska regulacyjnego, presji klientów etc.
20	20MA	B					x	Zarządzanie cyberbezpieczeństwem w formie obecnej wydaje się koncentrować na praktykach spełniania wymogów zgodności oraz prezentowania wyników operacyjnych w ujęciu ilościowym a nie jakościowym. Nie istnieją sektorowe czy regionalne „profile bezpieczeństwa" używające jakiejkolwiek metodologii (np. NIST Cybersecurity Framework), brak jest komunikacji ryzyk i zagrożeń, alerty dotyczące konkretnych operacji są najczęściej kierowane do niewłaściwych osób, z nieadekwatnym do komunikatu treścią (np. przekazywanie w ogólnym komunikacie danych IOC, brak koordynacji alertów i informacji wywiadu cybernetycznego na poziomie jednostek, ciągła rywalizacja zespołów CERT/CSIRT zamiast współpracy i współdzielenia informacji. System głównie funkcjonuje na zasadzie realizacji wymaganych prawem dokumentacji oraz współpracy opartej na relacjach osobistych a nie służbowych.
21	21DM	B, U		x				Istnieje kilka przepisów prawa, które są rozłączne zarówno na poziomie centralnym jak oddzielne są zespoły odpowiedzialne za ich realizację każdy oddzielnie realizuje wymagania jednak nigdy nie wystąpiła sytuacja wymagająca koordynacji realnych działań nawet ćwiczenia i gry sztabowe każdy z podmiotów realizuje oddzielnie. Są to: RCB dla IK i zarządzania kryzysowego, ABW dla działań antyterrorystycznych, Cert sektorowy dla dyrektywy NIS i ustawy KSC, KPRM dla ustawy "o stanach wyjątkowych"
22	22SP	B		x				
23	23SW	I, U					x	Realizacja zadań „właściwej władzy" poprzez każdego z ministrów odrębnie nie zapewnia spójności działań.
24	24MA	I		x				Krajowy system cyberbezpieczeństwa funkcjonuje od 4 lat. Szereg doświadczeń zostało zebranych. Procesy zarządzania wymagają doskonalenia. Szczególnie w sytuacji nadchodzącej zmiany, którą wniesie dyrektywa NIS2.
25	25KD	I				x		System jest tworzony, na obecnym etapie nie stanowi elementu jednolitego systemu bezpieczeństwa.
26	26SP	B					x	Bezpieczeństwo jest drogie i wymaga kadr, których brakuje i dlatego stosowane jest punktowo. Im ważniejsza instytucja, większy budżet czy po prostu większą świadomość to system działa lepiej. Jednak w skali całego kraju jeszcze wiele się musi zmienić, aby zadziałał. Ważne lokalnie, choć małe podmioty kierują się kosztami, bo nikt nie chce

								kupić wody czy prądu drożej z uwagi na jakieś tam bezpieczeństwo. Kryterium jest koszt dla licznego grona bardziej ubogich niż zapewnienie ciągłości dostaw w obliczu cyberataków.
27	27KA	B				x		W każdej z wymienionych kategorii widać bardzo wyraźnie, że występują istotne braki. Ustawa o KSC jest pierwszą próba systemowego wymuszenia wprowadzenia określonego ładu w obszarze cyber, jednakże wieloletnich zaniedbań nie da się skutecznie naprawić w krótkim okresie i bez dostatecznych nakładów finansowych zarówno na technikę jak i na budowanie świadomości (na wszystkich szczeblach). Trudno jest nie zauważyć braku podstawowych środków łączności służb, które byłyby kompatybilne i pozwalały na interoperacyjność. Zatem nie dziwi niedostatek sił, środków i podbudowy planistycznej w obszarze cyber. Wydarzenia ostatnich miesięcy (granica z Białorusią, wojna w Ukrainie) ewidentnie tę sytuację obnażają. Są jednocześnie nadzieją na uruchomienie procesów decyzyjnych i idących za tym działań i nakładów finansowych.
28	28RM	U					x	Nie ma możliwości opisania w kilku zdaniach, dlaczego model regulacyjny wprowadzony w Polsce jest zły. Zresztą PL to jedyny znany mi przykład państwa członkowskiego, w którym wyznaczono 11 organów właściwych za obszar cyberbezpieczeństwa, a jednocześnie nie ma ani jednego organu, który potrafi ten obszar skutecznie nadzorować i koordynować.
29	29GW	B				x		Moim zdaniem brak jest wsparcia dla działań wdrożeniowych zagadnienia cyberbezpieczeństwa, realizowane są działania kontrolne, typu audyty w ramach programu Cyfrowa Gmina.
30	30RT	B, U					x	Nie jest w ogóle zorganizowane na poziomie operacyjnym. Nie podejmowane są działania w celu synchronizacji działań dla wszystkich jednostek, w sytuacji zagrożenia cyberatakiem terrorystycznym, nawet nie ma procedur kontaktowania się. Nie odbywają się, co powinno nastąpić w ślad za uregulowaniem planu ogólnokrajowego, żadne ćwiczenia operacyjne w ramach CERT, pomiędzy wymienionymi jednostkami. Najważniejsze to poziom resortowo - samorządowy (np. ministerstwo energetyki i sołectwo). To pkt wyjścia planu.
31	31BC	A				x		Brakuje obligatoryjnego powołania pełnomocnika ds. cyberbezpieczeństwa w KAŻDEJ instytucji.
32	32KW	B				x		w mojej ocenie poziom regionalny w zasadzie nie funkcjonuje. Ustawa o Krajowym Systemie Cyberbezpieczeństwa stoi w sprzeczności z Ustawą o Zarządzaniu Kryzysowym (procesy vs. obiekty). System S46 (potrzebny i niezbędny do szybkiej wymiany informacji) został zaprojektowany w sposób uwłaczający standardom architektonicznym. Nie istnieje efektywne współdzielenie informacji o IoC pomiędzy wszystkimi interesariuszami (jeżeli masz IK to otrzymasz informacje o IoC z CSIRT.GOV, a jeżeli jesteś „tylko” OUK, to już nie). Brak współpracy pomiędzy CSIRT’ami. Jakiś podmiot

								merytoryczny i jednocześnie operacyjny musi realizować efektywny nadzór nad działaniem wszystkich.
33	33MM	B, U			x			wstawiłem „brak zdania”, ponieważ moim zdaniem połączenie wszystkich poziomów w jednym pytaniu nie daje szansy na jasną odpowiedź. W skrócie – na poziomie krajowym „Raczej TAK”, na pozostałych „Raczej NIE”
34	34RA	B					x	brak lokalnego wsparcia cybersecurity w gminach i podobnych jednostkach, nawet wsparcie IT jest problemem. Program Cyfrowa Gmina spowodował wzmożone zakupy sprzętu Cisco, niewiele więcej.
35	35KM	B, U		x				Zadania na poziomie krajowym są skuteczne natomiast w obszarze sektorowym i samorządowym działania są słabo doinwestowane przez co wdrożenie jest w fazie zalążkowej lub działania są prowadzone wyłącznie w ramach zaspokojenia minimalnych wymagań.
36	36ŁP	I, U		x				reakcje / działania podejmowane przez określone poziomy cyberbezpieczeństwa na zidentyfikowane zdarzenia i incydenty wydaje się dość skuteczna i dobrze adresowana. Przynajmniej w obszarach, które system jest w stanie dostrzec. Odrębna kwestią pozostaje profilaktyka w zakresie budowania świadomości użytkowników / uczestników poszczególnych procesów - tu niezbędna ciągła benedyktyńska praca.
37	37WW	B				x		Poza regulacjami (KSC, RODO) które spowodowały ze o cyberbezpieczeństwie wreszcie się mówi nie ma niestety programu wspierania sposobu osiągniecia celów jakie stawiał sobie ustawodawca. Obecnie pojedyncze inicjatywy będą odpowiadały na takie zapotrzebowanie, ale dalej szczególnie mniejsze jednostki są pozostawiane same sobie.
38	38SM	U		x				
39	39ŁT	B					x	Lata zaniedbań, brak aktów prawnych przez KSC, ignorowanie tematu cybersecurity, zwłaszcza w mniejszych jednostkach (np. JST), brak pieniędzy na cyberbezpieczeństwo, bezmyślne programy z dotacjami na digitalizację, które przeznaczane były głównie na brakujący hardware (np. desktopy, laptopy czy serwery) spowodowały, że poziom bezpieczeństwa państwa, zwłaszcza na niższych szczeblach administracji jest niski ze słabą efektywnością.
40	40WR	B		x				W mojej ocenie rozwiązania organizacyjne związane z cyberbezpieczeństwem na poziomie krajowym są dobrze zaprojektowane i funkcjonalnie sprawne. W szczególności na poziomie rządowym są jasno określone podmioty, kompetencje i zasady współpracy. Dotyczy to również infrastruktury krytycznej. Nie mam wiedzy natomiast, jak to wygląda na poziomie powiatowym i gminnym. Obawiam się, że poziom ten może być słabiej zaopiekowany, ale z drugiej strony pytanie jest, czy lepsze zaopiekowanie tego poziomu przyniesie większe korzyści niż koszty.
41	41ŁJ	A			x			Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Pełnomocnik przedstawia raporty z realizowanych zadań.

42	42JD	B, U				x		Wymagane jest dopracowanie odpowiedzialności (np. art. 21 w gminach mimo obowiązku nie jest spełniony) oraz drugi element podniesienie poziomu świadomości (nawet w zapisach ustawowych do osiągniecia zamierzonego poziomu)
43	43PS	B				x		Organizacja cyberbezpieczeństwa zorganizowana jest adekwatnie do obowiązujących przepisów. Nie oznacza to, że system jest adekwatny do wyzwań, jakie niesie obecny kontekst zagrożeń cyberprzestrzeni. Kluczowym wyzwaniem jest funkcjonowanie KSC równolegle do innych systemów zarządzania, a co za tym idzie ryzyko pojawiania się rozdźwięków.
44	44KP	B			x			
45	45SP	B			x			Co oznacza „dobrze zorganizowane", czy jest definicja tego pojęcia? Aby jednoznacznie stwierdzić, czy jest dobrze zorganizowane koniecznym jest przyjęcie konkretnych standardów i audyt niezależnej organizacji, która to sprawdzi.

1.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z zasadami i na wzór rozwiązań określonych w ***systemie zarządzania kryzysowego*** *(ustawie o zarządzaniu kryzysowym i dokumentach powiązanych) oraz z nim ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym oraz pod względem struktury i zawartości dokumentów planistycznych i zarządczych na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym, poprzez realizację tożsamych procesów i tworzenie dedykowanych zarządzaniu cyberbezpieczeństwem odpowiedników, takich dokumentów systemu zarządzania kryzysowego, jak: Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.*

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Z naszych doświadczeń zarządzanie kryzysowe jest systemem papierowym. Powstaje dużo dokumentów które nie mają realnego wpływu na funkcjonowanie organizacji.
2	2UM	B		x				Regulowanie tego samego obszaru w różnych aktach prawnych nie sprzyja jakości procesu. Co prawda, w ustawie o krajowym systemie cyberbezpieczeństwa w zakresie dokumentacji

								wymaganej od operatorów usługi kluczowej nawiązuje się do ustawy o zarzadzaniu kryzysowym, ale korelacja działań w obszarze cyberbezpieczeństwa powinna być większa, jednak z uwzględnieniem specyficznych wymogów poszczególnych sektorów
3	3BS	B		x				System cyberbezpieczeństwa powinien być zharmonizowany z innymi obszarami bezpieczeństwa Państwa, jednak jego struktura może być inna. Obecna struktura wydaje się poprawna, nie musi odwoływać się do innych rozwiązań.
4	4SK	U				x		Cyberbezpieczeństwo RP warunkowane jest w dużym stopniu odpornością operatorów kluczowych usług. W zarządzaniu kryzysowym obowiązuje zupełnie inny model = punktowy. W cyberbezpieczeństwie (dyrektywa NIS) model usługowy.
5	5MK	B, U	x					Niestety obecny rząd nie traktuje cyberbezpieczeństwa, jako odmiany bezpieczeństwa narodowego i buduje odrębny silos pt. cyberbezpieczeństwo. Tymczasem konsekwencje cyberataku mogą być odczuwalne w prawdziwym życiu, jako sytuacja kryzysowa (brak prądu), więc powinien to obsłużyć jeden system. Niestety obecny rząd utożsamia zarządzanie kryzysowe z zarządzaniem kryzysem, czego konsekwencją jest decyzja o likwidacji RCB i całego systemu i uruchomieniu go w MSWiA w oparciu o oficerów dyżurnych, z pominięciem całej planistyki i zadań ponadresortowych.
6	6ST	I, U		x				
7	7KG	B			x			Moim zdaniem UKSC niejako uzupełnia wprowadzone przez przepisy o zarządzaniu kryzysowym środki bezpieczeństwa w zakresie cyberodporności podmiotu, jeśli jest on równocześnie operatorem infrastruktury krytycznej oraz operatorem usługi kluczowej/operatorem usługi cyfrowej.
8	8DP	A	x					Przedstawione rozwiązanie pozwoli na efektywne funkcjonowanie dwóch systemów – zarządzania kryzysowego i cyberbezpieczeństwa. Jeżeli struktury, dokumenty i procesy będą tożsame, to istnieje duża szansa na sprawne działanie i wymianę informacji na każdym poziomie -krajowym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym. W takim przypadku istnieje prawdopodobieństwo, że w przypadku wystąpienia kryzysu nie dojdzie do sytuacji, w której poszczególne podmioty będą operować na różniącymi się procedurami i procesami.
9	9KM	B					x	Bezpieczeństwo to proces, w którym sytuacje kryzysowe stanowią 30%.
10	10BD	A		x				Może to spowodować podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa.
11	11KP	B				x		Choć zarządzanie cyberbezpieczeństwem, a w szczególności, procedury reakcji na incydenty, powinny uzupełniać się i nawiązywać do zarządzania kryzysowego, o tyle samo zarządzanie kryzysowe pozostaje inną, wydaje się szerszą dziedziną aniżeli cyberbezpieczeństwo.

12	12PM	B					x	W obecnej sytuacji organizacja zarządzanie cyberbezpieczeństwem powinno raczej przypominać odpowiednik WOT (ze stopniami analogicznymi do poziomu kompetencji i okresowymi ćwiczeniami, szkoleniami i centralnie (regionalnie, sektorowo) przygotowanymi wytycznymi) oraz kadrą menadżerską, ekspercką w stałych strukturach. Dla skutecznego działania trzeba ich zorganizować w hierarchiczną strukturę, centralnie udostępniać oprogramowaniem wspomagające ten obszar (i szkoleniami). Ponadto zadaniem takiej stałej struktury powinna być bieżąca współpraca z Policją i wojskiem, tak, aby z jednej strony wspierać osoby narażone na ataki, wspierać firmy (zwłaszcza infrastruktury krytycznej oraz urzędy). Organizacja zarządzania cyberbezpieczeństwem powinna de facto pełnić rolę aktywnego przeciwdziałania, a nie reaktywnego działania. Według zasady „Si vis pacem para bellum" (jeżeli chcesz pokoju szykuj wojnę). Wobec czego kluczową kwestią dla takiej organizacji powinien być jest czas detekcji, czas reakcji, możliwość skutecznego współdziałania, odpowiedzi i gromadzenie informacji dla właściwej oceny ryzyka i skutecznej odpowiedzi w skali kraju, a nie pojedynczej firmy, czy urzędu.
13	13RP	I		x				Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z określonymi i wdrożonymi zasadami oraz ujednolicona i zharmonizowana pod względem procesowym, planistycznym i operacyjnym poprzez realizację dedykowanych procesów cyberbezpieczeństwa.
14	14CT	B		x				Jednolitość zarządzania umożliwia eliminację luk oraz sprawniejsze zarządzanie. System cyberbezpieczeństwa państwa to element zarządzania kryzysowego.
15	15MB	A				x		Zadania cyberbezpieczeństwa w wielu aspektach inne niż zarządzania kryzysowego chociaż w zespole kryzysowym powinna być osoba również od cyber.
16	16KR	B					x	Zarządzanie cyberbezpieczeństwem to proces ciągły i nie może mieć charakteru działań kryzysowych, które z natury koncentrują się na zdarzeniach incydentalnych, a więc są responsywne wobec zagrożeń. Proces zarządzania cyberbezpieczeństwem powinien opierać się na planowaniu odpowiedzi na znane ryzyka z uwzględnieniem mechanizmów detekcyjnych, prewencyjnych i korekcyjnych.
17	17MM	I		x				
18	18WM	U					x	Obecna ustawa o zarządzaniu kryzysowym nie odpowiada wyzwaniom obszary cyber. Próba dostosowania ustawy o cyberbezpieczeństwie RP do obecnej ustawy o zarządzaniu kryzysowym przyniosłaby więcej szkód niż pożytku. Obecnie na forum UE trwają prace nad dyrektywą CER, która ma zmienić podejście do wyznaczani IK i tym samym zarzadzania kryzysowego na terenie UE. Dyrektywa CER ma być zintegrowana z zapisami dyrektywy NIS2 oraz DORA i w tym kontekście unifikacja zarządzania bezpieczeństwem IK, cyberbezpieczeństwem i sektorem bankowym zdecydowanie ma sens.

19	19DJ	A				x		Większość działań z obszaru cyberbezpieczeństwa to kwestie przygotowania na incydent, zabezpieczenia systemów IT/OT, szkolenia pracowników, monitorowania sieci, reagowania na incydent. Jest dużo elementów, które się przecinają, ale z kwestiami ochrony infrastruktury krytycznej, a nie zarządzania kryzysowego; zarzadzanie kryzysowe jest kolejnym etapem, kiedy incydent wymknie się spod kontroli. Ochrona infrastruktury krytycznej obejmuje wiele elementów, nie ograniczając się do cyberbezpieczeństwa. Także zakres przedmiotowy (rodzaje podmiotów objętych regulacją) jest węższy. System powinien być stopniowalny: od infrastruktury krytycznej (absolutnie niezbędne funkcje państwa), przez usługi kluczowe (ochrona życia i zdrowia, skuteczność państwa, stabilność i bezpieczeństwo gospodarki) do pozostałych podmiotów (inne firmy, dostawcy, obywatele). Podsumowując, część rozwiązań powinna zostać wprowadzona, ale większość zsynchronizowana.
20	20MA	B				x		Cyberbezpieczeństwo w zakresie swojej aktywności nie opiera się wyłącznie na realizacji strategii i operacji zarządzania incydentami, przez co nie może być postrzegane przez pryzmat jedynie sytuacji kryzysowej. W związku z cyfryzacją informacji i usług w gospodarce oraz strukturach państwowych, cyberbezpieczeństwo powinno być zintegrowane z systemem zarządzania kryzysowego, jednak powinno również zostać zintegrowane z systemem edukacji, systemem zdrowia i każdym innym, w którym występują procesy cyfryzacji. Najprostszym sposobem realizacji jest wyciągnięcie wniosków z podobnych praktyk w innych krajach i np. wprowadzenie jednolitego katalogu oczekiwań kontrolnych, jednolitego modelu zarządzania ryzykiem zintegrowanym ze wspomnianym katalogiem, określeniem wymaganych poziomów profili kontrolnych dla danych sektorów/systemów i monitorowanie ich procesów doskonalenia do i ponad wymagany poziom.
21	21DM	B, U		x				Ujednolicenie jest wskazane. Na poziomie gminnym jest to realizowane przez zespół odpowiedzialny za zarządzanie kryzysowe i obowiązki obronne państwa gospodarza (HMS). Problemem mogą być kwestie kompetencyjne organów centralnych.
22	22SP	B		x				
23	23SW	I, U				x		Obecna ustawa o ZK skupia się na reagowaniu na określony poziom dolegliwości zdarzenia (patrz definicja sytuacji kryzysowej), podczas w obszarze bezpieczeństwa cyber dominuje podejście oparte o budowanie odporności. Niniejsza uwag po wejściu w życie dyrektywy CER stanie się bezprzedmiotowa.
24	24MA	I		x				W szerokim ujęciu krajowy system cyberbezpieczeństwa jest powiązany z systemem zarządzania kryzysowego. Zatem organizacja zarządzania cyberbezpieczeństwem RP mogłaby być rozpatrywana podobnie, co zwiększyłoby sprawność i skuteczność działań na poziomie centralnym i lokalnym.

25	25KD	I	x					Ujednolicenie i zharmonizowanie oraz realizacja tożsamych procesów stanowi podstawę efektywnego działania.
26	26SP	B					x	To nie są tożsame procesy. Po pierwsze ryzyko braku dostępności czegoś kluczowego czy krytycznego jest inne najczęściej większe z uwagi na awarie niż cyberatak. Po 2gie internet nie zna granic, tak więc zajmowanie się cyberzagrozeniami regionalnie najczęściej ma znikomy sens. Po 3cie już zarządzanie kryzysowe tworzy wystarczającą ilość biurokracji. Więcej nie trzeba.
27	27KA	B		x				Koherentność metod działania jest bardzo zasadna, gdyż prowadzi do unifikacji rozwiązań (procesowych, technicznych, etc). Zatem oparcie się o „szkielet" KPZK (który już jest) jest jak najbardziej racjonalne. Należy, jednakże wzmocnić nacisk na aktualność i rzeczywistą skuteczność wypracowywanych planów i rozwiązań, gdyż są duże wątpliwości, czy nie są to dokumenty „na półkę" i służą jedynie formalnemu wykazaniu, że istnieją. Nie wolno tego uchybienia popełnić w obszarze cyber. Tak czy inaczej pójście ścieżką doskonalenie istniejącego systemu (KPZK), jego udoskonalania i obejmowania nim innych obszarów zarządzania bezpieczeństwem Państwa jest racjonalnie. Przez udoskonalenie rozumiem m.in. informatyzację tego systemu co pozwoliłoby na monitorowanie i zarządzanie sytuacją kryzysową w realnym czasie z minimalną, akceptowalną zwłoką. Obecny system jest systemem „analogowym" i służy raczej raportowaniu niż realnemu zarządzaniu. Zarządzanie sytuacją kryzysową powinno dawać możliwości monitorowania i reagowania na zdarzenia mogące doprowadzić do sytuacji kryzysowej niezależnie od rodzaju zagrożenia (katastrofy naturalnej, wojny czy cyberataku), gdyż skutki takie zdarzenia mogą doprowadzić do identycznych lub bardzo podobnych konsekwencji.
28	28RM	U			x			Zarządzanie kryzysowe w PL jest taką samą fikcją jak zarządzanie cyberbezpieczeństwem – nie wiem zatem, czy wzorowanie się na rozwiązaniach proceduralnych przyniosłoby jakąkolwiek poprawę. Oba obszary mają jednak swoją specyfikę, która jest trudna do przeniesienia. Zadania podejmowane w obszarze ZK mają jednak wyraźny kontekst terytorialny, te dotyczące domeny cyber – nie zawsze.
29	29GW	B		x				W takim przypadku jest szansa na systemowe ujednolicone rozwiązania, przygotowane przez ekspertów – dobre i tańsze ze względu na skalę.
30	30RT	B, U	x					Są ustalone procesy a kadry są wyszkolone. Powinno się oprzeć na tych istniejących rozwiązaniach, jednak należy wzbogacić SZK o jednostki cyberspec.
31	31BC	A		x				
32	32KW	B	x					prawdopodobnie najlepszym rozwiązaniem będzie harmonizacja obu regulacji, jednakże nie widzę żadnego uzasadnienia dla poziomów regionalnych, tam nigdy nie było i nie będzie żadnych kompetencji, a pojawia się tylko wielokrotne raportowanie tych samych zagadnień. Przykładem niech będzie dowolna organizacja infrastrukturalna mająca zakres działania na terenie całego kraju lub kilku województw. W przypadku wdrożenia stopni

								alarmowych ten sam raport musi być wysłany zarówno do RCB, jak i do wszystkich sztabów wojewódzkich, z tą różnicą, że sztaby wojewódzkie oczekują tego raportu odpowiednio wcześniej… Być może powinna powstać jedna regulacja zarządzająca kryzysem w obu obszarach.
33	33MM	B, U				x		te obszary tylko częściowo się pokrywają
34	34RA	B				x		Zmiany takich planów będą się ciągnąć miesiącami – potrzebna jest większa granulacja, żeby mogły być szybciej dostosowywane pod kątem nowych wektorów ataku
35	35KM	B, U			x			Nie znam dokumentów Krajowy Plan Zarządzania Kryzysowego, ministerialne, regionalne i sektorowe plany zarządzania kryzysowego, Narodowy Program Ochrony Infrastruktury Krytycznej.
36	36ŁP	I, U	x					Spójność w tym zakresie to oszczędność czasu, pracy i ograniczenie strat. W zasadzie obszary cyberbezpieczeństwa powinny być co do zasady modelowane przy bezpośrednim uwzględnieniu zakresów IK oraz być aktualizowane / rozrastać się wspólnie z nimi na inne moduły funkcjonowania społeczeństwa wynikające z analizy bieżących zagrożeń ujawniających się na świecie (np. rosyjska agresja na Ukrainę).
37	37WW	B	x					Skoro cyberprzestrzeń jest traktowana na równi z terytorium kraju, to absolutnie powinna być uwzględniona w systemie zarządzania kryzysowego.
38	38SM	U				x		Wskazane rozwiązania funkcjonują już w ramach *Narodowego Programu Ochrony Infrastruktury Krytycznej* w obszarze bezpieczeństwa teleinformatycznego.
39	39ŁT	B					x	Dotychczasowa praktyka zarządzania kryzysowego w naszym kraju jest powszechnie krytykowana za resortowość, upolitycznienie i nieskuteczność.
40	40WR	B			x			
41	41ŁJ	A				x		Analiza sposobu organizacji krajowego systemu cyberbezpieczeństwa, w tym jego powiązań ze sferą zarządzania kryzysowego, ustawą o działaniach antyterrorystycznych została przeprowadzona na etapie projektowania ustawy o krajowym systemie cyberbezpieczeństwa, w których uczestniczyłem w czasie pracy w Ministerstwie Cyfryzacji. Powyższe zostało skonsultowane w ramach rządowego procesu legislacyjnego i w Sejmie. Część informacji na ten temat zawiera uzasadnienie do ustawy o krajowym systemie cyberbezpieczeństwa. Inicjatywa zmian legislacyjnych – właściwość KPRM.
42	42JD	B, U		x				Bezpieczeństwo powinno posiadać zdefiniowane procesy i hierarchię
43	43PS	B				x		Konieczne jest ustandaryzowanie zarządzania cyberbezpieczeństwem RP oraz zarządzania kryzysowego. Jednak przyjęcie modelu zarządzania kryzysowego nie jest rozwiązaniem, które powinno być wzorcem. Docelowy model powinien korzystać zarówno z dobrych rozwiązań jakie wnosi model zarządzania kryzysowego jak również model zarządzania z aktualnego KSC.
44	44KP	B		x				
45	45SP	B		x				Raczej Tak – jeśli:

								• „Stan Internetu” uznajemy, jako „sytuację będącą następstwem zagrożenia i prowadzącą w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych, o których mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej”. • Przyjmiemy główne zasady - zapobieganie, podejmowanie zaplanowanych działań i reagowanie, zgodnie z art. 2. „zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych oraz na odtwarzaniu infrastruktury lub przywróceniu jej pierwotnego charakteru”. *Komentarz – tylko, co wtedy z KSC i KRI?*

1.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowane w pkt. 1.2. powyżej zorganizowanie, planowanie i dokumentowanie zarządzania cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione, jako:

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	**Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**
1	funkcjonujące niezależnie i równolegle do rozwiązań systemu zarządzania kryzysowego					
2	funkcjonujące równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim połączone					
3	w pełni zintegrowane z rozwiązaniami systemu zarządzania kryzysowego w jeden, spójny i jednorodny dokument planistyczny zarządzania, obejmujący problematykę dotyczącą zagadnień zarządzania kryzysowego i cyberbezpieczeństwa					

Lp.	Respon-dent	Obszar	Zdecy-dowanie TAK	Raczej TAK	Brak zda-nia	Raczej NIE	Zdecy-dowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B		2, 3			1	Trudno jednoznacznie odpowiedzieć na to pytanie. Z doświadczenia widzimy, że zarządzanie kryzysowe nie lubi się integrować z żadnymi innymi systemami i bardzo często ogranicza się do osób, które siedzą w jednym pokoju bez zbytniej współpracy z resztą organizacji. Z założenia KSC, zarządzanie kryzysowe i infrastruktura krytyczna to są obszary które powinny się integrować, ale w praktyce mając na uwadze obecne zaszłości, przyzwyczajenia ludzkie i profil osób zajmujących się zarządzaniem kryzysowym jest to bardzo trudne.
2	2UM	B		2				Jak wskazano wcześniej korelacja tych obszarów jest jak najbardziej pożądana, jednak trzeba mieć na uwadze fakt, że ustawa o krajowym systemie cyberbezpieczeństwa stanowi implementację dyrektywy unijnej i dotyczy operatorów usługi kluczowej, ponadto jak wskazano wcześniej powinno uwzględniać specyfikę poszczególnych sektorów
3	3BS	B		1, 2			3	Jw. 1.2 *System cyberbezpieczeństwa powinien być zharmonizowany z innymi obszarami bezpieczeństwa Państwa, jednak jego struktura może być inna. Obecna struktura wydaje się poprawna, nie musi odwoływać się do innych rozwiązań.*
4	4SK	U		2	1	3		Najbliżej do pkt 2. Nie da się w pełni niezależnie zaprojektować tych systemów, bo incydent bezpieczeństwa komputerowego może prowadzić do sytuacji kryzysowych. Ale nie każdy, co nawet wynika z UKSC
5	5MK	B, U	3					trudnym punktem w fazie reagowania (podczas obsługi incydentów) pozostaje moment, w którym kończą się analizy techniczne i sprawę trzeba przekazać do decyzji na szczebel polityczny. Dziś pomostem między światem techniki i polityki jest zespół incydentów krytycznych w RCB, które jest jednak za slabe do tej roli.
6	6ST	I, U	3			1, 2		
7	7KG	B		2				Przepisy o zarządzeniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa powinny się uzupełniać i moim zdaniem nie powinno się ich integrować do jednego systemu bezpieczeństwa. W obecnym stanie prawnym zarówno podmiot, który jest operatorem infrastruktury krytycznej oraz operatorem usługi kluczowej/operatorem usługi cyfrowej nie ma problemu w stosowaniu tych dwóch przepisów (procedury zarządzania kryzysowego np. w obszarze cyberbezpieczeństwa, w tym realizacji na poziomie podmiotu stopni alarmowych CRP mogą odwoływać się do procedur bezpieczeństwa teleinformatycznego).
8	8DP	A		2				Trudno jest stwierdzić, czy istnieje realna szansa połączenia zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa w jednym dokumencie planistycznym. Wspomniane obszary obejmują bardzo szerokie spektrum działania. Bardziej zasadne jest, aby osobno określać reguły działania i funkcjonowania

								(w tym kwestie odpowiedniego finansowania) wyżej wymienionych systemów. Oczywiście sytuacja kryzysowa może obejmować obszar zarządzania kryzysowego i cyberbezpieczeństwa, dlatego powinny być one ze sobą punktowo/problemowo połączone.
9	9KM	B	2					Kryzys to tylko jedna ze składowych.
10	10BD	A		2		1, 3		Ścisłe współdziałanie może się okazać niezbędne w obsłudze incydentu oraz zarządzaniu incydentem
11	11KP	B		2	1		3	Zgodnie z powyżej przytoczoną argumentacją. *Choć zarządzanie cyberbezpieczeństwem, a w szczególności, procedury reakcji na incydenty, powinny uzupełniać się i nawiązywać do zarządzania kryzysowego, o tyle samo zarządzanie kryzysowe pozostaje inną, wydaje się szerszą dziedziną aniżeli cyberbezpieczeństwo.*
12	12PM	B	2				1, 3	Jeżeli będzie niezależnie funkcjonować to będzie działało dla własnych celów. Jeżeli będzie w pełni zintegrowana z zarządzaniem kryzysowym to stanie się zbiurokratyzowaną reaktywną strukturą z długim czasem reakcji Taka organizacja powinna pełnić rolę społeczną wspierając firmy (informatyków, osoby odpowiedzialne za bezpieczeństwo), udostępniając najlepsze praktyki, oprogramowanie, szkolenia), policję, tak aby podnosić poziom reakcji i zwalczać aktywnie/minimalizować zagrożenia social engenering'u, wyłudzeń, fishingu, dezinformacji, i nieuprawnionego dostępu do informacji. Dla rzeczywistego podniesienia poziomu bezpieczeństwa trzeba zminimalizować bariery braku wiedzy, braku dostępności oprogramowania wspierającego (wysokie cny) oraz braku struktury organizującej współpracę. Niezwykle ważnym czynnikiem jest zapewnienie aktywnego przeciwdziałania i budowanie struktury współpracy
13	13RP	I	2		3		1	organizacja Krajowego Systemu Cyberbezpieczęństwa RP jest tematem o znacznie szerszej perspektywie niż sam system zarządzania kryzysowego. Dobrze byłoby znaleźć punkty styku w istotnych aspektach, jak np. dotyczących m.in. wyników szacowania ryzyka oraz z niego wynikającego zapewnienia niedoborów czy braków kluczowych zasobów, ponadto w aspekcie planów ciągłości działania i z nim zharmonizowanie planów. Ważnym aspektem są również kluczowe ryzyka ze względu na Cyberbezpieczęństwo Państwa, które powinny zostać uwzględnione w planach mitygujących zagrożenia ze względu na np. skutki. Jak przykładowo zapewnienie profesjonalnego wsparcia w zakresie np. usług analizy powłamaniowej i odtworzenia / przywrócenia ciągłości działania usług kluczowych. W pełni całkowita integracja i połączeniu obu systemów w jeden nie byłoby możliwe ze względu na fakt, że zarządzanie kryzysowe ze swojej natury odwołuje się głównie do skutków, natomiast w zarządzaniu Krajowym Systemem Cyberbezpieczęństwa główne akcenty kładzie się na zapobieganie powstaniem ewentualnych incydentów. Zatem warto dokonać ścisłej integracji obu systemów tam, gdzie następują związki przyczynowo-skutkowe i zastosować

								podejście procesowe jako obowiązkowe ze względu choćby na dobrze określony zakres odpowiedzialności porządkujący ewentualne z tego tytułu kwestie wypływające.
14	14CT	B	3				1, 2	Integracja zapewnia sprawność i łatwość w zarządzaniu. Dwie odrębne metodologie mogą wprowadzać chaos.
15	15MB	A		1, 2		3		Zadanie cyber są w wielu aspektach różne od zarządzania kryzysowego.
16	16KR	B	1, 2				3	
17	17MM	I	3			1, 2		
18	18WM	U	2			3	1	Obecna ustawa o zarządzaniu kryzysowym nie odpowiada wyzwaniom obszary cyber. Próba dostosowania ustawy o cyberbezpieczeństwie RP do obecnej ustawy o zarządzaniu kryzysowym przyniosłaby więcej szkód niż pożytku. Obecnie na forum UE trwają prace nad dyrektywą CER, która ma zmienić podejście do wyznaczani IK i tym samym zarzadzania kryzysowego na terenie UE. Dyrektywa CER ma być zintegrowana z zapisami dyrektywy NIS2 oraz DORA i w tym kontekście unifikacja zarządzania bezpieczeństwem IK, cyberbezpieczeństwem i sektorem bankowym zdecydowanie ma sens.
19	19DJ	A	2				1, 3	Uzasadnienie w punkcie wyżej. Konieczne jest odnalezienie optymalnych punktów wspólnych. Natomiast cyberbezpieczeństwo jest tylko jednym z elementów, które ZK powinno brać pod uwagę. *Większość działań z obszaru cyberbezpieczeństwa to kwestie przygotowania na incydent, zabezpieczenia systemów IT/OT, szkolenia pracowników, monitorowania sieci, reagowania na incydent. Jest dużo elementów, które się przecinają, ale z kwestiami ochrony infrastruktury krytycznej, a nie zarządzania kryzysowego; zarzadzanie kryzysowe jest kolejnym etapem, kiedy incydent wymknie się spod kontroli.* *Ochrona infrastruktury krytycznej obejmuje wiele elementów, nie ograniczając się do cyberbezpieczeństwa. Także zakres przedmiotowy (rodzaje podmiotów objętych regulacją) jest węższy.* *System powinien być stopniowalny: od infrastruktury krytycznej (absolutnie niezbędne funkcje państwa), przez usługi kluczowe (ochrona życia i zdrowia, skuteczność państwa, stabilność i bezpieczeństwo gospodarki) do pozostałych podmiotów (inne firmy, dostawcy, obywatele).* *Podsumowując, część rozwiązań powinna zostać wprowadzona, ale większość zsynchronizowana.*
20	20MA	B	3				1, 2	Raz jeszcze podkreślę, że cyberbezpieczeństwo nie ma na celu jedynie zarządzania incydentami, przez co powinno odnosić się do szerszego kontekstu regulacyjnego i być obecne w szerszej świadomości niż jedynie zarządzanie kryzysowe. Z uwagi na procesy cyfryzacji obecne w państwie, pełna integracja a nie punktowa jest wskazana w celu uwzględnienia natury dynamiki informacji już na poziomie projektowania systemu zarządzania kryzyso-

								wego a nie w „punktach stycznych”. Dobrym przykładem tego co powyżej jest zintegrowany system komunikacji kryzysowej w USA który obecnie przechodzi pełną integrację z uwagi na zjawiska cyber.
21	21DM	B, U	2	3		1		Wyzwaniem będą kwestie kompetencyjne organów centralnych.
22	22SP	B		2, 3		1		
23	23SW	I, U	2					Dotychczasowy system zarządzania kryzysowego wymaga zmiany podejścia z zarządzania sytuacjami kryzysowymi na budowanie odporności. Udzielona odpowiedź dotyczy sytuacji po wejściu w życie CER. Nie można obu systemów zintegrować, gdyż nie wszystkie przyszłe usługi kluczowe bazują na przetwarzaniu danych.
24	24MA	I		3		1, 2		Zarządzanie działaniami w obszarach bezpieczeństwa i cyberbezpieczeństwa wymaga kompleksowego podejścia. Synergia wydaje się możliwa, jeżeli weźmie się pod uwagę ich specyfikę, przenikanie się w praktyce, a jedocześnie zapewni zintegrowane rozwiązania, co zwiększy skuteczność i sprawność realizowanych działań.
25	25KD	I	3			2	1	
26	26SP	B		1, 2			3	Wszystko, począwszy od siatki pojęciowej, jest inne w zarządzaniu kryzysowym i cyberbezpieczeństwie. Inne podległości, inne raportowanie, brak punktów współpracy.
27	27KA	B	3			2	1	Konsekwentnie stojąc na stanowisku, że sytuacją kryzysową należy zarządzać całościowo, dopuszczałbym w okresie przejściowym rozwiązania odrębne, ale zintegrowane z systemem nadrzędnym, tj. systemem Zarządzania Kryzysowego. Warto pamiętać, że wszystkie systemy wymagają infrastruktury teleinformatycznej. Budowanie rozłącznych systemów często prowadziłoby do dublowania pewnych komponentów infrastruktury (lub niemożność skorzystania z już istniejących), co jest oczywistą niegospodarnością. Ponadto można przyjąć, iż pewne rodzaje danych mogą być wspólne dla systemów cyber jak i ZK). Zatem zasada re-używania danych też jest argumentem „za” w tej dyskusji.
28	28RM	U						Proszę zwrócić uwagę, że te pytania są o tyle wtórne, że praktycznie całość regulacji dotyczącej cyberbezpieczeństwa (z wyłączeniem obronności) to dziedzina regulacji prawa UE. W unijnym modelu cyberbezpieczeństwo to jest cały kompleks regulacji, omawiając tylko krajową UKSC traci Pan ten kontekst. Istnieje szereg regulacji UE które wprost dotyczą obszaru cyberbezpieczeństwa, a z uwagi na swoją formę (rozporządzenia) nie podlegają lub nie będą podlegały (w przypadku projektowanych aktów) transpozycji.
29	29GW	B		2	3	1		
30	30RT	B, U	2				3	Z uwagi na kwalifikacje kadry cyberbezpieczeństwa, które leżą po stronie teleinformatycznych zagadnień należy punktowo należy wiązać system. Węzłami powinny być osrodki CERT z komunikacji i nadzoru teleinformatycznego oraz systemami powiadamiania.
31	31BC	A	2	3	1			
32	32KW	B	3			2	1	jak wskazałem wcześniej Ustawa o Zarządzaniu Kryzysowym nie bierze pod uwagę procesów realizowanych przez daną organizację i bazuje na ochronie konkretnych obiektów, co

								w wielu przypadkach nie jest wystarczające. Pominięty jest także fakt możliwości wykorzystania systemów teleinformatycznych do destabilizacji, unieruchomienia lub zniszczenia infrastruktury fizycznej. Ścisła relacja pomiędzy bezpieczeństwem fizycznym a cybernetycznym jest faktem i wymaga jednorodnego podejścia
33	33MM	B, U						nie udzielam odpowiedzi, ponieważ jak wskazałem raczej nie zgadzam się takim rozwiązaniem
34	34RA	B		2		3		branżowe tematy mogą wymagac innych sposobów komunikacji i częstotliwości zmian– łatwiej jest dostosować mniejszy dokument połączony z głównym
35	35KM	B, U	3					System KSC budowany w ramach dotyczy zdarzeń o dużej skali dotykających wielu obywateli. Integracja na poziomie systemowym pozwoli na skuteczne i pełne wykorzystanie możliwości jakie już posiadamy i tych, które tworzymy.
36	36ŁP	I, U	3					Jw. *Spójność w tym zakresie to oszczędność czasu, pracy i ograniczenie strat. W zasadzie obszary cyberbezpieczeństwa powinny być co do zasady modelowane przy bezpośrednim uwzględnieniu zakresów IK oraz być aktualizowane / rozrastać się wspólnie z nimi na inne moduły funkcjonowania społeczeństwa wynikające z analizy bieżących zagrożeń ujawniających się na świecie (np. rosyjska agresja na Ukrainę).*
37	37WW	B	3					Jak wyżej zbyt wiele operacji prowadzimy w cyberprzestrzeni, żeby nie traktować jej jako kolejnego obszaru Państwa. *Skoro cyberprzestrzeń jest traktowana na równi z terytorium kraju to absolutnie powinna być uwzględniona w systemie zarządzania kryzysowego.*
38	38SM	U	2					
39	39ŁT	B	1	2			3	Cyberbezpieczeństwo to bardzo specyficzny, skomplikowany i wymagający zupełnie innych zasobów obszar, który w minimalnym stopniu (ale jednak – krytyczne punkty styku / przepływu informacji i zarządzania) powinien być powiązany z SZK.
40	40WR	B		2		1, 3		Zarządzanie cyberbezpieczeństwem w porównaniu z zarządzaniem kryzysowym jest realizowane w oparciu o nieco bardziej płaską strukturę. Wynika to z charakteru systemów IT i pozwala bardziej efektywnie realizować zadania. Zasadne zatem wydaje się, że planowanie i dokumentowanie tych dwóch obszarów powinno odbywać się równolegle. Jednak biorąc pod uwagę, że cześć elementów infrastruktury krytycznej posiada immanentną część w postaci systemów IT (tworząc funkcjonalnie całość), plany i dokumenty w tych obszarach powinny się zazębiać, a przynajmniej uwzględniać.
41	41ŁJ	A						Udzielono odpowiedzi w pkt. 1.2. *Analiza sposobu organizacji krajowego systemu cyberbezpieczeństwa, w tym jego powiązań ze sferą zarządzania kryzysowego, ustawą o działaniach antyterrorystycznych została przeprowadzona na etapie projektowania ustawy o krajowym systemie cyberbezpieczeń-*

								stwa, w których uczestniczyłem w czasie pracy w Ministerstwie Cyfryzacji. Powyższe zostało skonsultowane w ramach rządowego procesu legislacyjnego i w Sejmie. Część informacji na ten temat zawiera uzasadnienie do ustawy o krajowym systemie cyberbezpieczeństwa. Inicjatywa zmian legislacyjnych – właściwość KPRM.
42	42JD	B, U		2	1	3		
43	43PS	B	3				1, 2	Cyberprzestrzeń jako przestrzeń funkcjonowania człowieka jest obecnie pełnoprawną przestrzenią oddziałującą na społeczeństwo. Przekłada się to na zobowiązanie Państwa do nadzoru funkcjonowania tego wymiaru w sposób zintegrowany z pozostałymi przestrzeniami. Tylko w pełni zintegrowany model zarządzania pozwoli na wykorzystywanie efektów synergii i wyeliminowanie zagrożeń.
44	44KP	B	3	1, 2				
45	45SP	B		1, 2			3	Według art.3. (UoZK) definicja sytuacji kryzysowej brzmi następująco „Ilekroć w ustawie jest mowa o sytuacji kryzysowej − należy przez to rozumieć sytuację będącą następstwem zagrożenia i prowadzącą w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych, o których mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej”. Komentarz - Zagrożenia „Internetowe” są raczej punktowe i nie prowadzą do naruszenia, zerwania więzów społecznych …. itd., ale może nastąpić sytuacja, iż w przypadku cyberataku na obiekt infrastruktury krytycznej (zmiany procesów technologicznych itp.) ktoś doprowadzi do sytuacji kryzysowej, dlatego w punkcie 2 „funkcjonujące równolegle do rozwiązań systemu zarządzania kryzysowego, ale punktowo/problemowo z nim połączone” jest raczej TAK.

2. Efektywność struktur i relacji operacyjnych w systemie cyberbezpieczeństwa

2.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury organizacyjne, zaangażowane podmioty oraz relacje operacyjne systemu cyberbezpieczeństwa RP na poziomie krajowym, ministerialnym, regionalnym (wojewódzkim, powiatowym, gminnym) i sektorowym są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Nie widzimy wielkiej współpracy ani w sektorach, ani regionach. Firmy rzadko dzielą się informacjami o incydentach i słabościach. Zdarzają się akcje przeprowadzane przez CERT/CSIRT i czasem sektorowe spotkania/konferencje, jednak są to raczej sporadyczne działania.
2	2UM	B				x		W znanych mi przypadkach nie powołano sektorowych CSIRT-ów, istniejące rzadko podejmują zgłoszone tematy i nie informują o sposobie rozwiązania zgłoszonego incydentu. Ponadto wskazany uprzednio wynik audytów wykonywany w różnych podmiotach, szczególnie publicznych wskazuje, że stan faktyczny nie może być uznany za zadawalający
3	3BS	B		x				Na papierze wygląda to dobrze, jednak operacyjna realizacja kuleje.
4	4SK	U				x		Nie. Dlatego dokonuje się ich modyfikacji. Za cyberbezpieczeństwo powinny odpowiadać podmioty neutralne politycznie. A przykłady pokazują, że nie zawsze tak jest.
5	5MK	B, U				x		od szczebla wojewódzkiego w dół potrzebna jest praca u podstaw. Współpraca sektorowa w części sektorów usług kluczowych leży (np. ochrona zdrowia)
6	6ST	I, U	x					
7	7KG	B		x				Właściwie wdrożone przepisy ustawy i KSC oraz powołane tym aktem prawnym struktury (CSIRT poziomu krajowego, wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo) podmiotów uznanych za operatorów usług kluczowych moim zdaniem zapewniają efektywność krajowego systemu cyberbezpieczeństwa oraz odpowiedni poziom bezpieczeństwa państwa. Wprowadzenie procesu audytu w przepisach UKSC zgodnie z zasadą PDCA powoduje, że dokumentacja operacyjna w zakresie cyberbezpieczeństwa usługi kluczowej powinna być doskonalona (powinny być

								prowadzone działania korygujące i zapobiegawcze). Tak sam odwołanie do stosowania uznanych standardów takich jak ISO27001, ISO22301.
8	8DP	A	x					W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wskazano zadania i obowiązki poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa. Funkcjonowanie CSIRT NASK, CCIRT MON i CSIRT GOV pozwala na zapewnienie efektywności krajowego systemu cyberbezpieczeństwa, w szczególności w zakresie obsługi incydentów.
9	9KM	B				x		Komenda policji ewentualnie CUW na poziomie kilku gmin w mojej ocenie jest właściwym podejściem.
10	10BD	A			x			Będzie można stwierdzić po stopniu zrealizowania celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
11	11KP	B			x			
12	12PM	B					x	Obecne struktury są moim zdaniem nastawione reaktywnie. Wysokie bariery cenowe dostępu do wiedzy, dobrych praktyk, narzędzi i nieefektywne wydawanie środków, poprzez rozproszenie wydatków i słabą koordynację działań dają słabą wykrywalność i powolny czas reakcji
13	13RP	I			x			Ze względu na wczesny okres od wdrożenia Ustawy o krajowym systemie cyberbepzieczeństwa oraz krystalizowania się procesów oraz połączeń między instytucjami czy wczesny etap tworzenie instrumentów współpracy jak np. Platformy S46, ciężko jest móc jednoznacznie udzielić odpowiedzi na zadane pytanie.
14	14CT	B			x			Warto zapytać o świadomość istnienia takich struktur, służb i relacji.
15	15MB	A			x			Nie wiadomo, czy zapewniają odpowiedni poziom, bo nie było zmasowanego ataku takiego jak np. na Ukrainie.
16	16KR	B					x	
17	17MM	I				x		
18	18WM	U			x			Nie mam wiedzy na temat efektywności krajowego systemu cyberbezpieczeństwa.
19	19DJ	A		x				Większość struktur funkcjonuje poprawnie. Niedoskonałości systemu istnieją, ale są do dopracowania. Współpraca między różnymi podmiotami mogłaby funkcjonować lepiej, ale jest to problem nie tylko Polski. Brakuje średniego szczebla (operacyjnego) na wzór BSI lub ANSSI w krajach zachodnich, ale obecnie te zadania są realizowane przez inne podmioty i nie wpływa to na ogólny poziom bezpieczeństwa.
20	20MA	B					x	Jak w 1.1 *Zarządzanie cyberbezpieczeństwem w formie obecnej wydaje się koncentrować na praktykach spełniania wymogów zgodności oraz prezentowania wyników operacyjnych w ujęciu ilościowym a nie jakościowym. Nie istnieją sektorowe czy regionalne „profile bezpieczeństwa" używające jakiejkolwiek metodologii (np. NIST Cybersecurity Framework), brak jest*

								komunikacji ryzyk i zagrożeń, alerty dotyczące konkretnych operacji są najczęściej kierowane do niewłaściwych osób, z nieadekwatnym do komunikatu treścią (np. przekazywanie w ogólnym komunikacie danych IOC, brak koordynacji alertów i informacji wywiadu cybernetycznego na poziomie jednostek, ciągła rywalizacja zespołów CERT/CSIRT zamiast współpracy i współdzielenia informacji. System głównie funkcjonuje na zasadzie realizacji wymaganych prawem dokumentacji oraz współpracy opartej na relacjach osobistych a nie służbowych.
21	21DM	B, U		x				Zadania są zdefiniowane i na każdym szczeblu istnieje komórka odpowiedzialna za ich wykonanie jednak nie są one koordynowane co unaocznia się na szczeblu gminnym, gdzie spływają do realizacji wszelkie obowiązku. Jeśli chodzi o organizację na poziomie sektora warto zadbać o utrzymanie lub ulepszenie sektorowej i międzysektorowej wymiany wiedzy w ramach ISACa.
22	22SP	B		x				
23	23SW	I, U				x		Brak sektorowych SOC przy niespójności sektorów w ustawach o KSC i ZK powoduje chaos kompetencyjny i problemy z przepływem informacji.
24	24MA	I		x				W każdym z wymienionych aspektów krajowy system cyberbezpieczeństwa wymaga doskonalenia.
25	25KD	I				x		
26	26SP	B				x		Jeszcze na poziomie ministerialnym nie jest źle i widać współpracę. Jednak nawet na tym poziomie jednostki podległe MON i pozostałe działają odrębnie i bez widocznej dla mnie współpracy. Na poziomie wojewódzkim i niżej nie ma w zasadzie żadnej koordynacji. Nie ma też pomocy Państwa dla podmiotów komercyjnych zaangażowanych w system cyberbezpieczeństwa - jedyne co jest, to oczekiwania.
27	27KA	B				x		Ustawa o KSC (w wersji 1.0), mimo że niedoskonała nie została dotychczas skutecznie wdrożona. Za chwilę mamy wersję 2.0, którą nieco poprawia mankamenty poprzedniej, jednak jej skuteczne wdrożeni to też lata. Sklonowano CSIRTy, zatem nie mamy jednego, całościowego spojrzenia na cyber-sytuację w kraju. Budowany system S46, który ma być elementem spinającym i integrującym, to ciągle przyszłość. Zatem te podmioty, które mają wyższy poziom świadomości co do cyberzagrożeń samodzielnie próbują tworzyć i wdrażać strategie cyberbezpieczeństwa (jeśli dodatkowo mają środki na to). Zdecydowanie za mało wysiłku Państwa jest wkładane w budowanie cyberświadomości na wszystkich poziomach – zarówno w administracji jak i poza.
28	28RM	U					x	Ja nawet nie zgadzam się z postrzeganiem, że istnieje wojewódzki, powiatowy czy gminny poziom zarządzania cyberbezpieczeństwem.
29	29GW	B				x		
30	30RT	B, U					x	Samo zdefiniowanie nie decyduje o efektywnosci operacyjnej KSC potrzebne są treningi operacyjne.

31	31BC	A				x		
32	32KW	B					x	w mojej ocenie żaden system nie będzie działać na zasadach demokracji. Wymagany jest scentralizowany, efektywny i merytoryczny nadzór operacyjny, np. RCB, nad wszystkimi interesariuszami systemu. Dla przykładu przypadek z życia zupełnego braku efektywności: CSIRT.GOV identyfikuje długą listę „złośliwych" adresów IP, wysyła ją w wersji papierowej do RCB. RCB „już" po dwóch tygodniach robi wysyłkę (jako informacja niejawna) do podmiotów posiadających IK. Już po miesiącu podmiot otrzymuje w wersji papierowej listę adresów… Działanie nie ma już żadnego sensu operacyjnego.
33	33MM	B, U			x			patrz uzasadnienie 1.1. *wstawiłem „brak zdania", ponieważ moim zdaniem połączenie wszystkich poziomów w jednym pytaniu nie daje szansy na jasną odpowiedź. W skrócie – na poziomie krajowym „Raczej TAK", na pozostałych „Raczej NIE"*
34	34RA	B				x		Powiat i gmina są poza zakresem – brak im budżetu na fachowców. Specjalista cyber w gminie za 3000 miesięcznie?
35	35KM	B, U		x				System w ustawie jest zdefiniowany prawidłowo, ponieważ tworzony jest na podstawie dobrze wypracowanej strategii NIS. Problem leży we wdrożeniu, które kuleje, szczególnie na szczeblu samorządowym.
36	36ŁP	I, U		x				
37	37WW	B				x		Na poziomie krajowym mamy problem, ponieważ o ile CESIRT-y krajowe współpracują to już sektorowe zespoły nawet nie bardzo istnieją – poza finansami (KNF). Realnie przepisy istnieją, ale nie przekłada się to na działanie rzeczywiste.
38	38SM	U	x					
39	39ŁT	B		x				Same struktury opisane są względnie dobrze, gorzej z relacjami, a najgorzej – z faktycznym wykonywaniem obowiązków przez te podmioty.
40	40WR	B		x				Patrz pkt. 1.1 *W mojej ocenie rozwiązania organizacyjne związane z cyberbezpieczeństwem na poziomie krajowym są dobrze zaprojektowane i funkcjonalnie sprawne. W szczególności na poziomie rządowym są jasno określone podmioty, kompetencje i zasady współpracy. Dotyczy to również infrastruktury krytycznej. Nie mam wiedzy natomiast, jak to wygląda na poziomie powiatowym i gminnym. Obawiam się, że poziom ten może być słabiej zaopiekowany, ale z drugiej strony pytanie jest, czy lepsze zaopiekowanie tego poziomu przyniesie większe korzyści niż koszty.*
41	41ŁJ	A						Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.

42	42JD	B, U				x		Proponowałem zwiększenie roli wojewody w zakresie organizacyjnym, kontrolnym oraz możliwości egzekwowania
43	43PS	B				x		Struktury organizacyjne i relacje operacyjne nie zapewniają efektywności KSC. Występujący rozdział kompetencji na najwyższym poziomie (CSIRT krajowych) przekłada się na rozdźwięk działań na niższych poziomach i w efekcie wprowadza podatności systemowe.
44	44KP	B		x				
45	45SP	B		x				Tu są dwa pytania: *„…są właściwie zdefiniowane…" – raczej TAK, „…zapewniają efektywność…" – raczej NIE, ale to wynika z braku funduszy na elementy Cyberbezpieczeństwo w instytucjach.*

2.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury organizacyjne, zaangażowane podmioty i relacje operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami organizacyjnymi, podmiotami i relacjami operacyjnymi systemu zarządzania kryzysowego, np. poprzez pełne włączenie i nadanie m.in. Rządowemu Centrum Bezpieczeństwa (RCB) i organom regionalnym – np. wojewódzkim (wojewoda, WCZK, WZZK), podobnej roli, kompetencji, odpowiedzialności i rangi w systemie cyberbezpieczeństwa, jak w systemie zarządzania kryzysowego.

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Z naszych doświadczeń zarządzanie kryzysowe jest systemem papierowym. Powstaje dużo dokumentów które nie mają realnego wpływu na funkcjonowanie organizacji.
2	2UM	B		x				Unifikacja rozwiązań organizacyjnych jest wskazana, nadmierna ilość podmiotów nadzorujących i wykonawczych, zwłaszcza o krzyżujących się kompetencjach nie gwarantuje jakości procesu. Decyzja o tym jak powinna wyglądać docelowa struktura wymaga jednak uprzedniego sporządzenia mapy procesów tych jednostek i analizę punktów lub łańcuchów ich pokrywania się.
3	3BS	B				x		Nowe zadania zostały w miarę poprawnie zaprojektowane w nowelizacji UKSC.
4	4SK	U					x	Nie widzę takiej potrzeby
5	5MK	B, U				x		niestety resorty siłowe mają tendencję do autonomizacji i nie mogą znieść czynnika koordynującego, więc wyposażenie RCB w nowe kompetencje będzie trudne do przeforsowania w dyskusji z MSWiA i MON. Poza tym to głównie RZZK wymaga pilnego wzmocnienia.

6	6ST	I, U		x				
7	7KG	B			x			Dopóki podejście do ochrony infrastruktury krytycznej będzie miało charakter obiektowy i nie będzie uwzględniało świadczone przez operatorów/podmioty usług teleinformatycznych, rozwiązania zastosowanie obecnie w przepisach o zarządzaniu kryzysowym nie będą mogły być efektywnie przełożone na krajowy system cyberbezpieczeństwa. Obecnie ochrona danego obiektu (fizycznego) w danej lokalizacji (np. województwie) uznanego za infrastrukturę krytyczną nie ma przeszkód, żeby była np. planistycznie i zarządczo uwzględniana lokalnie. Natomiast systemy/usługi teleinformatyczne nie mają „granic" geograficznych więc trudno, żeby np. na poziomie lokalnym zarządzać ich ochroną.
8	8DP	A				x		Bardziej zasadne jest, aby funkcjonowały osobno dwa systemy – zarządzania kryzysowego i cyberbezpieczeństwa. Trudno powiedzieć, czy np. w przypadku wystąpienia równolegle katastrofy naturalnej i incydentu krytycznego (zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa) wymienione podmioty byłyby w stanie efektywnie i sprawnie realizować zadania w dwóch różnych obszarach.
9	9KM	B				x		Role powinny być ustrukturyzowane, ale wiodąca rola powinna być „na miejscu".
10	10BD	A				x		Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie podmioty w w/w zakresie.
11	11KP	B				x		Jak zostało wskazane wyżej, odpowiedzialność za cyberbezpieczeństwo powinna przypisana zostać nowym jednostkom, dedykowanym właśnie za ten obszar.
12	12PM	B					x	Takie podejście wzmacnia tylko reaktywny charakter organizacji zarządzania cyberbezpieczeństwem promując interes kilku firm. Urzędnicy i proponowane struktury nie zapewnią szybkiego czasu reakcji i możliwości przeciwdziałania (poprzez upowszechnienie wiedzy, narzędzi i hierarchicznej struktury współdziałania.
13	13RP	I			x			W mojej ocenie uwzględnienie wszystkich kluczowych interesariuszy w procesach ich dotyczących w zakresie budowania systemu cyberbezpieczeństwa ma istotne znaczenie. Nie pomijanie żadnego jest kluczem do osiągnięcia najwyższego poziomu funkcjonowania tego systemu jak i w konsekwencji osiągnięcia dobrej współpracy całego organizmu zapewnienia bezpieczeństwa kraju.
14	14CT	B		x				Im więcej struktur i służb, tym większy chaos może powstać.
15	15MB	A				x		Zadania są inne
16	16KR	B	x					Podniesienie rangi i ujednolicenie tak, integracja zdecydowanie nie.
17	17MM	I	x					
18	18WM	U	x					Unifikacja działań związanych bezpieczeństwem w obszarze usług kluczowych oraz IK powinna mieć miejsce ze względu na charakter powiązań między tymi elementami. Natomiast obszar cyber jest na tyle specyficzny, że nie można analizować go metodami adekwatnymi dla np. zagrożeń naturalnych typu pożar czy powódź. Dlatego Integralność obu

								systemów połączonych punktowo wydaje się właściwym kierunkiem. Dzięki temu możliwe jest agregowanie danych i analiza zbiorczych zagrożeń dla usług kluczowych i IK przy zachowaniu specyfiki każdego rodzaju zagrożeń.
19	19DJ	A					x	Podobnie jak we wcześniejszych odpowiedziach, pragnę zaznaczyć, że zarządzanie kryzysowe/ ochrona IK to nie są pojęcia tożsame z cyberbezpieczeństwem. Poza tym, w momencie, kiedy incydent wyeskaluje do poziomu kryzysu, to przestajemy mieć problem z komputerem, a zaczynamy z usługą – i wtedy dopiero wchodzi ZK.
20	20MA	B					x	Jak w 1.2 *Cyberbezpieczeństwo w zakresie swojej aktywności nie opiera się wyłącznie na realizacji strategii i operacji zarządzania incydentami, przez co nie może być postrzegane przez pryzmat jedynie sytuacji kryzysowej. W związku z cyfryzacją informacji i usług w gospodarce oraz strukturach państwowych, cyberbezpieczeństwo powinno być zintegrowane z systemem zarządzania kryzysowego, jednak powinno również zostać zintegrowane z systemem edukacji, systemem zdrowia i każdym innym, w którym występują procesy cyfryzacji. Najprostszym sposobem realizacji jest wyciągnięcie wniosków z podobnych praktyk w innych krajach i np. wprowadzenie jednolitego katalogu oczekiwań kontrolnych, jednolitego modelu zarządzania ryzykiem zintegrowanym ze wspomnianym katalogiem, określeniem wymaganych poziomów profili kontrolnych dla danych sektorów/systemów i monitorowanie ich procesów doskonalenia do i ponad wymagany poziom.*
21	21DM	B, U	x					Obecnie RCB i WCZK nie ma kompetencji dotyczących cyber i w sytuacji incydentu posiłkuje się przypadkowymi osobami np. Pełnomocnik ds. Cyber + biuro obsługowe/oddział informatyki, którzy nie są w stanie wykonawczo koordynować działania reagowania na zaawansowane zagrożenia.
22	22SP	B				x		
23	23SW	I, U				x		Nie widzę możliwości budowania CSIRT w każdym województwie.
24	24MA	I			x			Kierunek zmian wydaje się być właściwy, aczkolwiek przy zbyt powierzchownej wiedzy operacyjnej o systemie zarządzania kryzysowego trudno odpowiedzieć twierdząco.
25	25KD	I	x					
26	26SP	B		x				
27	27KA	B		x				Konsekwentnie – jak w odpowiedziach powyżej. Działajmy ewolucyjnie doskonaląc to co jest.
28	28RM	U					x	Odpowiadałem na to pytanie wyżej – system ZK jest daleki od doskonałości i strukturalnie/funkcjonalnie niedopasowany do potrzeb związanych ze sprawną komunikacją w obszarze cyber. RCB zajmuje się informowaniem o odśnieżaniu dróg i rozsyłaniem komunikatów o wichurach, więc w tym obszarze kompetencji trudno je rozszerzać o dodatkowe role dotyczące domeny cyber.
29	29GW	B		x				

30	30RT	B, U		x				RCB powinno być włączone w SZK. SZK jest przestarzałe RCB nie. Należy scalić i unowocześnić a w tym powiązać cyberbezpieczeństwo.
31	31BC	A		x				
32	32KW	B	x					z wyłączeniem struktur regionalnych, które nie wnoszą żadnej wartości jako pośrednik w obszarze cybernetycznym.
33	33MM	B, U				x		patrz uzasadnienie 1.2 *te obszary tylko częściowo się pokrywają*
34	34RA	B		x				Ma to sens z nadzorczego punktu widzenia
35	35KM	B, U	x					Uważam, że to jedyna słuszna droga rozwoju i implementacji KSC. Niestety nadążenie z kompetencjami będzie bardzo trudne.
36	36ŁP	I, U		x				Spójność organizacyjna, zarządcza i procesowa to jedyna droga do skuteczności. Wszystko zależy od kompetencji uczestników tych procesów na wszelkich poziomach, ale co do systemowości rozwiązania tak właśnie powinno być.
37	37WW	B		x				Jak wyżej, nie widzę powodu, dla którego cyberprzestrzeń mielibyśmy traktować inaczej niż inne wymiary państwa. *Na poziomie krajowym mamy problem, ponieważ o ile CESIRT-y krajowe współpracują to już sektorowe zespoły nawet nie bardzo istnieją – poza finansami (KNF). Realnie przepisy istnieją, ale nie przekłada się to na działanie rzeczywiste.*
38	38SM	U					x	Przyjęcie rozwiązania sektorowego ustanawiającego organy właściwe ds. cyberbezpieczeństwa na poziomie właściwych ministerstw jest odpowiednie.
39	39ŁT	B					x	Nie wyobrażam sobie takiej pełnej integracji i ujednolicenia, nadanie pełnych kompetencji i władzy RCB w zakresie cybersecurity – to nierealne. Każdy podmiot ma swoją specyfikę, potrzeby, kontekst organizacyjny, strukturę, własne procesy, używa innej technologii.
40	40WR	B					x	Spowoduje to rozbudowę strukturalną w obszarze cyberbezpieczeństwa nieuzasadnioną charakterystyką sieci IT.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 1.2. *Analiza sposobu organizacji krajowego systemu cyberbezpieczeństwa, w tym jego powiązań ze sferą zarządzania kryzysowego, ustawą o działaniach antyterrorystycznych została przeprowadzona na etapie projektowania ustawy o krajowym systemie cyberbezpieczeństwa, w których uczestniczyłem w czasie pracy w Ministerstwie Cyfryzacji. Powyższe zostało skonsultowane w ramach rządowego procesu legislacyjnego i w Sejmie. Część informacji na ten temat zawiera uzasadnienie do ustawy o krajowym systemie cyberbezpieczeństwa. Inicjatywa zmian legislacyjnych – właściwość KPRM.*
42	42JD	B, U			x			Możliwe, że to może zafunkcjonować, można np. rozszerzyć odpowiedzialności
43	43PS	B	x					Tylko jednolite podejście do cyberbezpieczeństwa może zapewnić adekwatne i wystarczająco szybkie decyzje w przypadku kryzysów.
44	44KP	B	x					

45	45SP	B				x		NIE – bo byśmy w wielu urzędach tworzyli dodatkowe/ równoległe/ kosztowne role urzędnicze, które nie są potrzebne.

2.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, poprzez m.in. rozszerzenie kompetencji i struktur oraz zapewnienie wiodącej roli RCB w szeroko definiowanym zintegrowanym zarządzaniu bezpieczeństwem krajowym, w tym zarządzaniu kryzysowym i cyberbezpieczeństwem, we współpracy z organami powołanymi ustawą o krajowym systemie cyberbezpieczeństwa (KSC), takimi jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy oraz, opcjonalnie, włączenie organów, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa w struktury RCB wraz z przejęciem ich kompetencji.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B			x			Struktury RCB są za małe, aby to udźwignąć
2	2UM	B		x				Unifikacja rozwiązań organizacyjnych jest wskazana, nadmierna ilość podmiotów nadzorujących i wykonawczych, zwłaszcza o krzyżujących się kompetencjach nie gwarantuje jakości procesu. Decyzja o tym jak powinna wyglądać docelowa struktura wymaga jednak uprzedniego sporządzenia mapy procesów tych jednostek i analizę punktów lub łańcuchów ich pokrywania się
3	3BS	B		x				Ujednolicenie struktur Państwowych jest odpowiednim kierunkiem, jednak sposób ich podporządkowania pod RCB wydaje się zbyt daleko idącym działaniem. Cała kwestia wymaga głębokiej analizy.
4	4SK	U				x		Nie widzę potrzeby integracji obu systemów. RCB nie ma potencjału ani władczości, aby koordynować to zagadnienie. ABW jest krajową władzą bezpieczeństwa i może pełnić rolę integrującą.
5	5MK	B, U				x		w obecnym rozdaniu politycznym dawanie jakiegokolwiek tlenu do RCB będzie tłamszone w zarodku przez resorty siłowe. Zresztą to nie RCB powinno mieć magiczny joystick, tylko przewodniczący RZZK
6	6ST	I, U		x				

7	7KG	B			x			Przepisy o zarządzeniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa powinny się uzupełniać i moim zdaniem nie powinno się ich integrować do jednego systemu bezpieczeństwa.
8	8DP	A				x		Podobnie jak w 2.2. Bardziej zasadne jest, aby funkcjonowały osobno dwa systemy – zarządzania kryzysowego i cyberbezpieczeństwa. Optymalnym rozwiązaniem byłyby, gdyby zostało stworzone osobne ponadresortowe centrum cyberbezpieczeństwa, które ściśle współpracowałoby z Rządowym Centrum Bezpieczeństwa.
9	9KM	B				x		Cyber jest coraz bardziej złożone i wymaga organicznej pracy u podstaw, a nie centralnego zarządzania.
10	10BD	A				x		Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie podmioty w w/w zakresie.
11	11KP	B		x				Wydzielenie kompetencji i ich harmonizacja pod egidą RCB (jako jednego miejsca przypisanej odpowiedzialności) wydaje się dobrym kierunkiem. Nadal jednak, procesy muszą być operacjonizowane oddzielnie.
12	12PM	B					x	Taka struktura daje tylko złudzenie zarządzania cyberbezpieczeństwem, bo jest reaktywne i w konfrontacji z agresywnymi działaniami (np. Rosji) skazuje Polskę na rolę ofiary.
13	13RP	I				x		Zgadzam się z tezą, że *Struktury operacyjne systemu cyberbezpieczeństwa powinny być ujednolicone i zharmonizowane ze strukturami operacyjnymi systemu zarządzania kryzysowego, ale nie poprzez rozszerzania kompetencji RCB a poprzez analizę ryzyka w zakresie Cyberbezpieczeństwa a dokładniej z niej płynących planów mitygacji ryzyk na wypadek przede wszystkim materializacji się kluczowych ryzyk w obszarze cyberbezpieczeństwa w aspekcie możliwie szybkim uruchamianiu rezerw celowych.*
14	14CT	B		x				Jak wyżej *Im więcej struktur i służb, tym większy chaos może powstać.*
15	15MB	A				x		Zakres działania jest inny.
16	16KR	B				x		Nie jestem przekonany, że RCB powinno być punktem centralnym a struktury KSC włączone go RCB. RCB może mieć rolę koordynującą, ale struktury KSC powinny być niezależne i posiadać własny, odrębny głos. W przeciwnym razie istnieje wysokie ryzyko obniżania priorytetów w obszarze cyberbezpieczeństwa na rzecz „bardziej namacalnych" zagrożeń np. kataklizmy naturalne. RCB wysyła komunikaty o wichurach i nawałnicach. Będzie to robić w odniesieniu do zagrożeń cyber? Wątpię a nawet jeśli to uważam, że byłoby to dalece nietrafione.
17	17MM	I		x				
18	18WM	U		x				Powinna istnieć jednostka w całości czuwająca nad zarżeniami usług kluczowych i IK może ty być RCB lub inny powołany do tego organ. Natomiast istnienie centrum gromadzącego i analizującego dane nie wyklucza istnienia wyspecjalizowanych jednostek zajmujących się

								np. niebezpieczeństwem, które raportują dane do centralnego ośrodka. Jednak takie działanie ma sens po wprowadzeniu nowej ustawy o zarządzaniu kryzysowym implementującej dyrektywę CER.
19	19DJ	A					x	Różne zadania, różne cele. Po drugie, RCB jest organem wspierającym Premiera, więc taka zmiana oznaczałaby de facto poszerzenie uprawnień Premiera. Nie ma w tym nic złego – taka koncepcja była rozważana. Została jednak odrzucona na rzecz obecnie istniejącego rozwiązania (większy udział ministrów działowych).
20	20MA	B				x		Po raz kolejny zachęcam do przyjrzenia się systemowi integracji cyberbezpieczeństwa w struktury zarządzania kryzysowego na przykładzie USA. CISA nie jest jednostką obejmującą pełne zarządzanie kryzysowe. Ma jednak kompetencje właściwe do tego, aby skutecznie realizować procedury reagowania kryzysowego, jednocześnie mając pełen mandat do zapobiegania kryzysom bez angażowania jednostek zarządzania kryzysowego. RCB nie wydaje się w obecnej formie w pełni kompetentne do przejęcia roli centralnego zarządzania, jednocześnie, zarządzanie centralne wydaje się podatne na słabości projektowe w przypadku zagrożeń cyber.
21	21DM	B, U	x					Warto skorzystać z doświadczeń innnych krajów takich jak Izrael lub Estonia, gdzie zagrożenia są traktowane realnie. RCB mogłoby stanowić centrum kompetencji centralnych i koordynacji działań w tym również wymuszać dostęp do informacji o incydnetach, koordynować reagowanie jako HUB pomiędzy różnymi CERTami centralnymi/sektorowymi oraz wspierać nadzór realizacji obowiązków czego nie realizują CERTy./ csirty sektorowe.
22	22SP	B			x			
23	23SW	I, U		x				Do zapewnienia interoperacyjności systemu cyberbezpieczeństwa niezbędny jest element między- i ponadresortowy. RCB może realizować tę funkcję.
24	24MA	I			x			Kierunek zmian wydaje się być właściwy, aczkolwiek przy zbyt powierzchownej wiedzy operacyjnej o systemie zarządzania kryzysowego trudno odpowiedzieć twierdząco.
25	25KD	I	x					
26	26SP	B		x				
27	27KA	B		x				j.w. Oczywiście natrafimy na problem braku wykwalifikowanych kadr (i ich adekwatnego wynagradzania) co w administracji państwowej jest ciągle problemem nierozwiązywalnym. *Ustawa o KSC (w wersji 1.0), mimo że niedoskonała nie została dotychczas skutecznie wdrożona. Za chwilę mamy wersję 2.0, którą nieco poprawia mankamenty poprzedniej, jednak jej skuteczne wdrożeni to też lata. Sklonowano CSIRTy, zatem nie mamy jednego, całościowego spojrzenia na cyber-sytuację w kraju. Budowany system S46, który ma być elementem spinającym i integrującym, to ciągle przyszłość. Zatem te podmioty, które mają wyższy poziom świadomości co do cyberzagrożeń samodzielnie próbują tworzyć i wdrażać strategie cyberbezpieczeństwa (jeśli dodatkowo mają środki na to). Zdecydowanie za mało*

								wysiłku Państwa jest wkładane w budowanie cyberświadomości na wszystkich poziomach – zarówno w administracji jak i poza.
28	28RM	U		x				Taka koordynacja jest potrzebna, ale patrząc na obecną strukturę RCB trudno mi sobie wyobrazić, aby była możliwa.
29	29GW	B		x				
30	30RT	B, U	x					Pełna zgoda co do ról pełnomocnika Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa, Punktów Kontaktowy ds. Cyberbezpieczeństwa, CSIRTy i włączenie Pełnomocnika Rządu ds. Cyberbezpieczeństwa do interoperacyjności. Tylko sprawny przepływ komunikacji, pomiędzy tą trójką daje podstawy do zorganizowania tzw. sztabu operacyjnego akcji, z kótrego wynika działanie operayjne w dół.
31	31BC	A		x				
32	32KW	B	x					bez centralizacji nie ma żadnej szansy na osiągnięcie efektywności.
33	33MM	B, U			x			rozwiązanie jest kuszące, ale raczej nie przy tym kształcie RCB. Wydaje mi się, że lepszym rozwiązaniem jest powołanie dedykowanej agencji do realizacji takiego celu
34	34RA	B				x		trudno mi sobie wyobrazić sytuację podejmowania decyzji operacyjnych przez organ centralny względem np. wyłączenia czy odbudowy systemu w jednostce samorządowej.
35	35KM	B, U		x				Taka ingerencja prawdopodobnie wywołałaby konieczność zmian ustawowych jednak docelowo RCB powinien zarządzać tym obszarem. Mnożenie bytów dalece komplikuje koordynowanie działań.
36	36ŁP	I, U		x				Jw. *Spójność organizacyjna, zarządcza i procesowa to jedyna droga do skuteczności. Wszystko zależy od kompetencji uczestników tych procesów na wszelkich poziomach, ale co do systemowości rozwiązania tak właśnie powinno być.*
37	37WW	B		x				W kontekście cyberbezpieczeństwa krajowego im prostszy model zarówno odpowiedzialności jak i decyzyjności tym lepiej dla systemu. Ostatecznie uczestnicy tego systemu powinni móc łatwo w nim uczestniczyć – zgłaszać, ale również z niego czerpać.
38	38SM	U					x	j.w. *Przyjęcie rozwiązania sektorowego ustanawiającego organy właściwe ds. cyberbezpieczeństwa na poziomie właściwych ministerstw jest odpowiednie.*
39	39ŁT	B				x		Harmonizacja – ok. Np. rozszerzanie roli struktur jednego podmiotu w obszarze cybersecurity nie zadziała wg mnie należycie, chyba że powstanie wiele CSIRTów sektorowych, które będą takim proxy pomiędzy strukturami RCB i podmiotami zaangażowanymi w krajowy system cybersec.
40	40WR	B			x			Co do zasady uważam, że kompetencje w zakresie cyberbezpieczeństwa powinny pozostać w obecnym, czyli niezintegrowanym z systemem zarządzania kryzysowego modelu.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1

								Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.
42	42JD	B, U			x			Ciekawy punk widzenia, możliwe, że ustabilizowane struktury będą funkcjonowały sprawniej
43	43PS	B	x					j.w. konieczność zapewnienia jednolitości podejścia jest kluczem do efektywności KSC. *Tylko jednolite podejście do cyberbezpieczeństwa może zapewnić adekwatne i wystarczająco szybkie decyzje w przypadku kryzysów.*
44	44KP	B	x					
45	45SP	B				X		

2.4. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowane w pkt. 2.3. powyżej zaangażowanie RCB w zarządzanie cyberbezpieczeństwem RP, zgodnie z zasadami i na wzór rozwiązań określonych w systemie zarządzania kryzysowego, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób:

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	**Sposób funkcjonowania proponowanego zorganizowania zarządzania cyberbezpieczeństwem RP**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**
1	RCB powinno mieć pełną odpowiedzialność za koordynowanie zintegrowanego zarządzania (identyfikowania zagrożeń, szacowania ryzyka, planowania i programowania działań) bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym					
2	RCB powinno mieć wiodącą rolę w zintegrowanym zarządzaniu bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, realizując w zakresie cyberbezpieczeństwa zadania, jak w zarządzaniu kryzysowym, w ścisłej współpracy z i w granicach kompetencji organów powołanych ustawą KSC, takich jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy ds.					

	Cyberbezpieczeństwa, organy właściwe, CSIRTy poziomu krajowego oraz podmiotów właściwych i organów regionalnych (np. wojewódzkich) zarządzania kryzysowego					
3	RCB powinno mieć ulokowane w swoich strukturach funkcje i kompetencje przypisane organom ustanowionym przez ustawę KSC, takim jak: Pełnomocnik Rządu ds. Cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy ds. Cyberbezpieczeństwa, i w pełni odpowiadać za koordynowanie zintegrowanego zarządzania bezpieczeństwem krajowym w zakresie zarządzania kryzysowego i cyberbezpieczeństwa					

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				1, 2, 3		W obecnej formie RCB nie jest w stanie pełnić takich funkcji. Jest ich za mało i działają za mało dynamicznie.
2	2UM	B		2				Rozwiązanie przedstawione w punkcie 2 wydaje się właściwe, nie prowadzi do silnej koncentracji wszystkich zadań i uprawnień dotyczących nieraz bardzo odległych kompetencji. Nadmierna centralizacja, zwłaszcza dokonana skokowo mogłaby spowodować pogorszenie jakości procesu zarzadzania cyberbezpieczeństwem wskutek nadmiaru zadań ciążących na RCB
3	3BS	B						
4	4SK	U					1, 2, 3	Nie widzę potrzeby integracji obu systemów. RCB nie ma potencjału ani władczości, aby koordynować to zagadnienie. ABW jest krajową władzą bezpieczeństwa i może pełnić rolę integrującą.
5	5MK	B, U					1, 2, 3	zarządzanie kryzysowe w RP sprawuje Rada Ministrów, a nie RCB. Jeśli już jakiś organ ma mieć władcze kompetencje ponadresortowe, to RZZK.
6	6ST	I, U	3		1, 2			
7	7KG	B			2			Przepisy o zarządzeniu kryzysowym oraz o krajowym systemie cyberbezpieczeństwa powinny się uzupełniać i moim zdaniem nie powinno się ich integrować do jednego systemu bezpieczeństwa.
8	8DP	A				1, 2, 3		Podobnie jak w punkcie 2.3 - optymalnym rozwiązaniem byłyby, gdyby zostało stworzone osobne ponadresortowe centrum cyberbezpieczeństwa, które ściśle współpracowałoby z Rządowym Centrum Bezpieczeństwa.
9	9KM	B	3					

10	10BD	A			1, 2, 3	3		Będzie można stwierdzić po stopniu zrealizowania celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
11	11KP	B		2	3	1		Jak wyżej. *Wydzielenie kompetencji i ich harmonizacja pod egidą RCB (jako jednego miejsca przypisanej odpowiedzialności) wydaje się dobrym kierunkiem. Nadal jednak, procesy muszą być operacjonizowane oddzielnie.*
12	12PM	B			3		1, 2	Uważam, że organizacja cyberbezpieczeństwa nie powinna być domeną urzędników, ale raczej wojska.
13	13RP	I				1, 2, 3		odpowiedź jak w punkcie 1.3. *organizacja Krajowego Systemu Cyberbezpieczęństwa RP jest tematem o znacznie szerszej perspektywie niż sam system zarządzania kryzysowego. Dobrze byłoby znaleźć punkty styku w istotnych aspektach, jak np. dotyczących m.in. wyników szacowania ryzyka oraz z niego wynikającego zapewnienia niedoborów czy braków kluczowych zasobów, ponadto w aspekcie planów ciągłości działania i z nim zharmonizowanie planów. Ważnym aspektem są również kluczowe ryzyka ze względu na Cyberbezpieczęństwo Państwa, które powinny zostać uwzględnione w planach mitygujących zagrożenia ze względu na np. skutki. Jak przykładowo zapewnienie profesjonalnego wsparcia w zakresie np. usług analizy powłamaniowej i odtworzenia / przywrócenia ciągłości działania usług kluczowych. W pełni całkowita integracja i połączeniu obu systemów w jeden nie byłoby możliwe ze względu na fakt, że zarządzanie kryzysowe ze swojej natury odwołuje się głównie do skutków, natomiast w zarządzaniu Krajowym Systemem Cyberbezpieczęństwa główne akcenty kładzie się na zapobieganie powstaniem ewentualnych incydentów. Zatem warto dokonać ścisłej integracji obu systemów tam, gdzie następują związki przyczynowo-skutkowe i zastosować podejście procesowe jako obowiązkowe ze względu choćby na dobrze określony zakres odpowiedzialności porządkujący ewentualne z tego tytułu kwestie wypływające.*
14	14CT	B		1, 2, 3				Każda armia ma jednego naczelnego dowódcę.
15	15MB	A				1, 2, 3		Zadania są inne, podporządkowanie zarządzaniu kryzysowemu nie jest konieczne.
16	16KR	B		1		2	3	
17	17MM	I	3			1, 2		
18	18WM	U		2		1, 3		Powinna istnieć jednostka w całości czuwająca nad zarżeniami usług kluczowych i IK może ty być RCB lub inny powołany do tego organ. Natomiast istnienie centrum gromadzącego i analizującego dane nie wyklucza istnienia wyspecjalizowanych jednostek zajmujących się np. niebezpieczeństwem, które raportują dane do centralnego ośrodka. Jednak takie działanie ma sens po wprowadzeniu nowej ustawy o zarządzaniu kryzysowym implementującej dyrektywę CER.
19	19DJ	A		2			1, 3	Uzasadnienie jak wyżej.

20	20MA	B		1, 3		2		Koordynacja zgoda, operacyjne procesy jednak to za daleko z uwagi na słabości centralnego zarządzania kryzysem.
21	21DM	B, U	2, 3	1				Wyzwaniem będą kwestie kompetencji ustawowych organów centralnych. Jednak należy dożyć do centralizacji kompetencji i obowiązkó na szczeblu krajowych gdyż jedto to jedyny efektywny sposób reakcji w sytuacji kryzysowej zaś scenariusze sytuacji kryzysowej w zarządzaniu kruyzysowym już zawierają incydenty cyber podobnie jak plany obronne oraz opiniowanie planów IK...i na poziomie wojewody odpowiadają za nie inne Oddziały (Oddział Obronny i WCZK) nie zawsze jest to skoordynowane - teoretycznie WCZK może nie mieć wglądu/wiedzy o istnieniu IK na terenie województwa oraz co zawiera Plan ochrony IK tworząc swoje własne plany ZK dla samorządów...
22	22SP	B		3	1, 2			
23	23SW	I, U	2		3	1		RCB nie może brać odpowiedzialności za skutki cyberataków na osiąganie celów biznesowych organizacji. Ta odpowiedzialność może dotyczyć tylko wpływu na bezpieczeństwo publiczne. Rola RCB będzie musiała być ponownie zdefiniowana po wejściu w życie dyrektywy CER. Opisana w dyrektywie „właściwa władza" ma kompetencje znacznie wykraczające poza możliwości obecnego RCB, które nie ma statusu organu administracji publicznej.
24	24MA	I			1, 2, 3			Kierunek zmian wydaje się być właściwy, aczkolwiek przy zbyt powierzchownej wiedzy operacyjnej o systemie zarządzania kryzysowego trudno odpowiedzieć twierdząco.
25	25KD	I		1	2, 3			Dla wysokiej skuteczności systemu konieczne jest wskazanie podmiotu jednoznacznie odpowiedzialnego za dany obszar i posiadającego odpowiednie kompetencje i narzędzia. W sytuacjach konieczności szybkiego i skutecznego działania jedynie wiodąca rola nie sprawdzi się
26	26SP	B			1, 2	3		
27	27KA	B	1, 2, 3					
28	28RM	U		1, 2, 3				Powyższe postulaty są interesujące, ale wymagają w pierwszej kolejności refleksji nad pozycją prawną RCB i relacji z innymi podmiotami odpowiedzialnymi za obszar cyberbezpieczeństwa.
29	29GW	B	1, 2, 3					
30	30RT	B, U	3					RCB musi mieć sztab kryzysowy (j.w.) To jedyny organ efektywnie gospodarujący bazą danych i posiadających już kompetencje alarmowe i komunikacyjne oraz infrastrukturę.
31	31BC	A	1, 2, 3					
32	32KW	B	1, 3			2		jak wyżej *bez centralizacji nie ma żadnej szansy na osiągnięcie efektywności*
33	33MM	B, U						nie udzielam odpowiedzi, ponieważ jak wskazałem raczej nie zgadzam się takim rozwiązaniem
34	34RA	B	2	3			1	uzasadniłem powyżej

								trudno mi sobie wyobrazić sytuację podejmowania decyzji operacyjnych przez organ centralny względem np. wyłączenia czy odbudowy systemu w jednostce samorządowej
35	35KM	B, U	2					RCB jako jednostka posiadająca doświadczenie powinna mieć wiodącą rolę, jednak powinna podlegać nadzorowi zgodnie z NIS.
36	36ŁP	I, U	3					to ogranicza rozrost obszarów wsparciowych (podwójny HR, adm., etc).
37	37WW	B		3				Uproszczenie odpowiedzialności za zarzadzanie kryzysami w obszarze takim jak cyberbezpieczeństwo jest wskazane ze względu na szybkość i konieczność podejmowania jednoznacznych decyzji.
38	38SM	U					1, 2, 3	
39	39ŁT	B				3	1, 2	Diabeł tkwi w szczegółach. Pełna odpowiedzialność za koordynację to wciąż zbyt dużo. Na pewno RCB powinno być ważnym, ale nie głównym elementem całego systemu cyberbezpieczeństwa w Polsce. Bardziej wierzę w koordynację branżową / sektorową – ze względu na wspólną znajomość zagrożeń w grupie podmiotów danego typu.
40	40WR	B		1				Rozłożenie kompetencji na kilka podmiotów może wydłużać proces decyzyjny, rozmywać odpowiedzialność oraz rodzić spory kompetencyjne. Lepszym rozwiązaniem jest ustanowienie jednego organu odpowiedzialnego za daną rzecz, w tym przypadku cyberbezpieczeństwo. Warto zadbać w takiej sytuacji o zmianę powiązanych aktów prawnych w celu wyeliminowania ryzyka wystąpienia ograniczeń prawnych w przepływie informacji pomiędzy podmiotami w systemie cyberbezpieczeństwa (np. dzisiaj ABW nie może przekazywać informacji istotnych dla bezpieczeństwa Państwa (RCB).
41	41ŁJ	A			1, 2, 3			Odpowiedź jak w pytaniu 1.2. *Analiza sposobu organizacji krajowego systemu cyberbezpieczeństwa, w tym jego powiązań ze sferą zarządzania kryzysowego, ustawą o działaniach antyterrorystycznych została przeprowadzona na etapie projektowania ustawy o krajowym systemie cyberbezpieczeństwa, w których uczestniczyłem w czasie pracy w Ministerstwie Cyfryzacji. Powyższe zostało skonsultowane w ramach rządowego procesu legislacyjnego i w Sejmie. Część informacji na ten temat zawiera uzasadnienie do ustawy o krajowym systemie cyberbezpieczeństwa. Inicjatywa zmian legislacyjnych – właściwość KPRM.*
42	42JD	B, U		1, 2, 3				
43	43PS	B	1, 2, 3					RCB powinno pełnić wiodącą rolę w organizowaniu KSC, jako podmiot ulokowany wystarczająco wysoko w strukturach Państwa.
44	44KP	B		1, 2, 3				
45	45SP	B				1, 2, 3		

2.5. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Podmioty systemu zarządzania kryzysowego, takie jak: RCB - koordynujące krajowe działania antykryzysowe, jak i podmioty regionalne, np. poziomu wojewódzkiego (wojewoda, WCZK, WZZK) powinny być włączone, zarówno do informowania o zagrożeniach cyberbezpieczeństwa oraz o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa, jak i do obsługi i zarządzania tymi incydentami.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B		x				Im więcej źródeł informacji o incydentach tym lepiej niemniej musiałby by to być skoordynowane, aby nie spowodować chaosu komunikacyjnego
2	2UM	B		x				W obecnym stanie mojej wiedzy o faktycznym stanie wiedzy i kompetencjach wymienionych organów trudno jest mi określić zdecydowanie czy wskazane podmioty odpowiadające za działania antykryzysowe byłyby w stanie udźwignąć ciężar zarządzania incydentami cyberbezpieczeństwa skoro nie bardzo radzą sobie z tym CSIRT-y. Natomiast funkcja informacyjna o tych incydentach (przekazywanych przez m.in. CSIRT-y) byłaby pożądana i możliwa do zrealizowania
3	3BS	B						
4	4SK	U		x				Z pierwszą częścią się zgadzam. Z drugą nie = obsługa i zarządzanie incydentami
5	5MK	B, U	x					RCB nie koordynuje krajowych działań antykryzysowych, ale powinno być zasilane tymi danymi
6	6ST	I, U		x				
7	7KG	B		x				Obecnie RCB jest włączone do informowania o zagrożeniach cyberbezpieczeństwa oraz do informowania o incydentach istotnych, poważnych i krytycznych cyberbezpieczeństwa np. poprzez przekazywanie operatorom infrastruktury krytycznej ostrzeżeń i alertów wydawanych przez CSIRT GOV. Jednak do zarządzania incydentami dla operatorów infrastruktury krytycznej właściwym jest CSIRT GOV co moim zdaniem skraca proces obsługi zdarzenia. RCB i tak jest włączony do tego procesu, gdyż organizuje pracę dla Zespołu ds. Incydentów Krytycznych, o którym mowa w art. 36 ust. 4 UKSC.
8	8DP	A	x					Należałoby wykorzystać do informowania społeczeństwa o zagrożeniach takie systemy jak „AlertRCB” oraz „Regionalny System Ostrzegania”.
9	9KM	B	x					Jako członek zespołu, a nie lider.
10	10BD	A		x				Zaangażowanie w/w podmiotów będzie właściwe ze względu na zakres ich zadań.
11	11KP	B				x		Podmioty dedykowane zarządzaniu kryzysowemu powinny być włączane tylko w te incydenty, które mogą prowadzić do zakłócenia funkcjonowania danych struktur państwowych. Bezzasadne wydaje się włączanie struktur dedykowanych zarządzaniu kryzysowemu

								wszystkim działaniom (w szczególności incydentom), którymi zajmują się jednostki dedykowane cyberbezpieczeństwu. Nie każdy incydent – a tych z natury zagrożeń cyberprzestrzeni jest dużo – prowadzi do kryzysu.
12	12PM	B					x	Tego typu zadania są domeną menadżerów bezpieczeństwa informacji i wojska oraz wywiadu. Zdecydowanie nie jest to domena polityków ani urzędników, ani administracji. Moim zdaniem proponowana struktura nie jest w stanie poprawić cyberbezpieczeństwo, ani nie pozwoli na efektywne wykorzystanie środków, jakie przeznaczamy na cyberbezpieczeństwo.
13	13RP	I	x					w zarządzaniu cyberbezpieczeństwem potrzebna jest natychmiastowa reakcja i wsparcie na wypadek materializacji się ryzyk np. w obszarze braku dostępności usług. Potrzeba wówczas szybkiej reakcji na incydenty w trybie 24/7, czy w zakresie realizacji inwestygacji powłamaniowej, jak i usuwanie skutków incydentów, a nawet w sytuacji ostatecznej np. przenoszenie do zapasowej infrastruktury czy innego centrum przetwarzania w przypadku zniszczenia wszystkich ośrodków przetwarzania, gdzie wcześniej usługa była świadczona.
14	14CT	B		x				Powinny mieć wiedzę oraz dostęp do informacji – incydent z zakresu cyberbezpieczeństwa może mieć przełożenie na zarządzanie kryzysowe.
15	15MB	A				x		Zadania są inne.
16	16KR	B				x		
17	17MM	I		x				
18	18WM	U				x		Powinna istnieć jednostka w całości czuwająca nad zarżeniami usług kluczowych i IK może ty być RCB lub inny powołany do tego organ. Natomiast istnienie centrum gromadzącego i analizującego dane nie wyklucza istnienia wyspecjalizowanych jednostek zajmujących się np. niebezpieczeństwem, które raportują dane do centralnego ośrodka. Jednak takie działanie ma sens po wprowadzeniu nowej ustawy o zarządzaniu kryzysowym implementującej dyrektywę CER.
19	19DJ	A		x				W przypadkach, kiedy istnieje ryzyko, że incydent doprowadzi do sytuacji kryzysowej, RCB powinno być informowane. Nie powinno być włączone na poziomie operacyjnym, bo to nie jest ten typ podmiotu, ale informowane.
20	20MA	B	x					W zakresie informowania i jako właściciel/interesariusz dla wpływu incydentu na dany region jest to właściwy kierunek zarządzania i zalecana praktyka.
21	21DM	B, U				x		Organ wojewody nie posiada obecnie stosownych kompetencji praktycznych a zagrożenia pochodzą spoza województwa a nawet kraju zatem obsługa zarządzania tylko w niektórych przypadkach a nie co do zasady. Również Policja nawet na poziomie Komendy Wojewódzkiej, gdzie jest zespół Cyber nie radzi sobie z reagowanie a raczej wolno reaguje po fakcie zbierając dowody. Z mojego doświadczenia wynika ze najefektywniej radzą sobie CERTy/ CSIRTy na poziomie krajowym /sektorowym które mają poważanie międzynarodowe i same nawiązują współpracuję międzynarodową, co zwiększa ich skuteczność.

22	22SP	B		x				
23	23SW	I, U		x				Świadomość publicznych skutków dysfunkcji operatora usługi kluczowej jest informacją ważną w procesie zarządzania kryzysowego. Jednak wymagałoby to zapewnienia transmisji i bezpośredniego dostępu do niejawnych danych. Taki system informatyczny na razie nie istnieje. W projekcie ustawy o KSC wpisano propozycję ustanowienia ISAC realizującego powyższe zadania.
24	24MA	I		x				Kierunek zmian wydaje się być właściwy, a podnoszenie kompetencji w wymienionych podmiotach jest uzasadnione, aby dzięki dostępowi do obrazu świadomości sytuacyjnej krajowego systemu cyberbezpieczeństwa były w stanie właściwie dostarczać dane oraz włączyć się do obsługi i zarządzania incydentami w miarę potrzeb.
25	25KD	I		x				
26	26SP	B		x				
27	27KA	B	x					
28	28RM	U		x				
29	29GW	B	x					
30	30RT	B, U					x	komunikat musi być z jednego źródła = RCB
31	31BC	A		x				
32	32KW	B	x					z zastrzeżeniem przejęcia pełnej odpowiedzialności i z wyłączeniem podmiotów regionalnych.
33	33MM	B, U		x				myślę, że to potencjalnie dobre rozwiązanie, w szczególności dlatego, że takie podmioty działają operacyjnie, a domena cyber coraz częściej jest elementem zarządzania kryzysowego praktycznie w każdej innej dziedzinie. Pozostałyby do ustalenia szczegółowe relacje tych podmiotów z pozostałymi podmiotami KSC
34	34RA	B	x					Jeżeli będzie to z kontekstem to da szanse podmiotom na przygotowanie się i ew. uniknięcie ataku.
35	35KM	B, U	x					Wyrażam pełną zgodność z powyższym stwierdzeniem.
36	36ŁP	I, U		x				Tak, ale te na poziomie regionalnym „włączone” natomiast koordynacja i odpowiedzialność strategiczna na poziomie centrali. Chodzi o zachowanie spójności operacyjnej i komunikacyjnej.
37	37WW	B		x				RCB posiadając wypracowane mechanizmy informowania w kierunku podmiotów i obywateli, ale również zgłaszania informacji przez nich może być naturalnie sprawnym interfejsem dla zagadnień cyberbezpieczeństwa. Warunkiem jest odpowiedzialna i wyszkolona kadra warunkująca wysoka jakość komunikacji.
38	38SM	U					x	

39	39ŁT	B				x		Raczej RCB znają się dobrze na klasycznych działaniach kryzysowych (np. zwalczanie klęsk żywiołowych) a nie na działaniach cybersecurity (brak kompetencji, brak specjalistów). O ile jeszcze rola informacyjna ok, o tyle zarządzanie incydentami nie powinno wg mnie leżeć w ich gestii.
40	40WR	B				x		RCB powinno uzyskiwać tylko informacje dotyczące cyberbezpieczeństwa w kontekście infrastruktury krytycznej.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1. *Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.*
42	42JD	B, U		x				
43	43PS	B				x		Zarządzanie incydentami cyberbezpieczeństwa powinno pozostać domeną CSIRT. Niemniej, konieczne jest adekwatne powiązanie innych podmiotów, takich jak WCZK.
44	44KP	B			x			
45	45SP	B		x				Informowania – TAK obsługa zarządzania tymi incydentami - zapewnienie odpowiednich narzędzi i wykwalifikowanej kadry, na przykład poprzez wykupienie usługi w firmach komercyjnych

2.6. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

CSIRT sektorowe powinny być ustanowione dla każdego sektora kluczowego dla sfery administracyjno-społeczno-gospodarczej kraju, w tym podmiotów realizujących zadania publiczne, w zakresie znacznie szerszym niż obecnie ustawowo zdefiniowana lista CSIRT sektorowych.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	**Respondent**	**Obszar**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**	**Uzasadnienie odpowiedzi:**
1	1BM	B		x				Nie do końca może zgodzę się dla każdego sektora. CSIRT to są niemałe stałe koszty wiec ich ilość należy przemyśleć. Niemniej kilka sektorowych CSIRT’ów by się przydało
2	2UM	B				x		Obecny stan wskazuje na niezdolność do wyczerpania pełnej listy CSIRT-ów sektorowych, poszerzanie tej listy obecnie nie ma sensu. Sytuacja może zmienić się w przyszłości, ale jednym z warunków tej zmiany jest poszerzenie bazy specjalistów mających odpowiednie

								przygotowanie i zdecydowanie bardziej energiczne działania ministra właściwego w celu powołania CSIRTów już ustanowionych.
3	3BS	B					x	Rozbudowa CSIRTów przy obecnym rynku jest kompletną utopią.
4	4SK	U	x					PLANOWANE SĄ TAKIE ZABIEGI
5	5MK	B, U	x					obecne linie wsparcia są niewystarczające. Nie ma np. CSIRTu dla NGOsów.
6	6ST	I, U		x				
7	7KG	B	x					CSIRT sektorowe/podsektorowe powinny być ustanowione dla każdego sektora/podsektora, gdyż specyfika działania każdej branży (sektora, podsektora) jest inna oraz na swój sposób specyficzna. Ponadto istnieją przepisy oraz standardy sektorowe/podsektorowe, które mają lub mogą mieć wpływ na bezpieczeństwo (cyberbezpieczeństwo) w danym sektorze/podsektorze. Także na poziomie EU istnieją oprócz agencji ENISA inne agencje branżowe dedykowane dla danych sektorów/podsektorów, które również wydają wytyczne mające pośredni lub bezpośredni wpływ na poziom bezpieczeństwa w danym sektorze/podsektorze. Dlatego CSIRT-y sektorowe/podsektorowe moim zdaniem mają większą skuteczność by zapewnić właściwy i optymalny do istniejących zagrożeń poziom cyberbezpieczeństwa w danym sektorze/podsektorze.
8	8DP	A		x				Trudno powiedzieć. Wydaje się, że obecny zakres jest wystarczający.
9	9KM	B		x				Specjalizacja.
10	10BD	A			x			Będzie można stwierdzić po stopniu realizacji celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
11	11KP	B		x				Każdy sektor kluczowy/resort z pewnością powinien posiadać własne zespoły (funkcje) odpowiedzialne za zapewnienie bezpieczeństwa. Nie znając szczegółów dotyczących budowy sieci teleinformatycznych na poziomie poszczególnych resortów, o ile możliwe jest monitorowanie i koordynowanie działań będących odpowiedzią na incydent na poziomie centralnym (unifikującym sektory) – taki kierunek wydaje się właściwszy.
12	12PM	B	x					Same CSIRT'y nie zapewnią współpracy i nie zwiększą dostępności wiedzy, narzędzi i nie zapewnią współdziałania (brak mechanizmów zachęcających informatyków i osób odpowiedzialnych za bezpieczeństwo na poziomie firm, urzędów itp.
13	13RP	I	x					CSIRT sektorowy jest w stanie zdecydowanie celniej rozpoznawać zagrożenia ze względu na specyficzne uwarunkowanie. Czym innym są standardy, urządzenia OT, protokoły w przemyśle np. ciężkim czy wydobywczym a czym innym w bankowości czy opiece zdrowotnej. Specyficzne wymagania wynikają z odrębnych kontekstów, zatem aby te konteksty móc rozumieć należy budować CSIRTY sektorowe.
14	14CT	B		x				Każdy wie, do kogo zgłosić – taki byłby efekt.
15	15MB	A		x				Dałoby to szansę na wzrost cyberbepieczeństwa w sektorach.
16	16KR	B	x					
17	17MM	I		x				

18	18WM	U	x					Zostanie to wprowadzone po dostosowaniu polskiego systemu zarzadzania kryzysowego do nowych dyrektyw CER i NIS2
19	19DJ	A			x			CSIRT to drogie przedsięwzięcie, nie zawsze konieczne. W niektórych sektorach, zwłaszcza infrastruktury krytycznej, ma to sens (bankowość, energia), ale w pozostałych wystarczą inne formy (np. wymiana informacji o podatnościach w sektorze uzdatniania wody pitnej albo szybkie wsparcie lotnego zespołu reagowania dla szpitali). Budowa centrum wymiany informacji (ISAC) albo wspólne budowanie kompetencji to równie przydatne, a często pomijane pomysły.
20	20MA	B	x					Nie tyle szerszym co precyzyjniej zdefiniowanym tak aby unikać problemów „problemów niczyich". Jednocześnie bariery informacyjne w zakresie współdzielenia informacji o zagrożeniach muszą być systemowo usunięte, tak aby zapewnić widzialność dla incydentów obejmujących więcej niż jeden sektor.
21	21DM	B, U				x		Nie powinno być z góry narzuconego obowiązku tworzenia csirtow dla wszytkich sektrów. Tutaj kluczowa jest współpraca i ustawa jej nie wymusi przy braku porozumienia. Dlatego należy tylko propoagowac idee csirtów sektorowych bez obowiązku ich ustanowienia – jednoczesnie wymuszając podległosc pod RCB, któ jeśli uzna za konieczne może zawnioskować o powstanie csirtu w sektorach gdzie to będzie uzasadnione.
22	22SP	B				x		
23	23SW	I, U	x					Wymóg SOC sektorowego już jest wpisany do projektu ustawy o KSC. CSIRT sektorowy ze względu na koszty je jest rozwiązaniem ekonomicznym.
24	24MA	I		x				Kierunek zmian wydaje się być właściwy, ale na pewno wymaga dialogu z CSIRT poziomu krajowego oraz organami właściwymi, a także działającym CSIRT sektorowym przy KNF. Taka dyskusja zapewniłaby właściwą wymianę doświadczeń i zwiększyła szanse na przyjęcie rekomendacji, które podniosłyby jakość nowo organizowanych struktur.
25	25KD	I		x				
26	26SP	B		x				
27	27KA	B	x					Celem nadrzędnym musi być doprowadzenie do uzyskania całościowego obaru sytuacji cyberbezpieczeństwa w kraju. Zatem, skoro nie udało się doprowadzić do powołania jednego CSIRY to należy doprowadzić do ich zintegrowania (system S46 ma temu służyć). Ponadto – struktury monitorowania stanu cyberbezpieczeństwa należy rozwijać w szerz i w dół. Zatem zgadzam się z postulatem.
28	28RM	U	x					To raczej nie podlega dyskusji, że tak być powinno – jednocześnie też wiadomo, dlaczego tego nie udało się osiągnąć. W PL dominuje myślenie sektorowo-silosowe, które jest naturalną barierą dla procesowego podejścia warunkującego skuteczny przepływ informacji.
29	29GW	B	x					

30	30RT	B, U	x					Zdecydowanie należy powołac CSIRT dla administracji najwyzszego szczebla państwa i to osobno dla każdej władzy ustawodawczej, wykonawczej, sądowniczej o wyższych kompetencjach np MSWiA, do odcięcia przepływu danych w sektorze energetycznym.
31	31BC	A		x				
32	32KW	B		x				CSIRT'y sektorowe, co do zasady, powinny się skupić na zadaniach klasy threat hunting, dla swojego sektora oraz na wsparciu w realizacji zadań obsługi incydentów dla podmiotów, gdzie zapewnienie profesjonalnej kadry jest nie możliwe, lub nie ma uzasadnienia ekonomicznego.
33	33MM	B, U			x			myślę, że wystarczające byłoby uruchomienie CSIRT-ów sektorowych w istniejącym zakresie i ewentualna korekta tego zakresu w oparciu o doświadczenia operacyjne. Wydaje mi się, że szczegółowe ustalenie zakresu dla CSIRT-ów sektorowych jest dość ryzykowne ze względu na potencjalnie bardzo różne ich role w KSC, uwzględniające poziomy dojrzałości poszczególnych sektorów
34	34RA	B	x					branże mają określone klucze w komunikacji, specyfikę, słownictwo i regulacje.
35	35KM	B, U				x		Na chwilę obecną działa kilka CSIRTow sektorowych. Dopiero po wdrożeniu pozostałych, zebraniu wiedzy i doświadczenia będzie można ocenić zasadność zmian.
36	36ŁP	I, U		x				Im bliżej przeszkoleni specjaliści mają do uczestników procesów tym lepiej wdrażają działania profilaktyczne, nie mówiąc o operacyjnym przeciwdziałaniu zaistniałym zagrożeniom.
37	37WW	B	x					Specyfika poszczególnych sektorów wymaga wręcz powołania specjalizowanych w danym sektorze wykfalifikowanych jednostek posiadających wiedzę specyficzną dla danego sektora przy jednoczesnym merytorycznym odnoszeniu jej w obszarze cyberbezpieczeństwa.
38	38SM	U		x				
39	39ŁT	B	x					Odpowiedź ta łączy się z innymi odpowiedziami w dokumencie. Obecnie system cyberbezpieczeństwa jest (podmiotowo) zbyt wąski i zbyt płytki, a przedmiotowo – zbyt niejasny i ogólny. Dlatego rozszerzenie listy CSIRTów sektorowych to jak najbardziej zasadny pomysł, że poprawić poziom bezpieczeństwa teleinformatycznego kraju.
40	40WR	B			x			To wszystko zależy od analizy ryzyka, a co za tym idzie bilansie korzyści i kosztów.
41	41ŁJ	A		x				Takie założenie wynika już z obowiązujących przepisów ustawowych, niemniej jest to fakultatywne. Powstanie CSIRT sektorowych jest uwarunkowane zapewnieniem finansowania, co potencjalnie w obecnie obowiązujących przepisach oznacza powiązanie z kontekstem sektorowym i możliwościami w tym zakresie.
42	42JD	B, U		x				
43	43PS	B	x					CSIRT sektorowe ma dużo większy poziom wyczucia problemów sektora, w którym został powołany.
44	44KP	B	x					
45	45SP	B		X				

3. Podmioty krajowego systemu cyberbezpieczeństwa

3.1. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Podmioty krajowego systemu cyberbezpieczeństwa operujące w sferze administracyjno-społeczno-gospodarczej (tj.: operatorzy usług kluczowych (OUK), dostawcy usług cyfrowych (DUC), wybrane instytucje centralne, wybrane jednostki administracji publicznej i sektora finansów publicznych, wybrane podmioty realizujące zadania publiczne) są właściwie zdefiniowane, co zapewnia efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Spotkaliśmy się z wieloma dziwnymi sytuacjami takimi jak elektrociepłownia, która jest częścią dużego prywatnego zakłady które kwalifikuje się do UOK i jednocześnie wiele wodociągów dla całkiem dużych miast, które nie są OUK. Duże zamieszanie jest też w obszarze służby zdrowia – patrz szpitale – wiele nie wie czy podlega czy nie.
2	2UM	B				x		Zdecydowanie zawyżono kryteria uznania w co najmniej kilku sektorach podmiotów będących OUK, na przykład w sektorze dostawy wody. Granica 500 tys. Odbiorców powoduje, że znakomita większość tych podmiotów nie jest OUK, a dużych aglomeracji miejskich o poziomie 100 – 400 tys. Jest wiele. Taka kuriozalna sytuacja występuje m.in. na Śląsku, gdzie wskutek podziału dawnego Wojewódzkiego Przedsiębiorstwa Wodociagów i Kanalizacji powstało kilkanaście podmiotów i żaden z nich nie kwalifikuje się na OUK, w tym miasto Katowice liczące ok. 320 tys. mieszkańców.
3	3BS	B				x		Obecnie zakres podmiotów i ich odpowiedzialność jest głównie przyporządkowana do OUK, pozostałe wymagania są dość ograniczone. Projekt NIS 2.0 lepiej to opisuje.
4	4SK	U		x				Tak, bo wątpliwości prowadzą do procesów, zmiany formy organizacyjnej działalności itd. wszystko, żeby ominąć przepisy UKSC
5	5MK	B, U		x				ważne, żeby aktualizować te wykazy i jasno określić role i odpowiedzialność
6	6ST	I, U		x				
7	7KG	B				x		Zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Uchwalenie dyrektywy NIS2 znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC.
8	8DP	A	x					W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz w odpowiednich rozporządzeniach podmioty te zostały szczegółowo zdefiniowane.

9	9KM	B		x				Brakuje wielkoobszarowych rolników, którzy mają bezpośredni wpływ na bezpieczeństwo państwa.
10	10BD	A		x				W/w podmioty zostały określone zgodnie z kryteriami przyjętymi w USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
11	11KP	B			x			
12	12PM	B					x	W/w elementy nie zapewniają transferu wiedzy, narzędzi i nie minimalizują kosztu, za to konserwują reaktywny układ
13	13RP	I			x			nie mam zdania czy są one właściwie zdefiniowane, aby zapewnić efektywność KSC i odpowiedniego poziomu bezpieczeństwa Państwa.
14	14CT	B			x			
15	15MB	A				x		Można byłoby bardziej dokładnie zdefiniować np. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.);
16	16KR	B				x		Praktyka pokazuje wiele błędnie wydanych decyzji dla OUK i pomijanie podmiotów o znacznie większym wpływie na cyberbezpieczeństwo.
17	17MM	I				x		
18	18WM	U				x		Obecnie nie ma jasnego kryterium wyłaniania operatorów usług kluczowych.
19	19DJ	A	x					Definicje podmiotów z UKSC są oparte na prawie unijnym (co zapewnia porównywalność z innymi państwami), uwzględnia potrzeby sektorowe i różnice w podejściu do krytyczności usług i stosowanych technologii.
20	20MA	B				x		Obecny system definicji wspiera bariery informacyjne pomiędzy zdefiniowanymi podmiotami i prowadzi do konfliktów interesów lub przekazywania „wg kompetencji” co istotnie wpływa na opóźnienie procesu reakcji na incydent.
21	21DM	B, U		x				Tak, ale nie ma koordynacji działań. Istnieje kilka przepisów prawa, które są rozłączne zarówno na poziomie centralnym jak oddzielne są zespoły odpowiedzialne za ich realizację. Każdy oddzielnie realizuje wymagania, jednak nigdy nie wystąpiła sytuacja wymagająca koordynacji realnych działań, nawet ćwiczenia i gry sztabowe każdy z podmiotów realizuje oddzielnie. Są to: RCB dla IK i zarządzania kryzysowego, ABW dla działań antyterrorystycznych, Cert sektorowy dla dyrektywy NIS i ustawy KSC, KPRM dla ustawy “o stanach wyjątkowych”
22	22SP	B		x				
23	23SW	I, U				x		Brak podejścia usługowego do typowania infrastruktury krytycznej.
24	24MA	I				x		Aktualnie wśród pomiotów KSC brakuje m.in. przedsiębiorstw telekomunikacyjnych/komunikacji elektronicznej, podmiotów odpowiadających za rejestry państwowe, jednostki finansów publicznych i realizujących zadania publiczne, a także wystarczająco świadomych swojej roli DUC. Rozszerzenie grup podmiotów, które niesie ze sobą dyrektywa NIS2

								dodatkowo zwiększy spektrum wyzwań związanych z reorganizacją KSC, ale jednocześnie podniesie potencjalną efektywność systemu, którą będzie trzeba osiągnąć.
25	25KD	I				x		
26	26SP	B				x		
27	27KA	B				x		Istnieją przykłady instytucji niezwykle ważnych dla bezpieczeństwa ekonomicznego państwa, które nie zostały wskazane jako OUK.
28	28RM	U					x	Gdyby tak było, Komisja nie proponowałaby wprowadzenia NIS2. Proszę zwrócić uwagę, że przyjęcie NIS2 między innymi ma rozwiązać problem z niespójnym definiowaniem OUK przez poszczególne państwa członkowskie.
29	29GW	B		x				
30	30RT	B, U		x				nie ma błędu w zdefiniowanych rolach ww podmiotów
31	31BC	A			x			
32	32KW	B		x				dyrektywa NIS2 powinna poprawić kryteria, jednocześnie należy zadbać, aby podmioty prywatne nie były pomijane ze względów politycznych.
33	33MM	B, U		x				nie znane mi są szczególne problemy związane ze zdefiniowaniem tych podmiotów
34	34RA	B				x		Własnie dlatego że są wybrane w drodze decyzji administracyjnej.
35	35KM	B, U			x			Faktem jest, że obecnie trwa ewaluacja i projektowanie zmian do ustawy i dyrektywy, jednak mamy za mało danych, aby jednoznacznie ocenić prawidłowość zdefiniowania oraz efektywność KSC.
36	36ŁP	I, U			x			
37	37WW	B				x		Odnosząc się wertykalnie do tego zagadnienie zapewne definicja jest zbliżona do poprawnej jednak w ujęciu horyzontalnym brakuje odniesienia do współpracujących pomiędzy sobą podmiotów np. produkcja energii jest zestawem działań związanych z wieloma podmiotami od dostawy paliwa, z którego jest ta energia produkowana aż po system dystrybucji do odbiorców końcowych. To różne podmioty, które ostatecznie powinny przy współpracy zapewniać stabilne działanie sieci energetycznej.
38	38SM	U		x				
39	39ŁT	B					x	Definicje zbyt ogólne, kryteria doboru - krótkie, lista podmiotów – utajniona. Nie tak to powinno wyglądać.
40	40WR	B		x				Nie spotkałem się z opinią by były tu jakieś większe niedociągnięcia.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1. *Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.*

42	42JD	B, U				x		Np. DUC w moim odczuciu nie jest dobrze zdefiniowany, OUK obecnie podstawą jest decyzja administracyjna
43	43PS	B					x	Obecny system, gdzie OUK wskazywane są przez OW generuje z jednej strony prostotę, a z drugiej strony łatwe zwolnienie się części podmiotów z spełniania obowiązków, które powinny wypełniać. Podejście proponowane w NIS2 są w tym względzie dużo bardziej adekwatne.
44	44KP	B		x				
45	45SP	B		x				Efektywność zależy także od przeznaczonych i zaangażowanych środków, nie tylko od tego, czy podmiot został właściwie zdefiniowany.

3.2. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Krajowy system cyberbezpieczeństwa powinien obejmować znacznie szerszy katalog typów podmiotów, niż ustawowo zdefiniowany, i być rozszerzony, co najmniej, o wszystkie podmioty wskazane w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa (np. o działaniach antyterrorystycznych, o obronie ojczyzny i innych), a także zawierać szerszy katalog typów podmiotów, klasyfikowanych jako dostawcy usług cyfrowych.

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B		x				Na pewno powinno być to uspójnione
2	2UM	B		x				W tym przypadku należy raczej poczekać na ewentualne wejście w życie dyrektywy unijnej której projekt znany jest pod nazwą NIS II, na razie istotniejsze jest wskazane w poprzednim punkcie obniżenie kryteriów powodujących uznanie podmiotów które już są w zasięgu uksc jako sektor lub podsektor, ale z powodu wysokiego pułapu na ogół jedynego kryterium się nie znalazły na liście OUK
3	3BS	B		x				Jw. W 3.1 Obecnie zakres podmiotów i ich odpowiedzialność jest głównie przyporządkowana do OUK, pozostałe wymagania są dość ograniczone. Projekt NIS 2.0 lepiej to opisuje.
4	4SK	U	x					Katalog będzie rozszerzany
5	5MK	B, U		x				KSC powinien dotyczyć styku każdego obywatela z cyberprzestrzenią
6	6ST	I, U		x				
7	7KG	B	x					Zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia

								usług kluczowych. Uchwalenie dyrektywy NIS2 znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC.
8	8DP	A		x				Jeżeli wskazane „w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa" podmioty realizują zadania przy użyciu systemów informacyjnych, to powinny być ujęte we wskazanym katalogu.
9	9KM	B	x					WiNES
10	10BD	A			x			Będzie można stwierdzić po stopniu realizacji celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
11	11KP	B		x				Rozszerzenie katalogu podmiotów, a w zasadzie jego doprecyzowanie może pozytywnie wpłynąć na świadomość w obszarze cyberbezpieczeństwa.
12	12PM	B	x					Jak we wcześniejszych odpowiedziach
13	13RP	I			x			Nie mam zdania. Zasadniczo im system jest czytelniejszy i czytelniejsze są kryteria oceny w interpretacji i tym mniej budzą wątpliwości, a interesariuszy mają konkretne wymagane obowiązki, wskazane rolę i wiedzą za co odpowiadają i w jakim zakresie. Stworzenie jasnego katalogu zawierającego wszystkie usługi i podmioty za nie odpowiadające i w jakim zakresie byłoby bardzo pomocne. Choć jej jawne upublicznienie mogłoby być też i niebezpieczne.
14	14CT	B		x				Znam podmioty, które świadczą istotne usługi i cieszą się, że nie ma ich w katalogach ustawowych, bo to „wymagałoby wydatków".
15	15MB	A			x			Pytanie jest zbyt przekrojowe jak na moją wiedzę.
16	16KR	B	x					
17	17MM	I		x				
18	18WM	U	x					Tego typu zmiany są już projektowane w dyrektywie CER i NIS2.
19	19DJ	A			x			Katalog podmiotów powinien być poszerzony, ale należałoby zapewnić wcześniej stopniowanie obowiązków (por. odpowiedź do pytania 1.3).
20	20MA	B		x				Z uwzględnieniem aspektu cyfryzacji tych podmiotów.
21	21DM	B, U	x					Istnieje kilka przepisów prawa, które są rozłączne, zarówno na poziomie centralnym, jak oddzielne są zespoły odpowiedzialne za ich realizację. Każdy oddzielnie realizuje wymagania, jednak nigdy nie wystąpiła sytuacja wymagająca koordynacji realnych działań, nawet ćwiczenia i gry sztabowe każdy z podmiotów realizuje oddzielnie. Są to: RCB dla IK i zarządzania kryzysowego, ABW dla działań antyterrorystycznych, Cert sektorowy dla dyrektywy NIS i ustawy KSC, KPRM dla ustawy "o stanach wyjątkowych"
22	22SP	B				x		
23	23SW	I, U	x					Postulat zostanie zrealizowany w chwilą implementacji dyrektywy CER i wdrożenia podejścia usługowego do wyłaniania IK.

24	24MA	I	x					Jw. *Aktualnie wśród pomiotów KSC brakuje m.in. przedsiębiorstw telekomunikacyjnych/komunikacji elektronicznej, podmiotów odpowiadających za rejestry państwowe, jednostki finansów publicznych i realizujących zadania publiczne, a także wystarczająco świadomych swojej roli DUC. Rozszerzenie grup podmiotów, które niesie ze sobą dyrektywa NIS2 dodatkowo zwiększy spektrum wyzwań związanych z qreorganizacją KSC, ale jednocześnie podniesie potencjalną efektywność systemu, którą będzie trzeba osiągnąć.*
25	25KD	I	x					
26	26SP	B				x		
27	27KA	B	x					Jest o oczywiste. To, że tego twórcy ustawy nie uczynili być może wynika z podejścia „nie wszystko na raz, bo się udławimy" (przepraszam za kolokwializm.
28	28RM	U				x		Nie każdy podmiot, który wykonuje ważne zadania (publiczne itp.) jednocześnie jest wrażliwy w dziedzinie cyber.
29	29GW	B			x			
30	30RT	B, U		x				Raczej tak, brakuje mi pewnych jednostek jak szpitale, portale społecznościowe, porty lotnicze, imprezy masowe, inne nie scharakteryzowane w ustawie
31	31BC	A		x				
32	32KW	B		x				Jak wyżej *dyrektywa NIS2 powinna poprawić kryteria, jednocześnie należy zadbać, aby podmioty prywatne nie były pomijane ze względów politycznych.*
33	33MM	B, U		x				wydaje się to merytorycznie uzasadnione, aby o cyberbezpieczeństwo dbały wszystkie istotne instytucje, a tak jawi mi się zaproponowany dodatkowy zbiór
34	34RA	B	X					Wynika z uzasadnienia powyżej. Właśnie dlatego, że są wybrane w drodze decyzji administracyjnej.
35	35KM	B, U			x			
36	36ŁP	I, U	x					Jw. Chodzi o ciągłą aktualizację obszarów IK równolegle z obszarami cyber… efekt synergii niezbędny.
37	37WW	B		x				Jest to konieczne ze względu na wciąż poszerzający się zasięg cyfryzacji procesów i sposobu działania podmiotów.
38	38SM	U						Ustawa o krajowym systemie cyberbezpieczeństwa – np. vide: art. 35, art. 79.
39	39ŁT	B	x					Odpowiedź analogiczna jak w pkt. 3.4. Dodatkowo, generalnie wg mnie – nie doceniamy wagi roli dostawców usług cyfrowych, których jest coraz więcej i którzy dostarczają coraz więcej rozwiązań, z których korzystamy codziennie w życiu zawodowym i prywatnym i które są bardzo istotnymi łącznikami różnych podmiotów w całej gospodarce. *Właściwie każdy podmiot na rynku (komercyjny, publiczny, NGO itd.) jest w obecnych czasach obecny w cyberprzestrzeni i narażony na cyberataki. Skuteczny atak nawet na z pozoru nieistotny podmiot może spowodować poważne braki usług, produktów, informacji i innych*

								dóbr na rynku, a w konsekwencji – doprowadzić do dezinformacji, chaosu, przerwania łańcuchów dostaw itd. Dlatego grono podmiotów powinno być max. szerokie
40	40WR	B			x			To wszystko zależy od analizy ryzyka, a co za tym idzie bilansie korzyści i kosztów.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1. *Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.*
42	42JD	B, U		x				Brakuje np. miejskich sieci IT, które faktycznie będąc słabo zabezpieczone narażają gminę wraz z podłączonymi jednostkami
43	43PS	B	x					Krytyczne dla zapewnienia cyberbezpieczeństwa jest znajomość łańcucha powiązań poszczególnych podmiotów i w tym względzie w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw.
44	44KP	B		x				
45	45SP	B		X				

3.3. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Krajowy system cyberbezpieczeństwa powinien obejmować najszerszy możliwy katalog typów podmiotów, klasyfikowanych jako: operatorzy usług kluczowych, dostawcy usług cyfrowych, instytucje centralne, administracja publiczna, jednostki sektora finansów publicznych, podmioty realizujące zadania publiczne, mających odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego.

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	**Respondent**	**Obszar**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**	**Uzasadnienie odpowiedzi:**
1	1BM	B			x			Patrząc na to jak dziś urzędu zupełnie nie przejmują się KSC to mam wątpliwości czy jest sens rozszerzać katalog podległych organizacji. Na pewno trzeba przyglądnąć się definicjom i ich sensowności
2	2UM	B		x				Docelowo tak, ale po spełnieniu warunków, o których mowa w poprzednich uzasadnieniach. Czyli raczej w wyniku procesu ewolucyjnego a nie jednorazowej rewolucji
3	3BS	B		x				Jw. W 3.1 Obecnie zakres podmiotów i ich odpowiedzialność jest głównie przyporządkowana do OUK, pozostałe wymagania są dość ograniczone. Projekt NIS 2.0 lepiej to opisuje.

4	4SK	U				x		Twierdzenie nieprecyzyjne, pod którym może kryć się wszystko. Co to znaczy możliwy najszerszy. Kluczowy coś oznacza. Więc nie każdy. A możliwy to określenie bardzo nieprecyzyjne, które może prowadzić do kolejnej fali procesów sądowych o to „dlaczego to ja jestem operatorem kluczowym, skoro prowadzę działalność w skali lokalnej?”.
5	5MK	B, U	x					tak, cyberbezpieczeństwo musi trafić pod strzechy
6	6ST	I, U		x				
7	7KG	B	x					Zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Uchwalenie dyrektywy NIS2 znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC.
8	8DP	A			x			Podobnie jak w punkcie 3.3 - jeżeli wskazane „w regulacjach dotyczących zarządzania kryzysowego, informatyzacji podmiotów realizujących zadania publiczne oraz w innych przepisach adresujących kwestie bezpieczeństwa” podmioty realizują zadania przy użyciu systemów informacyjnych, to powinny być ujęte we wskazanym katalogu.
9	9KM	B				x		Bez sensu
10	10BD	A			x			Będzie można stwierdzić po stopniu realizacji celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
11	11KP	B				x		Zbyt szeroki zakres podmiotów mających obowiązek notyfikacji do rządowych CSRIT może doprowadzić do wystąpienia szumu informacyjnego i odwrócenia uwagi od ryzyk faktycznie mogących naruszyć cyberbezpieczeństwo.
12	12PM	B	x					Jak we wcześniejszych odpowiedziach
13	13RP	I			x			nie mam zdania.
14	14CT	B		x				Cyberbezpieczeństwo to system naczyń połączonych. Oczywiście wymagałoby to zróżnicowania w zakresie obowiązków.
15	15MB	A				x		W przytoczonym stwierdzeniu nie wszystkie instytucje na pewno zależą na pewno od systemów informacyjnych.
16	16KR	B	x					
17	17MM	I		x				
18	18WM	U			x			
19	19DJ	A				x		Katalog podmiotów powinien być poszerzony, ale należałoby zapewnić wcześniej stopniowanie obowiązków (por. odpowiedź do pytania 1.3).
20	20MA	B		x				Jak w uzasadnieniu 3.2 *Z uwzględnieniem aspektu cyfryzacji tych podmiotów.*
21	21DM	B, U	x					Skutki incydentu w podmiocie mającym duży wpływ będą odczuwalne dla bezpieczeństwa publicznego, więc należy taki podmiot objąć KSC.

22	22SP	B		x				
23	23SW	I, U	x					Typowanie podmiotów poprzez ich nazwy nie zapewni właściwego poziomu bezpieczeństwa. Istotne są usługi, operatorzy usług i współzależności pomiędzy operatorami i podmiotami niezbędnymi do funkcjonowania operatorów.
24	24MA	I	x					Jw. *Aktualnie wśród pomiotów KSC brakuje m.in. przedsiębiorstw telekomunikacyjnych/komunikacji elektronicznej, podmiotów odpowiadających za rejestry państwowe, jednostki finansów publicznych i realizujących zadania publiczne, a także wystarczająco świadomych swojej roli DUC. Rozszerzenie grup podmiotów, które niesie ze sobą dyrektywa NIS2 dodatkowo zwiększy spektrum wyzwań związanych z reorganizacją KSC, ale jednocześnie podniesie potencjalną efektywność systemu, którą będzie trzeba osiągnąć.*
25	25KD	I	x					
26	26SP	B				x		
27	27KA	B	x					Jw. *Jest o oczywiste. To, że tego twórcy ustawy nie uczynili być może wynika z podejścia „nie wszystko na raz, bo się udławimy" (przepraszam za kolokwializm.*
28	28RM	U					x	
29	29GW	B		x				
30	30RT	B, U	x					Zdecydowanie tak, cyberbezpieczeństwo z natury rzeczy jest sferą mocno powiązaną z obywatelem. Im głębiej system ochrony cyberbezpieczeństwa wnika w struktury państwa tym lepiej dla obywatela. Taka filozofia powinna przyświecać ustawie.
31	31BC	A		x				
32	32KW	B				x		musi być wzięty pod uwagę rachunek ekonomiczny. Jednocześnie najlepszym rozwiązaniem byłoby stworzenie „prywatnej chmury dla podmiotów publicznych", która dostarczałaby wszystkie niezbędne narzędzia dla organów administracji, szkół, szpitali itp. w przestrzeni adresowej niedostępnej z sieci Internet. Zapewnienie odpowiedniej kadry, kompetencji i zasobów w sposób scentralizowany byłoby dużo tańsze i efektywniejsze z każdej perspektywy. W centralny sposób należałoby także udostępnić usługi dla wszystkich obywateli i interesariuszy po stronie sieci Internet.
33	33MM	B, U		x				j.w. *wydaje się to merytorycznie uzasadnione, aby o cyberbezpieczeństwo dbały wszystkie istotne instytucje, a tak jawi mi się zaproponowany dodatkowy zbiór*
34	34RA	B				x		Powinny być jasne kryteria. Wszyscy to tez nie jest dobra rzecz, bo skończy się na dodawaniu JDG, Fryzjerów itp…
35	35KM	B, U				x		Takie poszerzenie uczestników spowoduje przerost informacyjny. KSC i NIS dotyczy incydentów dużej skali mających wpływ na duże grono odbiorców.
36	36ŁP	I, U	x					Jak w p. 3.2

								Jw. Chodzi o ciągłą aktualizację obszarów IK równolegle z obszarami cyber… efekt synergii niezbędny.
37	37WW	B		x				Cyfryzacja procesów w obszarze działania państwa oraz gospodarki będzie się rozszerzać co oznacza potencjalne rozszerzanie się powierzchni ataków a to z kolei oznacza konieczne działania w kontekście konieczności ochrony cyfryzowanych zasobów.
38	38SM	U		x				
39	39ŁT	B	x					Odpowiedź analogiczna jak w 3.4 *Właściwie każdy podmiot na rynku (komercyjny, publiczny, NGO itd.) jest w obecnych czasach obecny w cyberprzestrzeni i narażony na cyberataki. Skuteczny atak nawet na z pozoru nieistotny podmiot może spowodować poważne braki usług, produktów, informacji i innych dóbr na rynku, a w konsekwencji – doprowadzić do dezinformacji, chaosu, przerwania łańcuchów dostaw itd. Dlatego grono podmiotów powinno być max. szerokie.*
40	40WR	B		x				Systemowe monitorowanie możliwie szerokiego katalogu typów podmiotów (jednak opracowanego w oparciu o analizę ryzyka, a co za tym idzie bilans korzyści i kosztów) rozwija zdolności wczesnego wykrycia i analizy anomalii w sieci, a co za tym idzie skutecznego reagowania na incydenty.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1. *Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.*
42	42JD	B, U	x					
43	43PS	B		x				j.w. – kluczowy jest łańcuch dostaw z określeniem krytyczności poszczególnych podmiotów. Jeżeli podmiot nie ma krytycznego znaczenia dla łańcucha dostaw, to nie musi być ujęty w KSC. *Krytyczne dla zapewnienia cyberbezpieczeństwa jest znajomość łańcucha powiązań poszczególnych podmiotów i w tym względzie w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw.*
44	44KP	B		x				
45	45SP	B				x		Nie ma potrzeby, aby tak rozszerzać.

3.4. W jakim stopniu zgadza się Pan(i) z poniższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Proponowany w pkt. 3.3. powyżej najszerszy możliwy katalog typów podmiotów krajowego systemu cyberbezpieczeństwa, jako mających odpowiednio duży wpływ na sferę administracyjno-społeczno-gospodarczą i bezpieczeństwa państwa, w przypadku ewentualnego ponownego ustawowego ustanawiania, powinien obejmować podmioty typu:

Proszę wstawić znak „x” w odpowiednim polu.

Lp.	Proponowane typy podmiotów krajowego systemu cyberbezpieczeństwa RP	Zdecydo-wanie TAK	Raczej TAK	Brak zda-nia	Raczej NIE	Zdecydo-wanie NIE
1	Energetyka					
2	Łączność (usługi pocztowe i kurierskie)					
3	Telekomunikacja i sieci teleinformatyczne					
4	Bankowość i infrastruktura rynków finansowych					
5	Sektor żywnościowy					
6	Wodociągi i kanalizacja					
7	Ochrona zdrowia					
8	Transport					
9	Ratownictwo					
10	Sektor chemiczny					
11	Przemysł / Produkcja					
12	Handel					
13	Usługi					
14	Administracja publiczna (rządowa i samorządowa) – wszystkie jednostki					
15	Instytucje urzędów centralnych					
16	Sektor finansów publicznych					
17	Sektor usług komunalnych					
18	Sektor usług publicznych					
19	Sektor kosmiczny					
20	Nauka i szkolnictwo wyższe					
21	Instytucje i ośrodki analityczne, doradcze, think-tanki (związane z władzą państwową i pozarządowe)					
22	Media (TV, radio, portale informacyjne)					
23	Infrastruktura cyfrowa (DNS, IXP, TLD)					

24	Usługi cyfrowe (platformy handlowe, wyszukiwarki, usługi chmury obliczeniowej**)**					
25	Usługi cyfrowe (platformy poczty elektronicznej, portale społecznościowe, itp.)					
26	Środki tożsamości elektronicznej oraz rozwiązania wykorzystujące środki tożsamości elektronicznej w realizowanych usługach					
27	Dostawa usług i systemów teleinformatycznych (TI/IT/ICT/OT/Telekomunikacja)					
28	Dostawa usług i systemów teleinformatycznych cyberbezpieczeństwa					
29	Wszystkie pozostałe typy podmiotów, nie wymienione wyżej, mające odpowiednio duży wpływ administracyjno-społeczno-gospodarczy i dotyczący bezpieczeństwa publicznego					
30	Inny (jaki?) …					
31	Inny (jaki?) …					
32	Inny (jaki?) …					

Lp.	**Respondent**	**Obszar**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**	**Uzasadnienie odpowiedzi:**
1	1BM	B		1, 3, 4, 5, 6, 7, 8, 9, 10, 15, 16, 17, 18, 22, 23, 24, 26, 27, 28		2, 11, 12, 13, 14, 19, 20, 21, 25		
2	2UM	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 16, 17, 23,	22, 26, 27	29	20, 21		Większość wymienionych typów podmiotów już obecnie znajduje się w zasięgu ustawy lub za chwilę się znajdzie w wyniku wejścia w życie (jeśli wejdzie) dyrektywy NIS II. Ponadto niektóre typy podmiotów jednoznacznie wykluczono, wskazując na inne regulacje (np. podmioty podlegające prawu telekomunikacyjnemu lub dostawców tożsamości) z niezbyt jasnych względów.

			24, 25, 28					Trzeba mieć też na uwadze, że nadmierne rozszerzanie zakresu podmiotów w tym katalogu nie jest wskazane. Obecnie nawet wielu OUK nie wypełnia wymogów ustawowych, m.in. z powodu wysokich i kosztownych wymagań nałożonych rozporządzeniem ministra cyfryzacji na wewnętrzne zespołu które powinny być powołane. Podmioty niechętnie sięgają tez po usługi zewnętrznych dostawców cyberbezpieczeństwa. W pierwszej kolejności należy zacząć egzekwować obecnie obowiązujący system prawny, w razie potrzeby z zastosowaniem kar przewidzianych w ustawie.
3	3BS	B	1, 3, 4, 5, 6, 7, 8, 9, 15, 19, 23, 24, 26	2, 5, 10, 11, 14, 16, 17, 18, 22, 25, 27, 28, 29		12, 13, 20, 21		
4	4SK	U	1, 2, 3, 4, 6, 7, 8, 10, 11, 15, 23, 25, 26, 27, 28	5, 9, 14, 22, 24	16, 17, 18, 19, 20, 21, 29	12, 13		To nie może być tak, że wszystko w państwie traktuje się jednakowo. Bo jakie obszary gospodarki zostałyby niekluczowe??? System cyberbezpieczeństwa musi zapewniać różne wymagania ochrony w zależności od istotności obiektu. Ja tych kryteriów nie odważę się podać
5	5MK	B, U	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 16, 23, 26, 27, 28					wybór 14 sektorów IK wydaje się optymalny
6	6ST	I, U		1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,				

				26, 27, 28, 29				
7	7KG	B	1, 3, 4, 8, 10, 11, 14, 15, 16, 18, 23, 24, 25, 26, 27, 28	2, 6, 7, 9, 17, 19, 20, 22, 29		5, 12, 13, 21		Zakres podmiotów uznanych zwłaszcza za OUK powinien być znacznie szerszy jak dotychczas i powinien uwzględniać łańcuch dostaw. Powinien być zweryfikowany wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. Uchwalenie dyrektywy NIS2 znacznie rozszerzy zakres podmiotowy stosowania przepisów UKSC.
8	8DP	A	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					W przypadku, gdy powyższe podmioty przetwarzają dane w systemach informacyjnych, to zdecydowanie powinny być włączone w krajowy system cyberbezpieczeństwa.
9	9KM	B	1, 2, 3, 4, 5, 7, 9, 15, 16, 18, 23, 24, 25, 26, 28, 29, 30	6, 8, 10, 11, 14, 17, 20, 27	19, 21	12, 13, 22		
10	10BD	A			1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14,			Będzie można stwierdzić po stopniu realizacji celów określonych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

					15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29			
11	11KP	B	1, 2, 3, 4, 10, 14, 15, 16, 17, 18, 19, 20, 22, 24, 25, 26, 27, 28	7, 21, 23, 29	11, 12, 13	6, 8, 9		
12	12PM	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					System zarządzania cyberbezpieczeństwem powinien działać na zasadach zbliżonych do wojska i powinien objąć przynajmniej jedną osobę (odpowiedzialną za IT lub bezpieczeństwo) w większości firm w Polsce
13	13RP	I		1, 2, 3, 4, 5, 6,				nie mam zdania, co do topologii podziału.

				7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29				
14	14CT	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 27, 28, 29	21	11, 20	12, 13		
15	15MB	A	1, 2, 3, 4, 5, 6, 7, 8, 9, 23, 24, 25, 26, 27, 28	10, 12, 14, 15, 17, 19, 22	11, 13, 16, 18, 20	21		
16	16KR	B	1, 2, 3, 4, 5, 6, 7, 8, 14, 15, 16, 19, 24, 26	9, 10, 11, 17, 18, 22, 23, 25, 27, 28	12, 13, 20, 21			
17	17MM	I	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 16, 19, 20,	11, 12, 17, 18, 21, 22, 24, 25, 27, 29	13			

			23, 26, 28					
18	18WM	U	1, 2, 3, 4, 6, 15, 23, 24, 25, 27, 28	5, 7, 8, 13, 14, 17, 26		9, 10, 11, 12, 16, 18, 29	19, 20, 21, 22	
19	19DJ	A	1, 3, 4, 6, 7, 8, 9, 10, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 27	11, 14, 20, 21	2, 5, 12, 13, 28, 29			Przed wskazaniem sektora należy dokonać starannej analizy, na ile dany sektor jest uzależniony od sprawności systemów IT/OT oraz jakie są możliwości zmiany (tzn. na ile sektor działa lokalnie). Przykładowo, logistyka jest krytycznie uzależniona od systemów IT/OT i zakłócenia mogą spowodować znaczne konsekwencje, ale większość centrali dużych firm znajduje się poza granicami Polski i próba narzucenia im zbyt daleko idących obowiązków może być trudna. Z drugiej strony, sporo systemów IT wykorzystywanych w medycynie jest krajowych i można im narzucić nowe obowiązki, nie zmniejszając jednocześnie konkurencyjności. Innym tematem jest stopniowanie obowiązków – zgłaszanie incydentów to jedno, ale np. narzucanie stosowania określonych rozwiązań (np. certyfikacja produktów, systemów i procesów). Ponadto ważne jest działanie przed incydentem – przygotowanie, ćwiczenia, szkolenia, podnoszenie świadomości, projektowanie systemów zgodnie z koncepcją security by design (uwzględnianie bezpieczeństwa przy projektowaniu nowych funkcjonalności). Wreszcie, dla większości podmiotów działających w gospodarce, bezpieczeństwo – niezależnie czy cyber czy inne – jest kwestią apetytu na ryzyko. Państwo powinno interweniować, kiedy są zagrożone dobra publiczne, takie jak stabilność gospodarki czy dane osobowe obywateli, ale nie powinno to być automatyczne.
20	20MA	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29	13, 17, 31, 32				Wraz ze wzrostem cyfryzacji obszarów życia i budowania cyfrowej tkaniny usług (serivices fabric), centralna rola państwa i tradycyjne obszary „infrastruktury krytycznej” przechodzą transformację w system zdecentralizowany, wzajemnie zależny. Najbardziej istotnym elementem infrastruktury krytycznej wydaje się być obywatel, który generalnie jest pomijany w aktualnych regulacjach. Obywatel jako użytkownik usług może podlegać atakom z użyciem inżynierii społecznościowej na masową skalę, przez szereg kanałów. Właściwy wgląd w te kanały, możliwość koordynowania incydentów, ale i negatywnych trendów może pomóc we wczesnym wykrywaniu i eliminowaniu zagrożeń dla całego społeczeństwa, ale i tradycyjnej „infrastruktury krytycznej”. Jako przykład może posłużyć tutaj sytuacja koordynacji ataków na maszty sieci 5G przez sieci społecznościowe, lub fora dyskusyjne.

21	21DM	B, U	1, 2, 3, 4, 6, 10, 14, 15, 16, 22, 23, 26	7, 8, 17, 18, 19, 20, 21, 24, 25, 28, 29	11, 12, 13			Trzeba zdefiniować odpowiednio duży wpływ poprzez katalog incydentów i wpływ, skutki na Funkcje Państwa, a nie tylko specyfikę podmiotu. Podmioty - szczególnie komercyjne, przeliczają wszystko na pieniądze i nie mają obowiązku zwracania uwagi na zaburzenie w świadczeniu usług dla społeczeństwa, a jeśli mają, to weryfikują wielkość kar, jako skutek, a nie skutek dla ogółu, dlatego odpowiedzialność personalna karna z zakazem pracy w tego typu podmiotach dla zarządzających tymi podmiotami może zmienić podejście.
22	22SP	B	1, 3, 4, 6	7, 8, 9, 10, 11, 23, 24, 26, 27	14, 19, 29	2, 5, 12, 13, 15, 16, 17, 18, 20, 21, 22, 25, 28		
23	23SW	I, U	1, 3, 4, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 18, 19, 21, 23, 24, 25, 26, 27, 28, 29	5, 20, 22	11, 12	2		W tabeli myli się sektory z dzielnością gospodarczą i usługami. W rzeczywistości jest to często jedna usługa realizowana przez powiązane ze sobą podmioty (producent +dostawca usług przesyłowych+ operator (-rzy) usługi kluczowej + ciągłość usługi kluczowej.
24	24MA	I	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					W dużym skrócie warto poszerzać katalog podmiotów, ale jednocześnie dołączać je do KSC w tempie, które uwzględni ich gotowość kompetencyjną oraz zapewni narzędzia potrzebne do współdziałania w KSC. Należy także rozważyć sposoby podnoszenia samoistnej odporności wymienionych podmiotów na potencjalne cyberzagrożenia.
25	25KD	I	1, 2, 3, 4, 5, 6, 7, 8,					

			9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					
26	26SP	B	1, 5, 6, 7, 8, 9, 26	3, 4, 10, 15, 16, 18, 20, 24, 27, 28	2, 11, 12, 14, 17, 19, 22, 25	13, 21, 23, 29		
27	27KA	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 14, 15, 16, 17, 22, 23, 24, 25, 26, 27, 28, 29	10, 11, 12, 18, 19, 20	13, 21			Państwo jest systemem naczyń połączonych. W tym przypadku systemami teleinformatycznymi. Zatem dysfunkcja jednego z nich ma oczywisty wpływ na pozostałe. Wielkość tego wpływu jest pochodną wielu czynników, jednakowoż bezwzględnie oddziaływają na siebie.
28	28RM	U						Proszę spojrzeć na definicje w NIS2. To pytanie jak rozumiem dotyczy OUK, a lista zawiera szereg podmiotów definiowanych jako dostawcy usług cyfrowych. To jest jeden z problemów obecnej UKSC – brak dostrzegania, że obszar cyber z definicji dotyczy tak zdarzeń transgranicznych, jak i skutków transgranicznych.
29	29GW	B	1, 3, 4, 5, 6, 7, 9, 15, 23, 24, 25, 26, 28	2, 8, 10, 11, 12, 13, 14, 16, 17, 18, 22, 27, 29	19, 20, 21			

30	30RT	B, U	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					cyberbezpieczeństwo to nie pożar to szerokie zagadnienie, którego punktem wyjścia jest budowa świadomości wokół zagrożeń cyberatakami. Obecność wszystkich obszarów państwa i wszystkich jednostek decydująca jest dla ukształtowania myśli obywatela o możliwościach wykorzystania cyberprzestrzeni przez wroga i kształtowania odpowiedniej świadomości i nawyków.
31	31BC	A	1, 2, 3, 4, 6, 7, 9, 10, 14, 15, 16, 17, 18, 19, 22, 23, 24, 25, 26, 27, 28,	5, 8, 11, 12, 13, 20, 21, 29				
32	32KW	B	1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	2, 12, 13, 29				należy każdorazowo analizować łańcuch dostaw dla podmiotów naturalnie wziętych pod uwagę.
33	33MM	B, U	1, 3, 4, 6, 9, 10, 14, 15, 16, 23, 26, 27, 28	2, 5, 7, 8, 11, 12, 17, 18, 19, 20, 21,	13			

				22, 24, 25, 29				
34	34RA	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	14, 15		12, 13		
35	35KM	B, U	1, 2, 3, 4, 6, 8, 9, 10, 23, 26	14, 15, 16, 18, 24, 25, 27, 28	5, 11, 17, 21, 29	12, 19, 20, 22	13	Objęcie systemem powinno być poprzedzone analizą wpływu. Te jednostki, których przerwy w dostarczaniu usług mają najmniejszy wpływ powinny być pominięte.
36	36ŁP	I, U	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29					Jedyna droga do najwyższej skuteczności działań i zapewnienia jak najwyższego poziomu bezpieczeństwa Państwa to jak najpełniejsza synergia i integracja działań przy uwzględnieniu wszelkich możliwych obszarów funkcjonowania organizacji. Nie ma mowy o przeroście czegokolwiek w tych zagadnieniach.
37	37WW	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 22, 23, 24, 25,	12, 13, 20, 21, 29				Wzmocnienie ustawowe pozwoli na możliwość umieszczenia w budżetach instytucji środków na cyberbezpieczeństwo co z kolei umożliwi realizację zadań z tego zakresu.

			26, 27, 28, 33					
38	38SM	U	*1*, 2, *3*, *4*, *6*, *7*, *8*, *11*, 14, 15, *16*, *17*, *18*, 20, *23*, *24*, 27, 28	5, 10, 19, 22				1, 4, 6, 7, 8 – opatrzone komentarzem „zał. Nr 1 do ustawy", autor przyjmuje za TAK 16, 17, 18, 23, 24 - opatrzone komentarzem „Rozporządz. w sprawie wykazu usług kluczowych (…)", autor przyjmuje za TAK 3, 11 – opatrzone komentarzem „tak, tylko kluczowe", autor przyjmuje za TAK 12, 13 – opatrzone komentarzem „brak sprecyzowania", autor przyjmuje za brak odpowiedzi
39	39ŁT	B	1, 2, 3, 4, 6, 7, 8, 9, 10, 13, 14, 15, 17, 22, 23, 24, 25, 26, 27, 28	5, 11, 12, 16, 18	29	19, 20, 21		Właściwie każdy podmiot na rynku (komercyjny, publiczny, NGO itd.) jest w obecnych czasach obecny w cyberprzestrzeni i narażony na cyberataki. Skuteczny atak nawet na z pozoru nieistotny podmiot może spowodować poważne braki usług, produktów, informacji i innych dóbr na rynku, a w konsekwencji – doprowadzić do dezinformacji, chaosu, przerwania łańcuchów dostaw itd. Dlatego grono podmiotów powinno być max. szerokie.
40	40WR	B	1, 3, 4, 6, 7, 9, 10, 15, 16, 23, 26, 27, 28	2, 11, 18, 19, 24	5, 8, 12, 13, 14, 17, 20, 25	21, 22, 29		Budowanie zdolności reagowania na incydenty komputerowe jest kosztowne, zatem objęte systemem cyberbezpieczeństwa powinny być jedynie te sektory, które generują znaczne ryzyka.
41	41ŁJ	A	1, 4, 6, 7, 8, 14, 15, 16, 17, 18, 23, 24		2, 3, 5, 9, 10, 11, 12, 13, 19, 20, 21, 25, 26, 27,			Katalog został zdefiniowany w ustawie o krajowym systemie cyberbezpieczeństwa, także na podstawie Dyrektywy 2016/1148/UE, tzw. Dyrektywa NIS i powinien obejmować co najmniej te sektory. Administracja publiczna została objęta obowiązkami na podstawie ustawy o krajowym systemie cyberbezpieczeństwa.

					28, 29			
42	42JD	B, U	1, 2, 3, 4, 6, 7, 9, 10, 14, 15, 16, 17, 22, 23, 26, 27, 28, 29	5, 8, 18, 25	11, 12, 13, 19, 20, 21, 24			
43	43PS	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 16, 19, 23, 26, 27, 28	11, 12, 13, 15, 17, 20, 21, 22, 24, 25, 29				j.w. – kluczowy jest łańcuch dostaw z określeniem krytyczności poszczególnych podmiotów. *Krytyczne dla zapewnienia cyberbezpieczeństwa jest znajomość łańcucha powiązań poszczególnych podmiotów i w tym względzie w KSC powinny być ujęte podmioty mające znaczenie krytyczne w łańcuchu dostaw.*
44	44KP	B	1, 3, 4, 6, 8, 9, 10, 15, 28	2, 5, 7, 11, 12, 13, 14, 16, 23, 24, 25, 26, 27	17, 18, 19, 20, 21, 22, 29			
45	45SP	B		1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 26, 27, 28				

4. Bezpieczeństwo teleinformatyczne usług, systemów i podmiotów systemu cyberbezpieczeństwa RP

4.1. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane i zapewniają efektywność krajowego systemu cyberbezpieczeństwa i odpowiedni poziom bezpieczeństwa państwa.

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Zdecydowana większość firm nie radzi sobie z monitorowanie środowisko OT, zarządzaniem podatnościami i analizą ryzyka
2	2UM	B				x		Uzasadnienie znajduje się w odpowiedziach na poprzednie tezy, brak egzekwowania obecnych wymagań, zbyt wysokie progi kryteriów uznania za OUK, brak odpowiedniej liczby specjalistów z dziedziny cyberbezpieczeństwa
3	3BS	B				x		Obecnie zakres wymagań jest bardzo ogólnie zdefiniowany
4	4SK	U				x		Nie do końca. Np. wywołane wcześniej CSIRTY
5	5MK	B, U				x		od zdefiniowania do wdrożenia daleka droga. Ze zdefiniowaniem też mamy problem, bo np. temat chmury obliczeniowej w sektorze usług kluczowych nie jest wystarczająco uregulowany i zdefiniowany.
6	6ST	I, U		x				
7	7KG	B		x				Moim zdaniem oparcie przepisów UKSC na uznanych standardach w zakresie bezpieczeństwa takich jak ISO27001, ISO22301 powoduje, że zastosowane rozwiązania zarządcze, organizacyjne i techniczne podmiotów krajowego systemu cyberbezpieczeństwa zapewniają efektywność krajowego systemu cyberbezpieczeństwa oraz odpowiedni poziom bezpieczeństwa państwa w stosunku do oszacowanych zagrożeń (analiza ryzyka prowadzona na poziomie podmiotu i świadczonych usług). Jedną z wad jest brak obowiązkowego ustanowienia w danym sektorze lub podsektorze właściwego CSIRT-u.
8	8DP	A		x				Należałoby wprowadzić obowiązek ustanowienia w jednostce organizacyjnej będącej częścią krajowego systemu cyberbezpieczeństwa „pełnomocnika ds. cyberbezpieczeństwa”, który posiadałby własny budżet na realizację zadań.
9	9KM	B				x		

10	10BD	A		x				W/w podmioty zostały określone zgodnie z kryteriami przyjętymi w USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
11	11KP	B				x		Obecna ustawa o KSC nie przewiduje żadnych katalogów proponowanych zabezpieczeń.
12	12PM	B					x	Obecne rozwiązania konserwują bariery poprawy poziomu cyberbezpieczeństwa: wysokie ceny dostępu do wiedzy, narzędzi, atomizacja i brak struktur współpracy
13	13RP	I			x			nie mam zdania.
14	14CT	B		x				
15	15MB	A			x			Polska nie była poddana tak zmasowanemu atakowi jak Ukraina i trudno powiedzieć, czy poziom jest odpowiedni.
16	16KR	B				x		
17	17MM	I				x		
18	18WM	U				x		Polskie przepisy implementują dyrektywę NIS, która będzie zmieniona przez dyrektywę NIS2 zmieniającą podejście do identyfikacji usług kluczowych, operatorów usług kluczowych i obiektów infrastruktury krytycznej. Obecnie przepisy w tym obszarze nie zapewniają unifikacji w obszarze zarzadzania bezpieczeństwem infrastruktury krytycznej.
19	19DJ	A		x				Bezpieczeństwo jest odpowiedzialnością każdego kierownika danego podmiotu. Mechanizmy ustawowe strukturyzują te rozwiązania, które ułatwiają realizację obowiązków.
20	20MA	B				x		Fakt aktywnej działalności instytutu NASK dla „CyberPolicy” nie oznacza faktycznego wdrożenia procedur i zaleceń tam zdefiniowanych. Wskazany wcześniej brak wprowadzenia jednolitego systemu katalogu kontrolnego oraz spójnego systemu zarządzania ryzykiem technologicznym, w tym profili ryzyk i kontroli dla sektorów wskazuje na niski poziom dojrzałości tego procesu w kraju.
21	21DM	B, U		x				
22	22SP	B				x		
23	23SW	I, U				x		Brak soc sektorowych
24	24MA	I				x		Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów KSC wymagają doskonalenia.
25	25KD	I				x		
26	26SP	B				x		
27	27KA	B				x		Posługując się przykładami kompromitacji systemów IT wielu różnych podmiotów, o których donoszą media (bo o innych nie wolno upubliczniać) bardzo łatwo jest postawić i obronić taką tezę.

28	28RM	U					x	Dość powiedzieć, że Pełnomocnik ds. Cyberbezpieczeństwa przez 3 lata nie potrafił powiedzieć, czy Kaspersky jest produktem, który powinien być stosowany w sieciach OUK, czy nie.
29	29GW	B		x				
30	30RT	B, U		x				rozwiązania zarządcze po uwzględnieniu ww. opisanych zmian i wymienione obecnie, nie budzą moich większych zastrzeżeń, choć technicznie nie są i nie aspirują być na poziomie "międzynarodowym" tj. brak jednostek z umiejętnościami kreowania wojny w cyberprzestrzeni (np. programowania malwareów), ale jak rozumiem to robi Sojusz dla Polski w Tallinie.
31	31BC	A				x		
32	32KW	B				x		wiele obszarów jest pominiętych, jak choćby odkrywanie/wyszukiwanie podatności w sprzęcie produkowanym przez polskie podmioty na polski rynek usług kluczowych (zbyt mały rynek dla podmiotów globalnych).
33	33MM	B, U		x				nie znane mi są szczególne problemy związane z tym zagadnieniem
34	34RA	B				x		Poza Cert KNF nie widzę żadnego zespołu, który coś by komunikował, wymieniał info
35	35KM	B, U		x				Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa są właściwie zdefiniowane. Problemem jednak pozostaje ich właściwe wdrożenie.
36	36ŁP	I, U		x				
37	37WW	B			x			Patrząc teoretycznie system jest sensownie zbudowany w praktyce brak odpowiedniej i nieustannej kampanii informacyjnej oraz skutecznych potencjalnych sankcji w praktyce opóźnia proces poprawy stanu bezpieczeństwa oraz stwarza wrażenie realizowania go w najprostszy często nieprofesjonalny sposób.
38	38SM	U		x				
39	39ŁT	B					x	Na razie wszystko wygląda fajnie w teorii (a tutaj nawet są dziury i niepełne pokrycie przepisami wszystkich podmiotów, które powinny być objęte) – ale w praktyce wygląda to wciąż słabo (podejście decydentów, brak budżetów, opóźnienia w stosunku do ilości i wagi cyberzagrożeń).
40	40WR	B		x				Z pozycji miejsc, które znam/pracowałem nie spotkałem się z negatywnymi informacjami na ten temat.
41	41ŁJ	A			x			Odpowiedź jak w pytaniu 2.1. *Nie realizuję zadań w urzędzie obsługującym Pełnomocnika Rządu ds. Cyberbezpieczeństwa, którego kompetencje obejmują wymieniony zakres krajowego systemu cyberbezpieczeństwa. Na tym poziomie może być sformułowana taka ocena. Pełnomocnik przedstawia raporty z realizowanych zadań. Organem opiniodawczym jest Kolegium ds. Cyberbezpieczeństwa.*

42	42JD	B, U				x		Na tym etapie ustawa moim zdaniem wprowadza pewne zadania nie do końca możemy powiedzieć o zbudowaniu „systemu", np. wskazywane podmioty są przez ministrów właściwych, ale na jakim standardzie?
43	43PS	B				x		Rozwiązania te dopiero teraz są budowane i ich obecna efektywność nie jest adekwatna. Przyjęte kierunki należy ocenić pozytywnie, ale wymagany jest jeszcze znaczny rozwój tych działań.
44	44KP	B				x		Działam głównie ostatnio w systemach radiowych dla rynku kolejowego. Zapóźnienie kolejowe co do systemów bezpieczeństwa ruchu kolejowego oceniam na bardzo duże.
45	45SP	B		x				

4.2. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny być zdefiniowane jednolicie dla wszystkich podmiotów i być oparte o te same normy, wytyczne lub standardy dla zapewnienia wspólnego, uznanego wzorca odniesienia i wzajemnego zaufania oraz podobnego i porównywalnego poziomu odporności i bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa.

Proszę wstawić znak „**x**" w odpowiednim polu.

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B				x		Zupełnie inne rozwiązania techniczne powinny być w małej gminie czy urzędzie a inne w elektrowni
2	2UM	B				x		Różnorodność branż i ich wpływu na życie społeczeństwa powoduje ze tak silna korelacja nie jest ani potrzebna, ani możliwa. Ponadto w wielu branżach obowiązują różne normy sektorowe, jedynym wspólnym mianownikiem jest rodzina norm ISO/IEC 27000, ewentualnie ISO/IEC dotyczące ciągłości działania i tak powinno pozostać. Pozostałe rodziny norm powinny podlegać świadomemu wyborowi przez podmioty danego sektora. Praktyka wskazuje ze nadmiar formalnych regulacji i wymagań powoduje ze nie są one faktycznie przestrzegane.
3	3BS	B		x				Co do zasady tak, ale warto wskazać różnice w różnych sektorach i organizacjach, co innego podmiot z OT/ICS/SCADA, co innego administracja publiczna, co innego operator telekomunikacyjny, a co innego DC.

4	4SK	U	x					Dlaczego powinny? Przecież zapisy ustawy i rozporządzenia w sprawie wymaganej dokumentacji do tego prowadzą… sama nazwa dyrektywy NIS do tego się sprowadza Nie wiem co oznacza określenie dla wszystkich podmiotów? Trzeba doprecyzować.
5	5MK	B, U			x			są normy sektorowe, np. dla wodociągów czy armii, których nie da się zastosować gdzie indziej.
6	6ST	I, U		x				
7	7KG	B		x				Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych i podmiotów krajowego systemu cyberbezpieczeństwa powinny jednolite, aczkolwiek w UKSC powinien znaleźć się przepis, że jeśli dla danego sektora lub podsektora obowiązują rozwiązania i standardy branżowe związane z cyberbezpieczeństwem to również mogą być stosowane. Normy takie jak ISO27001, ISO220301 czy ISO27032 są uniwersalne i jeśli przepisy UKSC będą się do nich odwoływać nie będzie problemów z ich stosowaniu w różnych podmiotach i sektorach.
8	8DP	A		x				Należałoby wprowadzić ustawowy obowiązek wdrożenia przez podmioty krajowego systemu cyberbezpieczeństwa norm np. ISO 27001.
9	9KM	B	x					CC
10	10BD	A			x			Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie podmioty w w/w zakresie.
11	11KP	B	x					Standardy chociażby prowadzenia dokumentacji czy organizacja poszczególnych obszarów systemu cyberbezpieczeństwa (jak monitoring, response, detection itp.) powinny być zdefiniowane i wymagane.
12	12PM	B	x					Takie rozwiązania zminimalizują ceny i poprawią dostępność wiedzy i narzędzi
13	13RP	I			x			rozwiązania techniczne bezpieczeństwa powinny być adekwatne i dostosowane do skali, zakresu i wpływu i szeroko rozumianego kontekstu zależnego od danego sektora.
14	14CT	B		x				
15	15MB	A		x				Będzie wtedy jasność oceny odporności, jak będzie jeden punkt odniesienia.
16	16KR	B	x					
17	17MM	I		x				
18	18WM	U	x					Standaryzacja zdecydowanie tak, ale z zachowaniem adekwatnych wymogów dla operatorów o różnej wielkości np. jeden standard dla dużych operatorów i drugi dla małych (chodzi o postawienie racjonalnych wymagań możliwych do spełnienia).

19	19DJ	A				x		Rozwiązania krajowe powinny być jednolite, co do wyniku, nie, co do środka. Środowiska IT/OT, kultury organizacyjne, zależności (wewnętrzne i zewnętrzne) są różne dla różnych podmiotów. Normy, które pasują dla szkoły podstawowej i dla fabryki mikrochipów, nie są dobre.
20	20MA	B		x				Jednolity powinien być katalog i metodologie zarządzania ryzykiem. Jednak powinien być on otwarty na kontrole i ryzyka specyficzne dla danego sektora lub charakterystyki operacyjnych podmiotów działających w systemie. Rozwiązania techniczne nie powinny być ujednolicane z uwagi na słabości technologiczne, jednak wskazane jest ustalenie minimalnego wymaganego poziomu funkcjonalności wraz z ośrodkiem certyfikacji/testów niezależnie potwierdzających (od producenta) spełnienie wymogów.
21	21DM	B, U				x		Poziom odporności i techniczne środki bezpieczeństwa powinny być oparte a podejście bazujące na ryzyku. Zadania są zdefiniowane i na każdym szczeblu istnieje komórka odpowiedzialna za ich wykonanie jednak nie są one koordynowane co unaocznia się na szczeblu gminnym, gdzie spływają do realizacji wszelkie obowiązku.
22	22SP	B	x					
23	23SW	I, U				x		Poszczególne sektory znacznie różnią się co do wymogów prawnych i stosowanych rozwiązań organizacyjnych.
24	24MA	I		x				Należy zwiększać dostępność wiedzy i kształcenia oraz podnoszenie kompetencji kadr, które odpowiadają w podmiotach KSC na różnych poziomach odpowiedzialności za rozwiązania zarządcze, organizacyjne i techniczne. Jednocześnie należy zachować konieczną elastyczność zastosowań dla wskazywanych norm, wytycznych i standardów w poszczególnych podmiotach.
25	25KD	I	x					
26	26SP	B				x		
27	27KA	B		x				Jednolita miara jest pożądana, ale specyfika też musi być brana pod uwagę, bo może zaburzyć ocenę.
28	28RM	U	x					Temu m.in. mają służyć programy certyfikacji wprowadzane w oparciu o rozporządzenie o cyberbezpieczeństwie.
29	29GW	B		x				
30	30RT	B, U		x				Ogólnie ok, tylko myślę o kadrach. Wydaje się, że w związku z brakiem specjalistów w zakresie cyberbezpieczeństwa, należy w miarę ujednolicać kompetencje i rozwiązania, by umożliwiać przepływ pomiędzy sektorami specjalistów oraz łatwiejszą ich adaptację w pracy.
31	31BC	A			x			

32	32KW	B	x					z zastrzeżeniem, że wybrany security baseline jest osiągalny dla wszystkich podmiotów i określi się wymagane poziomy dojrzałości (wdrożenia elementów dodatkowych ponad standard) w uzależnieniu od wagi/typu danej organizacji.
33	33MM	B, U				x		raczej nie, ponieważ dla wielu sektorów powinny istnieć szczególne wymagania, co zresztą w praktyce występuje. Te sektory mają inne profile ryzyka
34	34RA	B	x					Przykładem może być na przykład określenie „odpowiednio duży" jak wcześniej – bez wspólnej definicji każdy będzie rozumiał to inaczej. Dla niektórych Problem to incydent, dla innych problem to przyczyna incydentu
35	35KM	B, U				x		Rozwiązania wysokopoziomowe mogą być zdefiniowane w sposób jednolity dla wszystkich. Natomiast różnice pomiędzy branżami/obszarami na niskim poziomie (np. kolej, lotnictwo, przemysł chemiczny, administracja) są tak duże, że definiowanie jednolite spowoduje, że będą bezużyteczne.
36	36ŁP	I, U	x					Jak w 3.4 *Jedyna droga do najwyższej skuteczności działań i zapewnienia jak najwyższego poziomu bezpieczeństwa Państwa to jak najpełniejsza synergia i integracja działań przy uwzględnieniu wszelkich możliwych obszarów funkcjonowania organizacji. Nie ma mowy o przeroście czegokolwiek w tych zagadnieniach.*
37	37WW	B		x				Spójne wzorce przy uwzględnieniu specyfiki podmiotów są konieczne do zorganizowanego i jednolitego sposobu zarządzania w kontekście zagrożeń cyberbezpieczeństwa.
38	38SM	U	x					
39	39ŁT	B	x					Jednolitość norm / wytycznych spowoduje szybsze dostosowanie się podmiotów oraz bardziej powszechną świadomość ich istnienia.
40	40WR	B		x				Budowanie systemów cyberbezpieczeństwa w oparciu o normy i standardy jest uzasadnione. Mityguje to ryzyko braku kompatybilności, ułatwia projektowanie/dewelopment również dla mniej doświadczonych podmiotów. Problemem może być jednak zachowanie standardów mniej zamożnym organizacjom.
41	41ŁJ	A			x			W świetle przepisów ustawowych i rozporządzenia nt. dokumentacji związanej z cyberbezpieczeństwem podstawowe normy, w oparciu o które budowane jest cyberbezpieczeństwo w podmiotach zobowiązanych to ISO 27001, ISO 22301. Dodatkowo w świetle przepisów dotyczących audytu w sektorach przemysłowych stosowny audyt może być prowadzony na podstawie normy ISA 62443. Należy zatem zweryfikować tą tezę.
42	42JD	B, U	x					
43	43PS	B		x				Obecne podejście do ujednolicania podejścia w oparciu o analizę ryzyka jest najlepszym podejściem.
44	44KP	B		x				

45	45SP	B				x		Różne podmioty pełnią różną rolę, więc nie można zastosować tych samych wytycznych, norm itp.

4.3. W jaki stopniu zgadza się Pan(i) z powyższym stwierdzeniem, biorąc pod uwagę efektywność systemu cyberbezpieczeństwa na poziomie krajowym i bezpieczeństwo państwa?

Rozwiązania zarządcze, organizacyjne i techniczne bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, jako jednolite dla wszystkich podmiotów (jak w pkt. 4.2) w przypadku ewentualnego ponownego ustawowego ustanawiania, powinno być ustanowione w sposób, gdyby miały być na nowo ustawowo ustanowione, to powinny być oparte o:

Proszę wstawić znak „**x**” w odpowiednim polu.

Lp.	**Standardy bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa RP**	**Zdecydowanie TAK**	**Raczej TAK**	**Brak zdania**	**Raczej NIE**	**Zdecydowanie NIE**
1	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301)					
2	Normy ISO wskazane w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)					
3	Normy ISO (wskazane w regulacjach ustawy KSC (ISO 27001, ISO 22301) oraz w regulacjach ustawy o informatyzacji podmiotów realizujących zadania publiczne (ISO 20000 (-1, -2), ISO 27001, ISO 27002 (17799), ISO 27005, ISO 24762)					
4	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.)					
5	Normy ISO – szeroki katalog norm dotyczących aspektów bezpieczeństwa informacji i systemów teleinformatycznych (ISO 27001, ISO 27002, ISO 27005, ISO 24762/ ISO 27031, ISO 27032, ISO 27033, ISO 27034, ISO 27035, ISO 27040, itp.) oraz norm zarządzania usługami informatycznymi (ISO 20000 (-1, -2)) i ciągłości działania ISO 22301					

6	Standardy NIST dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania					
7	Polskie Narodowe Standardy Cyberbezpieczeństwa (NSC) (opracowane na podstawie standardów NIST)					
8	Standardy ITIL, RESILIA					
9	Dowolne standardy dotyczące cyberbezpieczeństwa, bezpieczeństwa informacji i systemów teleinformatycznych i ciągłości działania					
10	Inne (jakie?) …					

Lp.	Respondent	Obszar	Zdecydowanie TAK	Raczej TAK	Brak zdania	Raczej NIE	Zdecydowanie NIE	Uzasadnienie odpowiedzi:
1	1BM	B	1, 2, 3, 6, 7	4	5	8, 9		
2	2UM	B	1, 2, 3			4, 5, 6, 7, 8, 9		Jedynym wspólnym mianownikiem w obszarze bezpieczeństwa są normy rodziny 27 000, można również uznać za wspólnie wymagana normę dotyczącą ciągłości działania ISO/IEC 22301. Pozostałe normy (NIST) czy dobre praktyki (ITIL) powinny być stosowane z dobrowolnego wyboru danego podmiotu. Uzasadnienie podano w jednym z powyższych punktów
3	3BS	B	1, 6, 7	4		2, 3, 5	8, 9	
4	4SK	U	5					Chyba najbardziej kompleksowe i uniwersalne. Standardy narodowe np. NIST mogą być kwestionowane przez pewne państwa a to powinno być spójne. Dodałbym ISO 31000 do generalnego zarządzania ryzykiem w tych podmiotach, jako uzupełnienie 27005
5	5MK	B, U	1, 2, 3, 4, 5	6, 7	8	9		tłumaczenie standardów NIST (np. w SCCO) jest kłopotliwe, ponieważ znajdują się tam pojęcia spoza polskiego systemu prawnego. Ich przenoszenie jest czasochłonne.
6	6ST	I, U	1, 2, 3, 4, 5, 6, 7, 8, 9					
7	7KG	B	1, 2, 3, 4, 5, 6, 7, 8, 9, 10					W/w standardy są uniwersalne i jeśli przepisy UKSC będą się do nich odwoływać nie będzie problemów z ich stosowaniu w różnych podmiotach i sektorach. Powinno się uwzględniać także normy i standardy branżowe obowiązujące w danym sektorze lub podsektorze.

8	8DP	A	1, 2, 3, 4, 5, 6, 7, 8	9				Rozwiązania oparte na wyżej wymienionych normach w stopniu bardzo dobrym zapewniałyby bezpieczeństwo organizacyjne i techniczne systemów teleinformatycznych.
9	9KM	B	1, 6, 7	2, 3, 4, 5		8		KRI – nowelizacja ASAP
10	10BD	A			1, 2, 3, 4, 5, 6, 7, 8, 9			Organizacja zarządzania cyberbezpieczeństwem RP powinna być ustanowiona/ zdefiniowana zgodnie z kompetencjami oraz możliwościami realizacji zadań przez odpowiednie podmioty w w/w zakresie.
11	11KP	B	6	1, 2, 3, 4, 5, 7	8		9	
12	12PM	B	5					W/w normy są sprawdzonym sposobem zarządzania w skali podmiotu (firmy)
13	13RP	I	1, 9, 10		4, 5, 6, 7, 8		2, 3	standardy powinny być adekwatne do danej branży. Ich dobór powinien też zależeć od danej organizacji a ich ilość od poziomu dojrzałości. Sporo standardów da się na siebie nawzajem zmapować – są do siebie podobne. Ważne jest ciągłe doskonalenie organizacji, badać poziom jej dojrzałości, aby z czasem sięgać po więcej. Wydaje się mieć sens pozostawienie wyboru organizacjom standardów ze względu na ich branżowe wytyczne jak np.: ISO 62859 Elektrownie jądrowe -- Systemy opomiarowania i sterowania -- Wymagania dla koordynacji bezpieczeństwa i cyberbezpieczeństwa, czy ISO 19014 - Maszyny do robót ziemnych -- Bezpieczeństwo funkcjonalne -- Część 4: Projektowanie i ocena oprogramowania oraz transmisji danych dla elementów systemu sterowania związanych z bezpieczeństwem.
14	14CT	B	1, 2, 3, 4, 5, 6, 7, 8		9			Najlepiej korzystać z rozwiązań sprawdzonych, testowanych i skalowalnych.
15	15MB	A	1, 2, 3	6, 7	4, 5, 8	9		Zbyt duża ilość standardów zakłóca ocenę
16	16KR	B	1, 4, 5	7		6, 8	9	
17	17MM	I	3, 6	7		9		
18	18WM	U			1, 2, 3, 4, 5, 6, 7, 8, 9			Bez badań ciężko wskazać zestaw norm a tym bardziej nie jest możliwe wskazanie jednej.
19	19DJ	A		1, 2, 3, 4, 5, 6, 7	8, 9			Normy ISO są potężnym narzędziem, ale wymagają dodatkowej pracy – nie są gotowymi rozwiązaniami do wdrożenia. Różne normy ISO się uzupełniają, co jest dobre, ale zwiększa koszty (trzeba kupić i wdrożyć kilka norm). Ponadto, część systemów proponowanych przez normy ma dobre, zgodne z ISO, alternatywy. Nie trzeba np. używać ISO/IEC 27035, aby zbudować skuteczny i bezpieczny system reagowania na incydenty bezpieczeństwa informacji.

								Dodatkowym problemem jest to, że cała rodzina ISO 27000 jest oparta na ryzyku, czyli nie nadaje się do przymusowego wdrożenia (obowiązkiem ustawowym). ITIL i RESILIA nie są standardami, tylko bibliotekami dobrych praktyk, zbudowanych zresztą na fundamentach ISO 20000. Należy zaznaczyć, że nie ma zasady one size fits all. Różne rozwiązania działają dla różnych rodzajów podmiotów. Część międzynarodowych podmiotów (np. banki) mają obowiązek stosowania własnych metodyk i standardów; należy pamiętać, że system obowiązków nie może być zbyt sztywny.
20	20MA	B	6, 7	1, 2, 3, 4, 5		9		Koordynacja w zakresie cyberbezpieczeństwa wymaga standaryzacji języka i metod oceny ryzyka na poziomie transgranicznym a nie krajowym z uwagi na charakter zagrożeń cyber. Normy ISO w tym zakresie nie są wystarczająco precyzyjne, aby spełnić warunki komunikacji wspierające szybką koordynację reakcji na zagrożenia transgraniczne.
21	21DM	B, U		1, 4, 7	6, 8, 9	2, 3, 5		ISO20000 bazuje na itil, jednak itil to katalog dobrych praktyk bez obowiązku wdrażania całości – mniejszy podmiot łatwiej spełni ITILa, niż iso20000. Seria 270xx może być obowiązkowa, jednak należy dostosować wymagania do podmiotu i niekoniecznie należy wymagać jednocześnie 27035 i 27001. 17799 jest przestarzałą i bazuje na BS. NIST jest amerykański i tworzony na potrzeby US Gov, obok niego funkcjonują dokumenty CISA, FBI, US-CERT. Wymagalność komercyjnych norm może być kontrowersyjna. Tworzenie własnych standardów ma sens tylko, gdy jednocześnie wydana zostanie mapa zgodności z już istniejącymi pn. jeśli masz iso27001, to spełniasz całość lub większość, ponieważ istnieje już ich tak dużo i na pewno regulują wystarczająco kwestii np. niewymieniony COBIT, IEC62443 uznawany w przemyśle, wydania SANS i CIS.
22	22SP	B	1, 2, 3	4, 5, 6, 7		8	9	
23	23SW	I, U	10					Uwzględniające specyfikę sektorów.
24	24MA	I	1, 2, 3, 4, 5, 6, 7, 8, 9, 11					Podmioty KSC należy nie tylko zobowiązywać, ale przede wszystkim zachęcać do wdrażania rozwiązań, które wynikają z przytoczonych standardów, rekomendacji i dobrych praktyk, najlepiej dopasowanych do ich specyfiki działania.
25	25KD	I	5	4		1, 2, 3, 6, 7, 8, 9		Normy ISO są najpowszechniejszym standardem dla określenia szeroko rozumianego bezpieczeństwa informacji oraz są już wskazane w wielu regulacjach prawnych krajowych. Ujednolicenie standardu znacznie upraszcza kwestie związane z zarządzaniem oraz utrzymaniem systemu bezpieczeństwa oraz rozliczaniem realizacji zadań.

26	26SP	B		1	7	2, 3, 8	4, 5, 6, 9	
27	27KA	B	7					Generalnie można powiedzieć – lepszy dowolny standard niż żaden. Zatem jakikolwiek przyjmiemy i tak dokonamy kroku dziejowego. A ukonkretniając – NSC jest pewną, nazwijmy to zdroworozsądkową kompilacją ISO i NIST. Zatem skoro jest – stosujmy, ale jednolicie i powszechnie!
28	28RM	U						Normy międzynarodowe (ISO) – tak, natomiast wymienił Pan wyłącznie standardy związane z zarządzaniem, bez norm technicznych. A to jest jeden z głównych problemów dla bezpieczeństwa infrastruktury – brak takich norm lub ich problematyczny problem certyfikacji (jak w Common Criteria).
29	29GW	B	1, 2, 3, 4, 5, 6, 7, 8	9				
30	30RT	B, U	5, 6, 8					obowiązują nas normy i prawo międzynarodowe, nie jesteśmy państwem autarchicznym, należymy do organizacji międzynarodowych, których normy są dla Polski obowiązujące. Wybrałam tr. plus korporacyjne
31	31BC	A			1, 2, 3, 4, 5, 6, 7, 8, 9			
32	32KW	B	6, 7					standardy NIST mają bardzo pragmatyczne podejście do operacyjnej strony cyberbezpieczeństwa i oczywiście bez kłopotu można ich wymagania zmapować z wymaganiami ISO. Zostały także referencją dla NSC.
33	33MM	B, U		1, 2, 3, 4, 5, 6, 7, 12	8, 9			zaznaczyłem przydatność prawie wszystkich, co nie oznacza, że to kompletny katalog i mogę sobie wyobrazić inne zestawy dla różnych sektorów, dlatego też podtrzymuję odpowiedź na pyt. 4.2 *raczej nie, ponieważ dla wielu sektorów powinny istnieć szczególne wymagania, co z resztą w praktyce występuje. Te sektory mają inne profile ryzyka*
34	34RA	B	1, 2, 6, 7, 8, 9	3, 4, 5				Powinien być ustalony 1 max 2 standardy dla każdej z dziedzin inaczej nie będzie można tego ani dobrze zdefiniować ani skontrolować *ale 27005 jest już uchylona, mamy 31000
35	35KM	B, U	5	6, 7				Podejście normatywne jest słuszne i zapewnia prawidłowe pokrycie wszystkich obszarów bezpieczeństwa informacji. Standardy krajowe, jeżeli będą stosowane, będą najlepszym źródłem dobrych praktyk, ponieważ są dopasowane do naszej specyfiki.
36	36ŁP	I, U			1, 2, 3, 4, 5, 6, 7, 8, 9			
37	37WW	B	1, 5, 6, 7	2, 3, 8			9	Kluczowym elementem jest wybranie spójnych standardów i odejście od całkowitej dowolności interpretacji, ponieważ prowadzi to do skrajnych przypadków

								interpretowania punktów odniesienia do tylko tych, które są wygodne i łatwe do dostosowania.
38	38SM	U						Wskazane normy, standardy, wytyczne i dobre praktyki powinny zostać określone w Rozporządzeniu ministra właściwego ds. informatyzacji wraz z procedurami związanymi z: akredytacją, certyfikacją i deklaracją zgodności ICT (produktów, usług, procesów).
39	39ŁT	B		1, 2, 3, 4, 5, 6		7, 8	9	Mix wymagań z ISO i NIST będzie dobrym punktem wyjścia.
40	40WR	B						Nie mam wiedzy w tym zakresie.
41	41ŁJ	A						Odpowiedź jak w pytaniu 4.2. *W świetle przepisów ustawowych i rozporządzenia nt. dokumentacji związanej z cyberbezpieczeństwem podstawowe normy, w oparciu o które budowane jest cyberbezpieczeństwo w podmiotach zobowiązanych to ISO 27001, ISO 22301. Dodatkowo w świetle przepisów dotyczących audytu w sektorach przemysłowych stosowny audyt może być prowadzony na podstawie normy ISA 62443. Należy zatem zweryfikować tą tezę.*
42	42JD	B, U	6	1, 2, 3, 7	4, 5, 9	8		Normy powinny wspierać, definiować, ale jako odwołanie w ustawie.
43	43PS	B	1, 2, 3, 6, 7	4, 5, 8				Normy są ważne, niemniej to jednolitość podejścia do analizy ryzyka jest kluczowa dla efektywności działania KSC.
44	44KP	B			1, 2, 3, 4, 5, 6, 7, 8, 9			
45	45SP	B						Jak wyżej – nie można ustalić jednolitego rozwiązania dla wszystkich *Różne podmioty pełnią różną rolę, więc nie można zastosować tych samych wytycznych, norm itp.*

SUPLEMENT

1. Suplement nr 1. Załącznik nr 1. Arkusz kwestionariusza wywiadu eksperckiego,
2. Suplement nr 2. Załącznik nr 2. Zestawienia zbiorcze odpowiedzi respondentów w podziale na poszczególne problemy badawcze,
3. Suplement nr 3. Zbiór arkuszy kwestionariusza wywiadu eksperckiego z odpowiedziami respondentów.