WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

ROZPRAWA DOKTORSKA

„Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej”

mgr Dawid DUDA

Promotor: **dr hab. Monika SZYŁKOWSKA, prof. WAT**

Promotor pomocniczy: **dr Sylwia SZYBOWSKA**

Warszawa 2024

Spis treści

Wprowadzenie

„Cyber świat otacza mnie
Przed oczyma mi mknie
Analogowe niegdyś dźwięki
Zamienione na cyfrowe piosenki
Wywoływane kiedyś zdjęcia z kliszy
Drukowane są obecnie po przyciśnięciu myszki klawiszy.
[…]
O gdzież jesteście płonące uczucia
Zamienione zostały w sklasyfikowane odczucia
I tak umieramy po kawałku
Bo żyć się nie da w betonowym folwarku
Bo żadne kliknięcie myszy
Nie sprawi, że mnie miłość nas usłyszy
A świat pozbawiony miłości
W cyber otchłani sprawia, że się co najwyżej złościsz”[1].
Smigol, *Cyberświat*

Działania człowieka w coraz większym stopniu przenoszą się ze środowiska fizycznego do środowiska cyberprzestrzeni. Nie trudno zauważyć jak w przeciągu ostatnich lat technologie informacyjno-komunikacyjne (*ICT*) zmieniły praktycznie każdy aspekt ludzkiego życia, znacząco ułatwiając dzielenie się informacjami oraz usługami, a także dostępem do nich. Oprócz pozytywnego aspektu tego zjawiska, pojawia się również większa podatność na zagrożenia, a w związku z tym cyberbezpieczeństwo staje się jednym z najpoważniejszych wyzwań, jakiemu sprostać powinno nowoczesne państwo.

Powyższy wiersz pt. „Cyberświat” porusza dwie strony cyberświata. Pierwsza, która polega na możliwościach jakie oferuje współczesna technologia (w podanym przykładzie jest to intuicyjne i proste drukowanie zdjęć); a także negatywna, przejawiająca się w społecznej wartości cyberświata, gdzie ludzie zapominają o sobie nawzajem w rzeczywistości, opierając swoje życie i relacje jedynie na sferze cyber.

[1] Smigol, *Cyberświat,* https://www.twojewiersze.pl/pl/wiersz,aTFWNjMyQDNrN0I5KDk8MGQzcTE [dostęp 02.01.2022 r.].

W literaturze przedmiotu i regulacjach prawnych znaleźć można wiele odniesień dotyczących znaczenia i kształtowania systemu bezpieczeństwa narodowego (państwa), jednakże w obszarze cyberbezpieczeństwa państwa występuje swego rodzaju niedobór w tym zakresie. Istnieje zatem potrzeba usystematyzowania i poszerzenia wiedzy, a także zaprezentowania wniosków opracowanych dzięki zastosowaniu różnych (względem analizowanych problemów i weryfikowanych hipotez) metod badawczych.

Temat pracy pt. „Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej" jest bezsprzecznie kluczowy oraz jak najbardziej aktualny, ponieważ dotyczy sfery bezpieczeństwa państwa. Wyniki badań mogą spowodować wypełnienie luki naukowej jaką jest m.in. poszerzona analiza społecznej części systemu cyberbezpieczeństwa państwa. Ważną więc kwestią jest zbadanie tego obszaru, aby nie tylko dokonać oceny ww. systemu, ale również wskazać możliwe kierunki i obszary jego udoskonalenia. W zależności od wyników badań, te rekomendacje mogą być różne, ponieważ zróżnicowany okazać się może wynik analizowanych problemów badawczych, a w związku z tym weryfikowanych hipotez badawczych. Fundamentalne jest zidentyfikowanie i analiza zdefiniowanego obszaru badań, z zastosowaniem metodologii typowej dla prowadzenia naukowych badań społecznych, tak aby stanowiło to podstawę dalszego rozwoju tego komponentu systemu cyberbezpieczeństwa państwa.

Rozprawa w syntetyczny sposób ukazuje problematykę poziomu kompetencji cyfrowych użytkowników Internetu w Polsce, tj. nauczycieli oraz uczniów szkół podstawowych. W celu kompleksowego przedstawienia tematyki należy skoncentrować sie na podejściu interdyscyplinarnym do tego problemu poprzez polskie regulacje prawne, dokumenty związane z działalnością szkół podstawowych czy też wytyczne i przepisy obowiązujące w Unii Europejskiej.

Analiza ta pozwala dostrzec zmiany i różnice w postrzeganiu cyberbezpieczeństwa przez wyżej wymienione grupy, co prowadzi do wniosku o potrzebie znalezienia wspólnych, wielowymiarowych rozwiązań mogących przyczynić sie do polepszenia danego stanu wiedzy. Wiążąc się to powinno z głęboką analizą dotychczasowego sposobu zdobywania i doskonalenia umiejętności cyfrowych.

W dysertacji ukazano podstawowe wyzwania związane z niespójnością definicyjną cyberprzestrzeni w wybranych państwach. Uwypuklono potrzebę rozwoju systemu oświatowego do realizacji całościowej edukacji cyfrowej wraz z uwzględnieniem tzw. konsumentów końcowych, tj. nauczycieli, opiekunów, wychowawców czy rodzi-

ców, gdyż są to środowiska, które pierwszorzędnie powinny kształtować właściwe zachowania w sieci młodych podopiecznych i dzieci.

Skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa - stanowi podstawowe założenie rozprawy. Ustalenie poziomu kompetencji cyfrowych użytkowników i wskazanie braków pozwoli na omówienie kluczowych obszarów do doskonalenia.

Celem głównym badań w obszarze podjętego problemu było zbadanie istniejących rozwiązań państwa polskiego w zakresie działań realizowanych na rzecz budowania oraz podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP. Szerzej cel badań opisano w podrozdziale 1.3. Cel badań. Tak, aby ukazać różnorodność zjawiska opracowano porównanie w ramach trzech województw, co pozwoliło wskazać różnice i podobieństwa w opisywanym wymiarze.

W pracy podczas procesu badawczego wykorzystano kilka metod badawczych tj. statystyczną i sondażu diagnostycznego, analizy i krytyki piśmiennictwa, analizy i konstrukcji logicznej. Zastosowano natomiast następujące techniki badawcze: wywiad, ankietowanie, badanie dokumentów oraz jako narzędzie kwestionariusz ankiety i wywiadu.

Strukturę pracy tworzy sześć rozdziałów. Pierwsza część stanowi opis metodologiczny dysertacji. Wyszczególniono metody badań, narzędzia i techniki procesu badawczego, dokonano charakterystyki i opisano wskazaną próbę badawczą.

Druga, obejmuje zakres pojęciowy i definicyjny kluczowych zagadnień- m.in. istotę cyberbezpieczeństwa, pojęcia, zakres oraz jego strukturę. Szczególną uwagę zwrócono na zakres opisania cyberprzestrzeni w kontekście globalnym. Na tej podstawie, wskazano różnice w postrzeganiu kwestii cyberbezpieczeństwa i rozumienia definicji w wybranych państwach biorąc pod uwagę dostępną literaturę przedmiotu tak polską, jak i zagraniczną.

W kolejnym rozdziale dokonano szczegółowej analizy: struktury systemu cyberbezpieczeństwa RP, dedykowanych dokumentów strategicznych i regulacji prawnych w obszarze cyberbezpieczeństwa. Przedstawiono także istotne z punktu widzenia budowania świadomości i kompetencji cyfrowych właściwe podmioty oraz instytucje. Wskazano rolę aktualnej polityki Unii Europejskiej w podejściu do zapobiegania cyber-

zagrożeniom. Zawarto najnowsze uregulowania prawne, stąd praca podlegała bieżącym zmianom i aktualizacjom.

W dalszej części opracowana została identyfikacja, klasyfikacja i charakterystyka zagrożeń cyberprzestrzeni, tj. ataki, kradzieże, blokowanie dostępu, spam czy ataki socjotechniczne i wynikające z nich wyzwania cyberprzestrzeni. Rozkłady statystyczne przedstawiono zarówno w ujęciu tabelarycznym jak i opisowym. Wyszczególniono cyberzagrożenia mające znaczenie w kontekście funkcjonowania państwa.

Piąty rozdział dotyczy społecznej świadomości cyberzagrożeń i poziomu kompetencji cyfrowych użytkowników. Zawarto autorską definicję kompetencji cyfrowych. Przeprowadzono analizę wiedzy i poziomu umiejętności poruszania się w cyberprzestrzeni na tle wybranych państw ze szczególnym uwzględnieniem uczniów szkół podstawowych państw Grupy Wyszechradzkiej.

Niezwykle istotny z uwagi na tzw. wartość dodaną, jest rozdział szósty, w którym zaprezentowano analizę wywiadów eksperckich oraz wyniki badań sondażowych. Pogłębione wywiady indywidualne przeprowadzono z Zastępcą Dyrektora Departamentu Kształcenia Ogólnego i Podstaw Programowych w Ministerstwie Edukacji Narodowej, Wiceprezesem Oddziału Polskiego Towarzystwa Informatycznego, prokuratorem i biegłym sądowym w śladach cyfrowych i pracownikiem Naukowej i Akademickiej Sieci Komputerowej. Ponadto, zawarto informacje z rozmowy dostępnej na platformie *YouTube* z Dyrektorem Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. W ramach badania ankietowego otrzymano odpowiedzi ponad 1500 nauczycieli oraz ponad 2500 uczniów z trzech województw, co pozwoliło na opracowanie porównania poziomu kompetencji cyfrowych. Wszystkie przytoczone dane dotyczą wybranej próby badawczej na terytorium trzech województw Rzeczypospolitej Polskiej z uwzględnieniem wieku respondentów jako kryterium.

Ostatni element dysertacji stanowi koncepcja rekomendacji / propozycji zmian w zakresie włączenia zadań w obszarze budowania i podnoszenia świadomości społecznej cyberbezpieczeństwa jako elementu struktury krajowego systemu cyberbezpieczeństwa RP. Autor ma świadomość faktu, iż przeprowadzone badania stanowią początek i skromny wkład w analizę wielorako uwarunkowanej przestrzeni cyfrowej w kontekście zdolności i umiejętności użytkowników.

1. Metodologiczne podstawy dysertacji

1.1. Przyczyny podjęcia badań

Zainteresowania badawcze doktoranta oraz przekonanie, iż kwestie przeciwdziałania zagrożeniom w cyberprzestrzeni w systemie cyberbezpieczeństwa państwa powinny być rozpatrywane wielopoziomowo, zdecydowały o podjęciu tej tematyki.

Obecny charakter zagrożeń sprawia, że poszczególne podsystemy bezpieczeństwa państwa muszą współdziałać w celu osiągnięcia efektu synergii. Intensywny rozwój technologii informacyjno-komunikacyjnych (dalej również *ICT*) kształtuje współczesne funkcjonowanie społeczeństwa i wpływa na jego bezpieczeństwo. Działanie indywidualnego obywatela, czy grup osób pełniących różne role w społeczeństwie w ramach korzystania z różnego rodzaju cyfrowych usług, może mieć konkretne przełożenie na postrzeganie całego systemu cyberbezpieczeństwa. Z drugiej strony, jakikolwiek element systemu cyberbezpieczeństwa państwa może również oddziaływać bezpośrednio lub pośrednio na użytkownika, jednak skutki tego oddziaływania trudno obecnie jednoznacznie przewidzieć i ocenić.

Tematyka pracy „Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej" i aktualność zagadnień w niej podejmowanych są niezwykle istotne z punktu widzenia bezpieczeństwa państwa. Poszerzanie wiedzy, jak i świadomości w tym obszarze powinno odbyć się z korzyścią dla całego społeczeństwa.

Biorąc pod uwagę powyższe czynniki – powstała potrzeba wskazania przedmiotu oraz celu badań. Wynika to z ciągu przyczynowo-skutkowego, ponieważ przy planowaniu działań, należy określić jaki będzie obiekt zainteresowań badawczych i cel działań, tak aby spełnione zostały warunki, które badanie zakładało.

1.2. Przedmiot badań

Zdaniem M. Cieślarczyka przedmiotem badań są *„fakty, procesy i zjawiska"*[2]. J. Sztumski z kolei, określa przedmiot badań jako *„wszystko, co się składa na rzeczywistość społeczną, tak więc zbiory społeczne i zbiorowości, instytucje społeczne, zjawiska*

[2] M. Cieślarczyk, 2003, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich,* Wydawnictwo Akademii Obrony Narodowej, Warszawa, s. 27.

i procesy społeczne”[3]. Z kolei wg W. Puśleckiego to *„ściśle zdefiniowana część – wycinek rzeczywistości społeczno – przyrodniczej, która stanowi obiekt zainteresowań poznawczych określonej dyscypliny naukowej”*[4]. T. Pilch z kolei przedmiot badań określa jako *„zadanie stojące przed nami w chwili uświadomienia sobie konieczności przeprowadzenia badań empirycznych”.*

Przedmiotem badań niniejszej dysertacji były działania realizowane na rzecz budowania i podnoszenia kompetencji cyfrowych użytkowników w ramach systemu cyberbezpieczeństwa RP.

Przedmiot przyjętych badań rozprawy jest dość rozległy, ponieważ obejmuje:

- zagadnienia dotyczące bezpieczeństwa państwa;
- kwestie obejmujące system cyberbezpieczeństwa RP, mechanizmy współpracy pomiędzy poszczególnymi organami (krajowymi, sektorowymi);
- zagadnienia związane z zagrożeniami oraz wyzwaniami cyberprzestrzeni i ich wpływem na funkcjonowanie państwa;
- problematykę kompetencji cyfrowych użytkowników, a co jest z tym związane – ich świadomości w cyberprzestrzeni;

Zakres podmiotowy stanowili natomiast: użytkownicy Internetu, pracownicy bądź przedstawiciele instytucji związanych z problematyką cyberbezpieczeństwa oraz uczniowie klas szkół podstawowych jak i nauczyciele tych szkół.

Wyróżnia się ponadto następujące zakresy rozprawy:

- zakres przestrzenny: obejmujący środowisko cyberbezpieczeństwa RP oraz wybranych innych państw w zakresie kompetencji cyfrowych;
- zakres czasowy: przypadający na lata 2021-2024.

1.3. Cel badań

Podjęte badania miały na celu:

- analizę istniejących rozwiązań w zakresie działań państwa polskiego realizowanych na rzecz budowania oraz podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP, m.in. w ustawie o krajowym systemie cyberbezpieczeństwa, Doktrynie Cyberbezpieczeństwa RP oraz Strategii Cyberbezpieczeństwa RP;

[3] J. Sztumski, 1995, *Wstęp do metodologii i technik badań społecznych,* Wydawnictwo Śląsk, Katowice, s. 7.
[4] W. Puślecki, 1995, *Metody badań pedagogicznych,* Wydawnictwo ODN, Kalisz, s. 3.

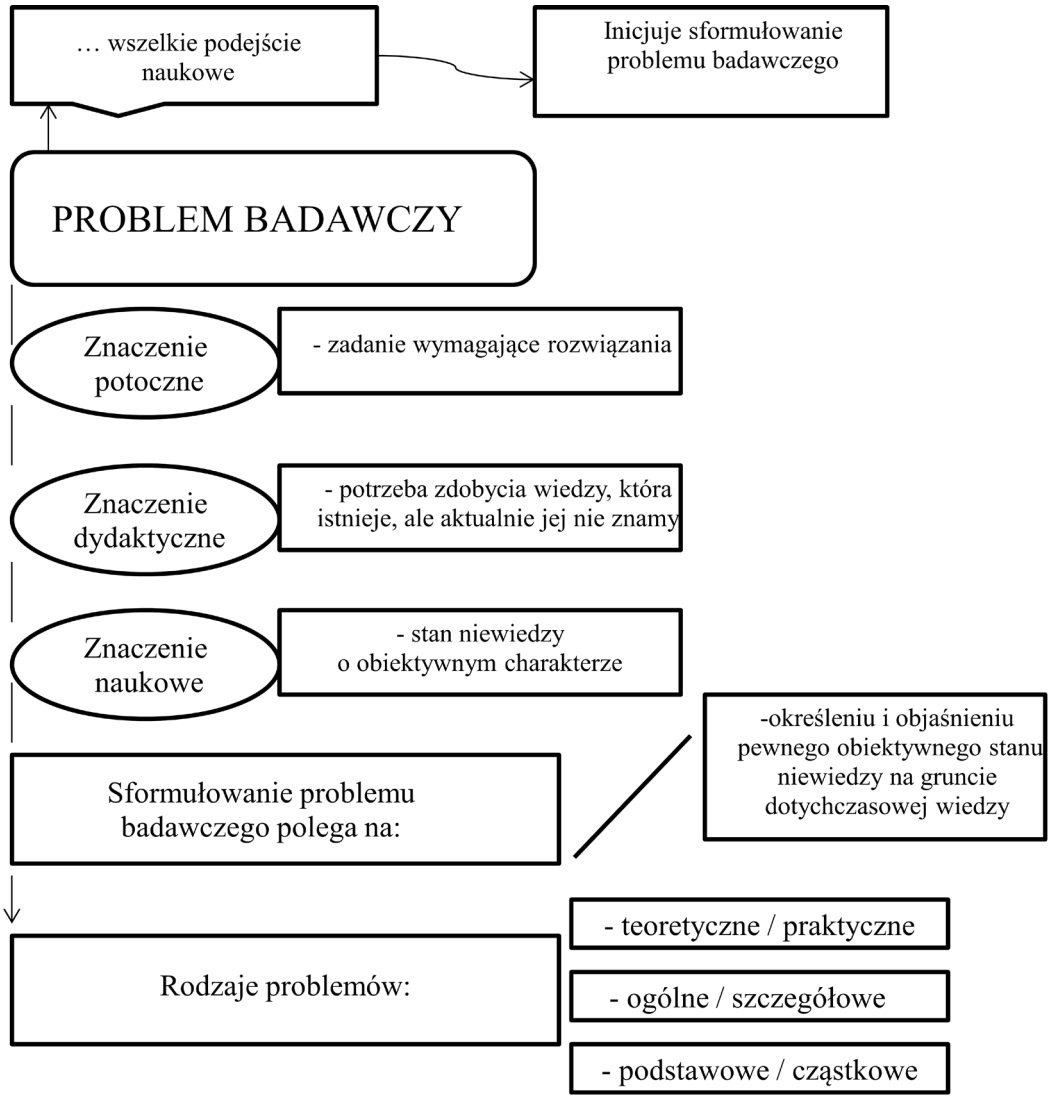
- określenie miejsca Krajowego Systemu Cyberbezpieczeństwa w całym systemie cyberbezpieczeństwa RP, w ramach którego wyodrębnia się trzy podsystemy: kierowania, ogniwa operacyjne, publiczne i prywatne ogniwa wsparcia;
- ocenę działania Krajowego Systemu Cyberbezpieczeństwa i określenie kierunków jego rozwoju;
- wskazanie podmiotów i instytucji kluczowych w obszarze budowania świadomości i kompetencji cyfrowych użytkowników;
- oszacowanie poziomu wiedzy i umiejętności użytkowników sieci;
- określenie cyberzagrożeń szczególnie istotnych z punktu widzenia funkcjonowania państwa;
- wzbogacenie wiedzy w zakresie poziomu świadomości cyberzagrożeń i kompetencji cyfrowych wskazanej grupy badawczej w przypadku badania sondażowego przeprowadzonego za pomocą anonimowej ankiety;
- w obszarze wywiadów eksperckich: ocenę kierunków kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa, uzyskanie opinii na temat realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji, ocenę sposobów edukacji i metod użytkowników sieci.

Zdefiniowany zakres dysertacji przewiduje: diagnozę aktualnego stanu wiedzy użytkowników w obszarze cyberbezpieczeństwa, identyfikację zagrożeń i wyzwań systemu cyberbezpieczeństwa – docelowo – w przypadku pozytywnie zweryfikowanej hipotezy – także opracowanie rekomendacji w zakresie budowania świadomości i kompetencji cyfrowych wpisujących się w wytyczne określone m.in. w Strategii Cyberbezpieczeństwa RP, mogące mieć znaczący wpływ na kształtowanie systemu cyberbezpieczeństwa RP.

1.4. Problemy naukowe

Pierwszym etapem zadań naukowych jest określenie problemu badań, właściwie określone problemy badawcze są gwarancją rzetelności i sensem jakichkolwiek badań naukowych.

Pojęcie problemu pochodzi z j. greckiego *„problema”* - przeszkoda, trudność. Można to rozumieć jako zadanie, zagadnienie wymagające rozwiązania, wyjaśnienia czy jako po prostu sprawę sporną. Istotę i znaczenie problemu badawczego przedstawia poniższy rysunek.



Rys. 1.1. Istota problemu badawczego (źródło: opracowanie własne na podstawie: J. Apanowicz, 2002, *Metodologia ogólna*, Wydawnictwo Diecezji IV Bernardinum, Gdynia, s. 43)

Zdaniem autora, pojęcie problemu właściwie określa M. Łobocki *„jest to pytanie, na które odpowiedzi szukamy na drodze badań naukowych, czyli poprzez wysiłek i dociekanie”*[5]. Problemem badawczym nazywa się bodziec intelektualny wywołujący reakcję w postaci badań naukowych. Aby był on empirycznie uzasadniony, musi zostać jasno i dokładnie sformułowany[6].

Uwzględniając powyższe, w związku z określonym celem badań oraz wstępną analizą literatury przedmiotu, wskazano główny problem badawczy w niniejszej dyser-

[5] M. Łobocki, 2007, *Wprowadzenie do metodologii badań pedagogicznych*, Wydawnictwo Oficyna Wydawnicza Impuls, Kraków, s. 110.
[6] Ch.Franfort-Nachmias, D.Nachmias, 2001, *Metody badawcze w naukach społecznych*, Wydawnictwo Zysk i S-ka, Poznań, s. 67-68.

tacji, stanowiący odpowiedź na pytanie: Jakie czynniki i działania mają wpływ na budowanie świadomości oraz kompetencji cyfrowych w zakresie cyberbezpieczeństwa?

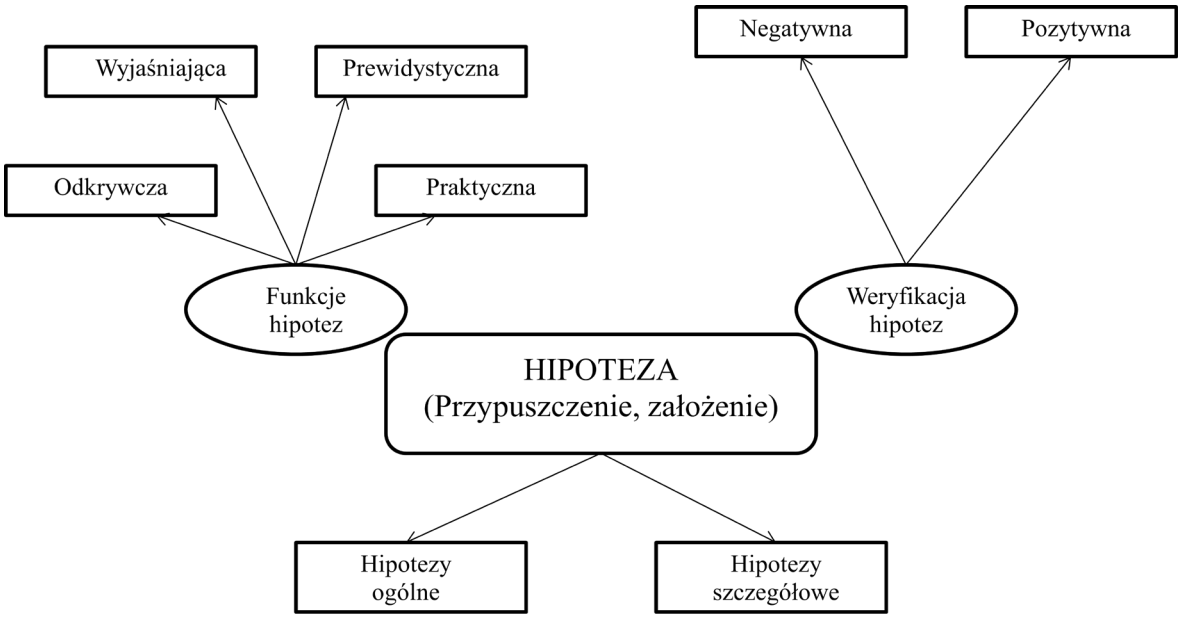
Rozwiązanie wyżej zdefiniowanego głównego problemu badawczego, możliwe jest poprzez znalezienie odpowiedzi na pytania w zakresie problemów szczegółowych:

- Które przepisy prawne regulują kwestie cyberbezpieczeństwa w RP?
- Które ze wskazanych w przepisach podmiotów i instytucji mają określone zadania w obszarze budowania świadomości i kompetencji cyfrowych użytkowników?
- Jaki jest istniejący zakres wiedzy użytkowników oraz sposób jej pozyskiwania w zakresie cyberbezpieczeństwa?
- Jakie standardy obowiązują w zakresie kompetencji cyfrowych?
- Jaki jest poziom kompetencji obywateli w zakresie cyberbezpieczeństwa?
- Jaki jest poziom świadomości w obszarze cyfrowych zagrożeń wśród użytkowników sieci?
- Jakie istnieją metody i obszary edukacji użytkowników?
- Które z zagrożeń w dziedzinie cyberbezpieczeństwa mogą oznaczać największe wyzwanie dla funkcjonowania państwa?
- Czy kompetencje cyfrowe mogą mieć wpływ na poziom cyberbezpieczeństwa?

1.5. Hipoteza robocza

Hipoteza z greckiego *„hipothesis”* oznacza przypuszczenie lub podkład. Hipoteza jest prawdopodobieństwem istnienia (obecności) bądź nie, danej rzeczy, zdarzenia lub też zjawiska (procesu) określonego czasem i miejscem. Stanowi prawdopodobieństwo związku określonych zjawisk z innymi lub zależności pomiędzy nimi. Opierając się na udowodnionych twierdzeniach i metodach wypróbowanych można przyjąć, że przy pomocy danych sposobów uzyskiwane jest oczekiwane rozwiązanie[7]. Istotę i funkcje hipotez przedstawia rysunek nr 1.2.

[7] J. Apanowicz, 2002, *Metodologia ogólna*, Wydawnictwo Diecezji IV Bernardinum, Gdynia, s. 48.



Rys. 1.2. Istota i funkcje hipotez (źródło: opracowanie własne na podstawie: J. Apanowicz, 2002, *Metodologia ogólna*, Wydawnictwo Diecezji IV Bernardinum, Gdynia, s. 48)

„Naukowa hipoteza jest przypuszczeniem wynikającym z dotychczasowego stanu naszych badań, opartych na nauce i dotyczącym stanu naszej wiedzy” [W. Pytkowski][8]. K. Ajdukiewicz twierdzi, że hipotezą jest nieprzyjęta jeszcze racja, którą rozważa się w trakcie prób wyjaśnienia danego faktu[9]. J. Pieter natomiast, określa hipotezę jako przypuszczenie co do istnienia lub nieobecności danej rzeczy bądź zjawiska w określonym miejscu i czasie[10]. Podsumowując dotychczasowe rozważania, można stwierdzić, że hipotezą jest proponowana odpowiedź, weryfikowana po przeprowadzeniu badań.

W celu uporządkowania rozważań, osiągnięcia wskazanego celu badawczego oraz wyjaśnienia problemu badawczego, przyjęto następującą hipotezę roboczą:

- Skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa.

Wynikiem tak postawionej hipotezy roboczej i problemów szczegółowych są hipotezy szczegółowe:

- Użytkownicy bez odpowiednich kompetencji w zakresie cyberbezpieczeństwa mogą stanowić jedno ze słabszych ognisk systemu cyberbezpieczeństwa.
- Edukacja może przekładać się bezpośrednio na poziom świadomości użytkowników w cyberprzestrzeni i ich kompetencje cyfrowe.

[8] W. Pytkowski, 1981, *Organizacja badań i ocena prac naukowych*, Wydawnictwo PWN, Warszawa, s. 153.
[9] K. Adjukiewicz, 1975, *Logika pragmatyczna,* Wydawnictwo PWN, Warszawa, s. 42.
[10] J. Pieter, 1975, *Zarys metodologii pracy naukowej*, Wydawnictwo PWN, Warszawa, s. 25.

- Poziom świadomości obywateli korzystających z sieci - w zakresie cyberbezpieczeństwa jest niewystarczający.
- Stałe rozwijanie kompetencji cyfrowych może pozwolić na minimalizację ryzyka wystąpienia określonych zagrożeń w cyberprzestrzeni.

1.6. Metody badawcze

J. Sztumski wskazuje, iż metoda badawcza to *„system założeń i reguł pozwalających na uporządkowanie teoretycznej lub praktycznej działalności, aby możliwe było osiągnięcie założonego celu”*[11]. W. Zaczyński określa metodę badań jako *„systematycznie stosowany sposób, to znaczy w określonym przypadku z zamiarem zastosowania go również przy ewentualnym powtórzeniu się podobnego zadania”*[12].

Ponadto, T. Pilch wyszczególnia następujące założenia i warunki poprawnej metody badawczej, która powinna:

- zmierzać najkrótszą drogą do zrealizowania podjętego zadania badawczego;
- określać sposób postępowania badawczego odpowiadający ogólnej koncepcji badań;
- sugerować właściwy wybór technik badawczych;
- precyzować terytorialne i czasowe ramy pracy w postaci hipotez i ułatwić opracowanie badań w ich postaci;
- być odpowiednia do problemu, który jest do rozwiązania[13].

Organizacja badań powinna zostać poprzedzona skrupulatnym przygotowaniem procedury badawczej, ponieważ jak zaznacza W. Zaczyński *„organizacja i metody badań wyznaczane są przez problemy i powiązane z nimi hipotezy. Tak więc musi odpowiadać tej metodzie, która z kolei powinna być właściwa do rozwiązywanych problemów”*[14]. W przypadku dysertacji proces badawczy jest cyklem badań składający się z czterech etapów.

Pierwszy z etapów to projektowanie problemu badawczego. Problem badawczy wyznacza treść, kierunek i zakres badań. Podczas jego określania błędy popełnione będą wpływać na dalsze badania. Formułując problem badawczy należy wziąć pod uwagę szereg czynników np. wykonalność rozwiązania problemu, jego złożoność, związek z własnymi zainteresowaniami, czas, jaki trzeba poświęcić na realizację badań i waż-

[11] J. Sztumski, 2005, *Wstęp do metod i technik badań społecznych,* Wydawnictwo Śląsk, Katowice, s. 46.
[12] W. Zaczyński, 1990, *Praca badawcza nauczyciela,* Wydawnictwo WSiP, Warszawa, s. 18.
[13] T. Pilch, 1995, *Zasady badań pedagogicznych,* Wydawnictwo Akademickie ŻAK, Warszawa, s. 66.
[14] W. Zaczyński, *Praca badawcza…,* op. cit., s. 153.

ność jak i znaczenie rozwiązania problemu. Niezwykle istotny czynnik, o ile nie najważniejszy to cel rozwiązania problemu.

Kolejny etap stanowi rozwiązanie problemu badawczego. W tym miejscu wskazać należy dwie części tego etapu. Pierwsza to koncepcja. Drugą natomiast stanowi realizacja badań, do której zaliczyć należy: przeprowadzenie badań wstępnych i zasadniczych, uporządkowanie wyników badań, ich analiza oraz opracowanie materiałów badawczych[15].

Następnie występuje uogólnianie i wnioskowanie. Uogólnianie jest teoretycznym lub praktycznym połączeniem części, cech, właściwości i stosunków badanych zjawisk lub faktów, które to poddane analizie w całościowym ujęciu umożliwiają stawiać całkiem nowe wnioski. Wnioskowanie jest podstawowym procesem myślowym, przyjmującym w swoim rozumowaniu jako podstawę – prawdziwość podanego zdania i na tej podstawie dochodzenie do przeświadczenia o prawdziwości innego albo innych (kolejnych) zdań. Wnioskowanie stanowi rozumowanie, które polega na wyprowadzaniu nowych wniosków czy twierdzeń. Wnioskować znaczy domniemywać bądź wnosić ze znanych sytuacji czy faktów, nowe – inne zdania stanowiące rozstrzygnięcie[16]. Wynika z tego, iż wnioskowanie jest procesem mającym na celu wskazanie najbardziej znaczących wyników badań, przedstawionych przy pomocy określonych danych.

Ostatni etap to weryfikacja i wejście w kolejny cykl badań. Wszechstronne i dokładne wniknięcie w rozpatrywane dane umożliwia na wykrycie połączeń i logicznych związków a także zależności między procesami (zjawiskami). Poprzez analizę ustala się dowody, formułuje pojęcia i twierdzenia a także odpowiada na pytania jak i czy w ogóle zakładany cel badań został osiągnięty. Same fakty – bez interpretowania, nie są wiarygodnym wyjaśnieniem. Z tego też względu schemat wyjaśnienia powinien zawierać: obserwacje, spostrzeżenia, doświadczenia, ogólne twierdzenia, teorie, wysnucie i przełożenie prognoz na zrozumiały język[17]. Wejście w kolejny cykl badań oznacza rozpoczęcie wszystkich procedur badawczych od początku, ponieważ cykl badawczy jest procesem, czyli szeregiem czynności powtarzających się w określonych odstępach czasu i z określoną kolejnością.

Przyjęta hipoteza robocza i określony wyżej problem badawczy, wraz z wynikającymi z niego problemami szczegółowymi – narzuciły potrzebę zastosowania w proce-

[15] J. Apanowicz, *Metodologia…,* op. cit., s. 98.
[16] Ibidem, s. 27.
[17] J. Apanowicz, 2000, *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania,* Wydawnictwo Diecezji Pelplińskiej Bernardinum, Gdynia, s. 165-168.

sie badań odpowiednich metod, technik oraz narzędzi badawczych. W założonej procedurze badawczej ujęto je w czterech etapach, spośród których wyróżniono okresy badań: wstępnych oraz właściwych. W ramach badań wstępnych dokonano analizy literatury przedmiotu, wykonano czynności pozwalające na analizę problemu, wskazanie i opisanie hipotez oraz metod i technik badawczych. Dzięki tym badaniom przeprowadzonej analizy literatury przedmiotu dopracowano niektóre elementy podstaw metodologicznych dysertacji jak np. hipotezy czy cel badań. Badania właściwe, inaczej zasadnicze, miały na celu zgrupowanie wiarygodnych danych i informacji zgodnie z przyjętą koncepcją rozwiązania problemu badawczego. Badania właściwe zatem obejmowały przeprowadzenie wywiadów eksperckich oraz kwestionariuszy – ankiet wśród grup badawczych.

Na podstawie dokonanej analizy i selekcji metod badawczych, wyszczególniono poniższe:

1. Metody:

- statystyczna i sondażu diagnostycznego – polegające na wyciąganiu wniosków z wyodrębnionych cech zbiorów elementów statystycznych w ujęciu tak jakościowym, jak i ilościowym, ponadto, gromadzenie faktów i informacji o strukturalnych i funkcjonalnych zjawiskach i dynamice ich rozwoju;
- analizy i krytyki piśmiennictwa – mające charakter pomocniczy, bowiem dzięki nim możliwe jest wykazanie luk w obecnym stanie wiedzy bądź kierunku dyskusji naukowej;
- analizy i konstrukcji logicznej – scalające treści badanego problemu i pozwalające wysunąć nowe, optymalne rozwiązania, pozwala to formułować twierdzenia ogólne na podstawie uznanych twierdzeń cząstkowych.

2. Techniki:

- wywiad – pozyskiwanie danych poprzez bezpośrednią rozmowę;
- ankietowanie – pisemne udzielanie odpowiedzi na pytania tworzące logiczny i spójny zestaw, służący do rozwiązania wskazanej tezy lub problemu badawczego;
- badanie dokumentów – analiza ilościowa i jakościowa dokumentów i zawartej w nich treści, w zależności od potrzeb będą to sprawozdania, zakresy obowiązków, opinie (wyniki badań, raporty cyberbezpieczeństwa, cyberzagrożeń).

3. Narzędzia:

- kwestionariusz ankiety / wywiadu – narzędzie przeznaczone do rejestrowania odpowiedzi respondentów, kwestionariusz zawierający logiczną kompozycję pytań musi tworzyć zwartą i konsekwentną całość, dotyczącą jedynie jednego zjawiska.

4. Zmienne:

- zmienna niezależna – działania realizowane na rzecz budowania i podnoszenia poziomu kompetencji cyfrowych użytkowników w ramach systemu cyberbezpieczeństwa RP;
- zmienna zależna – poziom wiedzy użytkowników w obszarze cyberbezpieczeństwa i jej wpływ na system cyberbezpieczeństwa RP.

Stąd, właśnie skuteczność tych działań będzie miała wpływ na poziom wiedzy użytkowników.

W dysertacjach czy innych pracach naukowych uogólnienia tworzy się przy użyciu tzw. indukcji niezupełnej. Badania wówczas przeprowadza się na niepełnej liczbie danych (tj. zdarzeń, przedmiotów, elementów etc.) pewnego określonego globalnego zbioru. Niepełny zbiór powinien stanowić próbę reprezentatywną, która charakteryzuje się określoną liczebnością i właściwościami statystycznymi badanej zbiorowości. Zmienną zatem stanowi dowolna cecha, czynnik, właściwość etc. przybierająca charakterystyczne i reprezentatywne wartości w danym zbiorze. Wyróżnia się trzy podstawowe rodzaje zmiennych: zależne, niezależne oraz pośredniczące. Zmienne zależne stanowią skutek w prowadzonym badaniu naukowym. Te zmienne w danym procesie czy zdarzeniu ulegają zmianom. Zmiennymi niezależnymi natomiast określa się te zmienne, które zależą od zmiennych zależnych. Zmienne niezależne są więc tymi zmiennymi, które mają działanie, oddziaływanie na zmienne zależne. Stanowią przyczynek do określonego skutku, tak więc do zmian w zmiennych zależnych[18].

Dzięki obranej metodologii, możliwe było określenie poziomu kompetencji cyfrowych uczniów szkół podstawowych i ich nauczycieli. Wynik badania określił m.in. najczęściej wykorzystywane przez użytkowników aplikacje, poziom wiedzy dotyczący prewencji w Internecie oraz zakres wiedzy w obszarze najczęstszych zagrożeń. Niezwykle ważnym okazało się ocenienie czy szkoła posiada procedury na sytuacje związane np. z cyberbullingiem.

Wywiady z osobami zatrudnionymi (z sektora cyberbezpieczeństwa)

[18] J. Apanowicz, *Metodologia…,* op. cit., s. 53.

określonymi w ustawie o krajowym systemie cyberbezpieczeństwa z 2018 roku[19] dotyczyły funkcjonowania instytucji, roli, zadań, organizacji szkoleń dla pracowników w kontekście zwiększania świadomości w zakresie cyberzagrożeń. Interesujące jest także zdiagnozowanie sposobu funkcjonowania określonych instytucji, metod wzmacniania wiedzy dotyczącej świadomości cyberzagrożeń.

Poza diagnozą stanu wiedzy, krytyką literatury, analizą formalno-prawną autor zamierzał zbadać relacje w zakresie stanu wiedzy i umiejętności cyfrowych i sposobów ich doskonalenia oraz wpływ użytkowników na cały system cyberbezpieczeństwa. Okazało się, iż w wyniku przeprowadzonych badań autor znalazł ramową koncepcję uzupełnienia zidentyfikowanych luk systemowych.

1.7. Ograniczenia badawcze

Ograniczenia badawcze związane były przede wszystkim z obszarem wywiadów eksperckich. Kilka prywatnych podmiotów zajmujących się cyberbezpieczeństwem odmówiło realizacji badania powołując się na brak czasu, bądź zaznaczając, że dana tematyka nie mieści się w obszarze ich zainteresowań. Pojawiły się również głosy ze strony instytucji państwowych – przekierowujące do innych podmiotów celem realizacji rozmów.

Warto podkreślić jednak również fakt, iż swego rodzaju niechęć szkół do udziału w badaniu spowodowana była koniecznością poświęcenia czasu na realizację badania. Ponadto, dyrektorzy szkół na bazie swoich doświadczeń argumentowali decyzje faktem udziału w różnego rodzaju badaniach w ubiegłych latach, a następnie braku informacji zwrotnej o wynikach. Zdarzyło się, iż nie został podany żaden argument w kwestii odmowy udziału w badaniu.

Aktualność wskazanego obszaru jak i zmieniający się stale krajobraz cyberbezpieczeństwa (związany z implementacją nowych regulacji i realizacją strategii) stanowił konieczność określenia ram czasowych dysertacji- do kwietnia 2024 r.

1.8. Analiza stanu wiedzy – przegląd literatury przedmiotu / kwerenda literatury

Obszar tematyczny rozprawy nie jest dogłębnie zbadany i nie był szeroko podejmowany, należy ponadto mieć świadomość, że po powstaniu niniejszej dysertacji

[19] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560 z późn. zm.).

nadal wiele kwestii pozostanie do zbadania. Wiąże się to z faktem, iż podjęta tematyka jest dynamiczna zarówno w czasie, jak i jej rozwoju. Wyzwanie to staje się coraz bardziej złożone i wymaga cyklicznej analizy, co jednocześnie stanowi o jego istotnym znaczeniu.

Celem bardziej wnikliwej eksploracji badanego zjawiska, autor w swojej pracy odwołuje się do opracowań w zakresie literatury przedmiotu, aktów prawnych zarówno narodowych i międzynarodowych, dokumentów i koncepcji strategicznych oraz raportów instytutów badawczych i innych organizacji. Uzupełnienie poglądów w obszarze przede wszystkim cyberprzestrzeni i zdolności cyfrowych stanowią materiały pokonferencyjne, jak również publikacje internetowe wraz z analizami i danymi statystycznymi.

W literaturze przedmiotu znaleźć można publikacje np. C. Banasińskiego[20], który opisuje prawne podstawy cyberbezpieczeństwa czy też specyfikę zagrożeń w cyberprzestrzeni. Wartą uwagi pozycją z punktu widzenia autora jest „*Cyberbezpieczeństwo dzieci i młodzieży – realny i wirtualny problem polityki bezpieczeństwa",* pod red. M. Górki[21]. Twórcy poruszają problemy facebook'owego dzieciństwa, cyberprzemocy, jak również postępu technologicznego będącego źródłem zagrożeń. Kwestie życia w świecie najnowszych technologii przybliża *„Uczeń bezpieczny w cyberprzestrzeni"* pod red. D. Szeligiewicz-Urban[22]. Bardzo interesujące i przydatne opracowanie w zakresie definicyjnym stanowi praca M. Szyłkowskiej *„Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje"*[23]. Źródło wiedzy dla niniejszej dysertacji i rozważań stanowi także zbiór rozdziałów w pracy pod red. T. Dębowskiego *„Cyberbezpieczeństwo wyzwaniem XXI wieku"*[24] oraz S. Gwoździewicz i K. Tomaszyckiego *„Legal and Social Aspects of Cybersecurity"*[25]. Są to kluczowe publikacje w opisywanym obszarze tematycznym.

Jedną z najbardziej kluczowych regulacji prawnych omawianej tematyki jest

[20] C. Banasiński (red. nauk.), 2018,*Cyberbezpieczeństwo. Zarys wykładu,* Wydawnictwo Wolters Kluwer Polska, Warszawa.
[21] M. Górka (red. nauk.), 2017, *Cyberbezpieczeństwo dzieci i młodzieży – realny i wirtualny problem polityki bezpieczeństwa"*, Wyd. Difin, Warszawa.
[22] D. Szeligiewicz-Urban (red. nauk.), 2012, *Uczeń bezpieczny w cyberprzestrzeni*, Wydawnictwo Humanitas, Sosnowiec.
[23] M. Szyłkowska, 2019, *Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje*, Wydawnictwo Sine Qua Non, Kraków.
[24] T. Dębowski (red. nauk.), 2018, *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Wydawnictwo Archae-Graph, Wrocław.
[25] S. Gwoździewicz, K. Tomaszycki (red. nauk.), 2020, *Legal and Social Aspects of Cyberecurity*, Wydawnictwo Difin, Warszawa.

Konstytucja RP z 1997 r.[26], która w art. 5 wskazuje na bezpieczeństwo obywateli. Cyberbezpieczeństwo jest obszarem, składową całego bezpieczeństwa państwa i narodu.

Wynik implementacji pierwszego europejskiego prawa w zakresie cyberbezpieczeństwa, tzw. Dyrektywy NIS (z 2016 r.)[27] stanowi w Polsce ustawa o krajowym systemie cyberbezpieczeństwa (z 2018 r.)[28], która określa ogółem system oraz wchodzące w jego skład podmioty wraz z ich zadaniami oraz obowiązkami.

Kwestie cyberbezpieczeństwa ujęto również w innych regulacjach prawnych. Nowelizacja ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[29], określa, iż w sytuacji zewnętrznego zagrożenia państwa spowodowanego m.in. działaniami w cyberprzestrzeni, Prezydent RP może (na wniosek Rady Ministrów), wprowadzić stan wojenny – w całym państwie bądź na jego części. Tak więc niezgodne z prawem działania w cyberprzestrzeni, mogą nieść za sobą skutki bardziej poważne, aniżeli „tylko" te wynikające z zapisów Kodeksu Karnego[30] (stanowiące o przestępstwach przeciwko ochronie informacji).

Według Doktryny Cyberbezpieczeństwa z 2015 r.[31], która była dokumentem koncepcyjnym tj. mogącym stanowić jedynie punkt wyjścia do dalszych prac na rzecz wzmocnienia cyberbezpieczeństwa RP, niemającym jednak mocy prawnej, system cyberbezpieczeństwa dzieli się na trzy podsystemy. Krajowy system cyberbezpieczeństwa jest jedynie częścią całego systemu cyberbezpieczeństwa państwa. Niektóre z podmiotów KSC wpisują się w kilka podsystemów, co rodzi problem rozgraniczenia obowiązków i uprawnień oraz właściwego ich przydzielenia do danego podsystemu. Należy wskazać miejsce i rolę KSC w całym systemie cyberbezpieczeństwa państwa. Oprócz instytucji i organów istnieje niedoceniony komponent społeczny, również wymagający szczegółowej analizy.

---

[26] Konstytucja RP z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78, poz. 483 z późn. zm.).
[27] 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.
[28] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560 z późn. zm.).
[29] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. 2011 nr 222, poz. 1323 z późn. zm.).
[30] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. 1997 nr 88, poz. 553 z późn. zm.).
[31] Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

W odniesieniu do Strategii Bezpieczeństwa Narodowego (2020 r.)[32] istnieje zapis dotyczący rozwijania kompetencji, wiedzy i świadomości zagrożeń w społeczeństwie, w obszarze cyberbezpieczeństwa. Biorąc pod uwagę najnowszą Strategię Cyberbezpieczeństwa RP na lata 2019-2024[33] , w stosunku do poprzedniej (2017-2022), cel, który został określony jako *„stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli”* rozszerzono o *„rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni”*. Tak więc wspomniana świadomość jest niezwykle istotnym czynnikiem w kształtowaniu bezpiecznej cyberprzestrzeni.

Raporty cyberbezpieczeństwa zawierające statystyki zagrożeń dla instytucji, podmiotów oraz organizacji wskazują zagrożenia występujące w cyberprzestrzeni z podziałem na poszczególne kategorie. Opracowania stworzone zostały przez m.in. właściwe Zespoły *CSIRT* (ABW, MON, NASK), Orange Polska, EXATEL czy ESET.

Zdecydowanie więcej jest dostępnych materiałów o charakterze specjalistycznym i syntetycznym w obszarze cyberbezpieczeństwa aniżeli w kwestii kompetencji cyfrowych. Na uwagę zasługują opracowania NASK traktujące o poziomach kompetencji cyfrowych np. nauczycieli w zdalnym nauczaniu czy świadomości nastolatków w zakresie higieny cyfrowej.

Źródło wiedzy w zakresie rozwoju uczniów w sferze cyberbezpieczeństwa stanowią programy i plany kształcenia w szkołach. Inną kwestią jest sposób ich wykorzystywania i realizowania, co zachęca do weryfikacji tego stanu. Istnieją badania dotyczące wykorzystania nowoczesnych technologii informacyjnych i komunikacyjnych biorące pod uwagę różne aspekty pracy szkoły.

Pomimo faktu, iż przeprowadzone zostały projekty dotyczące określania dostępności nowoczesnych technologii w szkołach, wskazać można nadal pewien niedobór w tym obszarze, co potwierdziła m.in. sytuacja związana z pandemią COVID-19 – konieczność wprowadzenia edukacji cyfrowej.

1.9. Wnioski

Wybrany problem badawczy pt. ”Jakie czynniki i działania mają wpływ na budowanie świadomości oraz kompetencji cyfrowych w zakresie cyberbezpieczeństwa?”

[32] Strategia Bezpieczeństwa Narodowego, Warszawa 2020, (M.P. 2020 poz. 413 z późn. zm.).
[33]Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Warszawa 2019 (M.P. 2019 poz. 1037 z późn. zm.).

nie był jeszcze przedmiotem tego rodzaju badań w ścisłym znaczeniu. W związku z tym charakter badań określić można jako innowacyjny. Ważność tejże tematyki badawczej jest wynikiem jej aktualności, która odwołuje się do kwestii bezpieczeństwa państwa i narodu oraz dynamicznych zmian zachodzących w środowisku bezpieczeństwa, determinowanych m.in. przez szeroko rozumianą cyberprzestrzeń.

Badania stanowić będą bodziec do rozwoju dziedziny nauk społecznych i dyscypliny naukowej jaką są nauki o bezpieczeństwie. Bez wątpienia tematyka ta zainteresować powinna zarówno podmioty i instytucje oraz organizacje związane z szeroko rozumianym cyberbezpieczeństwem, jak i indywidualnych użytkowników chcących zwiększyć swoją świadomość sytuacyjną cyberzagrożeń.

W obszarze planowanych efektów badań wystąpiło określenie wiedzy dotyczącej działań mających wpływ na budowanie świadomości i kompetencji cyfrowych. Drugim zakładanym efektem jest uzyskanie informacji o metodach nauczania cyfrowych użytkowników. Kolejny efekt związany jest ze wzrostem świadomości zagrożeń w cyberprzestrzeni. Najważniejszy element jednak dotyczy rozwiązań mających na celu ulepszenie obecnego stanu wiedzy w zakresie świadomości zagrożeń w cyberprzestrzeni oraz świadomości w kształtowaniu systemu cyberbezpieczeństwa.

Konkludując, zrealizowane efekty badań są następujące: określenie poziomu świadomości użytkowników i sposobów jej zwiększenia; wskazanie metod nauczania użytkowników i określenie ich skuteczności; podanie rozwiązań prawnych w zakresie budowania świadomości i kompetencji cyfrowych oraz propozycje zmian; identyfikacja oraz wskazanie kierunków rozwoju systemu cyberbezpieczeństwa.

Niezwykle istotnym efektem badań jest również wskazanie sposobów rozwoju umiejętności wykorzystywania technologii cyfrowych i włączenia społecznego.

Jednym ze sposobów upowszechniania wyników badań może być publikowanie ich w celu np. wykorzystania w organizacjach, instytucjach i podmiotach związanych z cyberbezpieczeństwem. Szczególnie przydatne będą wnioski z możliwością wykorzystania ich jako rekomendacji skierowanych do szkół, w celu inicjowania działań wspierających rozwój kompetencji cyfrowych uczniów.

2. Istota cyberbezpieczeństwa

2.1. Definicje, aspekty techniczne, technologiczne i społeczne cyberprzestrzeni. Ujęcie cyberprzestrzeni w polskich regulacjach

Niniejszy podrozdział zawiera przegląd informacji dotyczących cyberprzestrzeni oraz jej ujęć rozumianych w wybranych państwach. Ponadto, eksploracja wskazanego obszaru pozwoliła na ustalenie pewnych ograniczeń cyberprzestrzeni i implikacji z nimi związanych.

Nieustanny rozwój technologii informacyjno-komunikacyjnych tworzy zależności między życiem milionów użytkowników Internetu. Kreuje nie tylko nowe możliwości, ale także nowe wyzwania i zagrożenia. Jeszcze kilkadziesiąt lat temu niewyobrażalne dla całego świata była międzynarodowa wymiana informacji, użytkowanie e-bankowości czy korzystanie w różnych aspektach z portali społecznościowych. Takie zachowania są przyczynkiem do cyfryzacji ludzkiego życia czy wręcz wirtualizacji rzeczywistości. Poniższa tabela przedstawia procentowy udział ludzi korzystających z sieci w określonych regionach świata. Co szczególne interesujące – stanowi podstawę analizy dynamiki procesu jakim jest globalizacja.

Tab. 2.1

Dostępność do Internetu w skali świata

STATYSTYKI DOTYCZĄCE KORZYSTANIA Z INTERNETU NA ŚWIECIE 2021						
Regiony świata	**Ludność (2021)**	**Populacja % użytkowników Internetu na świecie**	**Użytkownicy Internetu 31 Mar 2021**	**Wskaźnik penetracji (% Pop.)**	**Wzrost 2000-2021**	**Internet całego świata %**
Azja	4,327,333,821	54.9 %	2,762,187,516	63.8 %	2,316.5 %	53.4 %
Europa	835,817,920	10.6 %	736,995,638	88.2 %	601,3 %	14.3 %
Afryka	1,373,486,514	17.4 %	594,008,009	43.2 %	13,058 %	11.5 %
Ameryka Łacińska	659,743,522	8.4 %	498,437,116	75.6 %	2,658.5 %	9.6 %
Ameryka Północna	370,322,393	4.7 %	347,916,627	93.9 %	221.9 %	6.7 %
Bliski Wschód	265,587,661	3.4 %	198,850,130	74.9 %	5,953.6 %	3.9 %
Oceania /	43,473,756	0.6 %	30,385,571	69.9 %	298.7 %	0.6 %

Australia						
ŚWIAT OGÓŁEM	7,875,765,587	100.0 %	5,168,780,607	65.6 %	1,331.9 %	100.0 %

Źródło: opracowanie własne na podstawie: Statystyki w Internecie, www.internetworldstat.com/stats.htm [dostęp 02.06.2021 r.]

Najmocniej umiejscowionym w sieci regionem jest Ameryka Północna, choć Europa wytrwale walczy o to miano (odpowiednio blisko 94 % do 88 %). W ciągu ostatniego dwudziestolecia, w kwestii progresu dostępu do Internetu największy postęp uczyniła Europa. Najmniejszy udział w tzw. Internecie świata mają Ocenia/Australia oraz Bliski Wschód, związane jest to z niewielką populacją. Wracając natomiast do wskaźnika penetracji – nasycenia siecią na ostatniej pozycji plasuje się Afryka z wynikiem ok. 43 %. Powyższe liczby i procenty świadczą o tym, jak ogromne znaczenie ma obecnie status *„online”*. Pandemia koronawirusa jeszcze mocniej wpłynęła na aktywność użytkowników w sieci. Można by mnożyć przykłady dotyczące wzrostu użycia Internetu spowodowanego tą sytuacją. Zajęcia szkolne czy uczelniane przeniosły się do świata wirtualnego, zaś wiele firm zdecydowało o prowadzeniu swojej działalności tylko przy użyciu tej technologii.

Nie jest w pełni znany źródłosłów pojęcia cyberprzestrzeni, można stwierdzić, iż stanowi ono hybrydę dwóch słów – *kybernets* – z greckiego sternik, kontrolować, oraz *space*, co z angielskiego oznacza – przestrzeń. Nie są określone również związki pojęcia cyberprzestrzeń z cybernetyką. Zwraca się uwagę, iż z etymologicznego punktu widzenia pojęcie cyberprzestrzeni wywodzi się z cybernetyki[34], która ukształtowana została przez prof. Norberta Weinera, amerykańskiego matematyka jeszcze w 1948 r. Zdefiniował ją jako kontrolę i komunikację między światem zwierząt oraz maszyn. To właśnie koncepcja N. Weinera wskazując na nowe formy interakcji między ludźmi i maszynami tworzące system funkcjonujący w nowym środowisku, była punktem wyjścia do stworzenia określenia cyberprzestrzeń[35].

Literatura przedmiotu definiuje „cyberprzestrzeń” jako ogół powiązań o charakterze wirtualnym, czyli nieprzestrzennym, powstałych poprzez ich fizyczne manifesta-

[34] M. Lakomy, 2015, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersystetu Śląskiego, Katowice, s. 74.
[35] R. Ottis; P. Lorents, 2010, *Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security: 5th International Conference on Information Warfare and Security, Academic Conferences Limited*, Dayton, Ohio, USA, 267−270.

cje (komputery czy też infrastruktura telekomunikacyjna)[36]. „*Przestrzeń informacji, którą tworzą łącznie wszystkie sieci komputerowe*"[37]. Bardziej dokładną, dość precyzyjną definicję cyberprzestrzeni podają P. Tekielska i Ł. Czekaj[38]: „*mianem cyberprzestrzeni wyraża się sieć łączącą systemy komputerowe, które obejmują jednostki centralne i ich oprogramowanie, ale także dane, środki i sposoby ich przesyłania. Cyberprzestrzeń dotyczy systemów powiązań internetowych, usług teleinformatycznych oraz systemów zapewniających prawidłowe funkcjonowanie kraju, tj. systemy transportu, systemy infrastruktury energetycznej, łączności, gazowej, wodociągowej czy ochrony zdrowia*". W opisie tym ujęto niezwykle cenne obszary państwa, czyli systemy składające się na infrastrukturę krytyczną. Tak więc cyberprzestrzeni przypisuje się ogromną wartość.

Niezwykle trafną odpowiedzią na pytanie co, kto, gdzie, w jakim celu, w cyberprzestrzeni? – jest propozycja definicji M. Szyłkowskiej: *„cyberprzestrzeń – obszar (systemy, sieci, urządzenia), w którym funkcjonuje zdigitalizowana informacja wytworzona przez człowieka (twórcę informacji) w dowolnej formie (dźwięk, obraz, dane) w którym to obszarze informacja może być: wytwarzana, przetwarzana, transmitowana i przechowywana – determinując dalsze powiązania i działania poprzez cele (cel powstania) i funkcje (przekazanie informacji), aby osiągnąć za jej pomocą określony skutek (lub zmianę)[39].* Charakterystyka ta odbiega dość znacząco od innych, w szczególności podkreślając istotę informacji oraz cel (cele powstania).

Powieść *Neuromancer* W. Gibsona stanowi podwaliny definicji cyberprzestrzeni. Mimo, że od jej napisania minęło już 30 lat, to nadal treść wydaje się być aktualna. *„To jest halucynacja, konsensualna, cyberprzestrzeń, doświadczana każdego dnia przez użytkowników we wszystkich regionach świata, przez dzieci nauczane matematycznych pojęć. Stanowi to graficzne odwzorowanie danych pobieranych z wszelkich banków na wszystkich komputerach świata. Niewyobrażalna złożoność[40]"*. W swojej definicji au-

[36] M. Madej, 2009, *Rewolucja informatyczna – istota, przejawy oraz wpływ na przestrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Wydawnictwo PISM, Warszawa, s. 28.
[37] D. D. Denning, 2002, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo WNT, Warszawa, s. 25.
[38] P. Tekielska, Ł. Czekaj, 2014, *Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego* [w:] M. Gorka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa.
[39] M. Szyłkowska, 2014, *Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Wydawnictwo WSPoL, Szczytno, s. 483.
[40] W. Gibson, 2009, *Neuromancer*, Wydawnictwo Książnica, Warszawa, s. 43.

tor wskazuje podstawowe elementy opisywanego zjawiska: rozległość, złożoność, bezprzestrzenność oraz jedną całość.

Wspomniane nienaukowe rozumienie słowa *„cyberprzestrzeń"* będące wytworem wyobraźni i niezidentyfikowanego zjawiska stopniowo zaczęło zmieniać się w kierunku sfery realnej, ale niematerialnej działalności ludzkiej, złożonej z sieci i komputerów. Następnie zaczęło się ono przejawiać w dokumentach czy strategiach państwowych, np. strategiach bezpieczeństwa[41].

Aby zrozumieć znaczenie słowa *„cyberprzestrzeń"* należy odnieść się do uregulowań prawnych, doktryn i strategii. Powszechnie cytowaną definicją jest ta, sformułowana przez Departament Obrony USA „*globalna domena środowiska informacji, która składa się z współzależnych sieci, te zaś tworzone są poprzez infrastrukturę technologii informacyjnej (IT) i zawartych danych, w tym: sieci telekomunikacyjne, Internet, systemy komputerowe, kontrolery oraz procesory*[42]. Opis ten nie zawiera żadnych odniesień w stosunku do społeczeństwa, użytkownika czy relacji ich łączących. Jest to *sensu stricte* podejście techniczne. Rozwinięcie tej kwestii przyjęto w 2003 r. w *Narodowej Strategii dla Bezpiecznej Cyberprzestrzeni*[43], co stanowi obecnie już historyczne rozwiązanie rządu USA w tamtych latach. Strategia definiowała cyberprzestrzeń jako nerwowy-system kontroli państwa. Złożona z setek tysięcy połączonych komputerów, routerów, serwerów, kabli światłowodowych, umożliwiających działanie infrastruktury krytycznej. Właściwe jej funkcjonowanie ma zasadnicze znaczenie dla całej gospodarki i bezpieczeństwa narodowego[44]. Poprzez nazwanie cyberprzestrzeni systemem nerwowym państwa odczytać należy, że to niezwykle rozległy system mający w swoim zasięgu sektory gospodarki, administracyjne, bezpieczeństwa czy infrastruktury krytycznej. Stąd, przestrzeni tej przypisywana jest ogromna wartość, która stanowić będzie o rozwoju całego kraju.

Przechodząc na grunt europejski, jak wskazano w słowniku pojęć z zakresu społeczeństwa informacyjnego, Komisja Europejska zdefiniowała cyberprzestrzeń jako *„wirtualną przestrzeń, w której krążą elektroniczne dane, te zaś przetwarzane są przez*

[41] T.R. Aleksandrowicz, K. Liedel, 2014, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Wydawnictwo Difin, Warszawa, s. 23.
[42] G.A. Crowther, 2017, *The Cyber Defense Review*, Vol. 2, No. 3, Army Cyber Institute, s. 63.
[43] *National Strategy to Secure Cyberspace, U.S. Department of Homeland Security,* 2003, https://georgewbush-whitehouse.archives.gov/pcipb/ [dostęp 04.09.2021 r.].
[44] https://www.cisa.gov/national-strategy-secure-cyberspace [dostęp 04.09.2021 r.].

komputery PC na całym świecie[45]*"*. Podstawą tej definicji jest przestrzeń wirtualna, zawierająca przesyłane dane (w domyśle są to strony internetowe, procesy czy aplikacje). Pewne zawężenie odczuć można przybliżając się znaczeniu komputerów PC – „*personal computer"*. Tak więc czy oznacza to, że według tej definicji składową cyberprzestrzeni nie są inne urządzenia przetwarzające dane w sieciach (typu smartfony, tablety, smartwach-e)? W praktyce rzeczywiście te urządzenia nie wpisują się w charakterystykę cyberprzestrzeni zgodnie z ujęciem Unii Europejskiej.

W ww. definicjach kontekst narzędziowy jest najmocniej zaznaczony, niestety stanowi to o marginalizowaniu bądź pomijaniu kontekstu społecznego cyberprzestrzeni, odnoszącego się do użytkowników cyberprzestrzeni. Komponent społeczny obejmuje środowisko, które jest rezultatem niematerialnej formy interakcji między ludźmi, usługami i oprogramowaniem realizowanymi przez urządzenia techniczne i sieci; stąd równie ważna jest relacja z ludźmi i wspomniane interakcje[46].

Zdaniem autora niniejszej dysertacji, cyberprzestrzeni nie da się analizować w zakresie jedynie technologicznym. Stanowi ona cały mechanizm społeczny, mechanizm komunikacji, zaś warstwa cyfrowa jest jej bodźcem. Tak naprawdę więc, kwestie interoperacyjności systemów informatycznych, zwalczania cyberprzestępczości czy umiejętności współżycia społecznego w sieci, stoją na równo ze sobą w aspekcie użytkowania sieci, co jednocześnie powinno wpłynąć na kreowanie bezpieczeństwa w cyberprzestrzeni.

Próby zdefiniowania cyberprzestrzeni dokonywane są najczęściej w strategiach cyberbezpieczeństwa danego państwa. Taka analiza stworzona została w oparciu o rozwiązania pochodzące z Polski na tle również innych państw m.in. z Niemiec, Czech, Słowenii, Litwy, Anglii, Francji oraz Rumunii.

Jako pierwsza wskazana będzie charakterystyka przyjęta w Strategii Cyberbezpieczeństwa[47] z roku 2011 przez zachodniego sąsiada Polski, czyli Niemcy. *„Cyberprzestrzeń to wirtualna przestrzeń wszystkich systemów informatycznych połączonych na poziomie danych w skali globalnej. Podstawą cyberprzestrzeni jest Internet jako*

---

[45] Słownik pojęć z zakresu społeczeństwa informacyjnego, Komisja Europejska, https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http://eurovoc.europa.eu/6140 [dostęp 04.09.2021 r.]; cyt. za: B. Drawińska-Kania, 2017, *Koszty cyberprzestępczości-perspektywa rachunkowości*, „Zeszyty Naukowe SGH w Warszawie", nr 157, s. 91.

[46] J. Rzucidło, J. Węgrzyn, 2015, *Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni,* „Przegląd Prawa Konstytucyjnego" 5/27, s. 142.

[47] *Cyber Strategy for Germany, 2011, Federal Minister of the Interior and Community,* https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 [dostęp 02.09.2021 r.].

uniwersalna i publicznie dostępna sieć połączeń i transportu, która może być uzupełniana i dalej rozbudowywana przez dowolną liczbę dodatkowych sieci danych. Systemy informatyczne znajdujące się w odizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni"[48]. Opis ten odnosi się do kwestii technologicznych cyberprzestrzeni i to właśnie stanowi jej podstawę. Podobnie jak w przypadku definiowania przez Komisję Europejską, w tym miejscu również dostrzec należy fundament – *„wirtualną przestrzeń",* tak więc wyodrębnioną logicznie przestrzeń – nie w sensie fizycznym. Niemieckie ministerstwo bardzo trafnie wskazało na atrybut cyberprzestrzeni jako możliwość jej rozbudowy. Tym samym nie ograniczają swojej definicji do jedynie istniejących już połączeń i sieci, ale również dostosowują ją do zmieniającego się otoczenia i środowiska. Niemieckie podejście do tematyki cyberprzestrzeni jest płynne i rozwojowe.

Do kwestii przestrzeni odwołują się także Rumuni[49]. *„Wirtualne środowisko generowane przez infrastrukturę cybernetyczną, w tym przetwarzane, przechowywane lub przekazywane informacje dotyczące treści, jak również działania podejmowane w tym środowisku przez użytkowników"*[50]. W ujęciu tym przenika również kontent socjologiczny, który jeszcze bardziej uwypuklony jest we Francji[51] czy Austrii, łączącej ww. kryteria. *„Cyberprzestrzeń to przestrzeń wirtualna wszystkich systemów informatycznych połączonych ze sobą na poziomach danych w skali globalnej. Podstawą cyberprzestrzeni jest Internet, czyli uniwersalna i publicznie dostępna sieć połączeń i transportowa, która może być stale uzupełniana i rozszerzana poprzez inne sieci danych. W języku potocznym cyberprzestrzeń odnosi się również do globalnej sieci różnych niezależnych infrastruktur, sieci telekomunikacyjnych oraz systemów komputerowych. W sferze społecznej korzystanie z tej sieci globalnej pozwala jednostkom na interakcje, rozpowszechnianie informacji, wymianę pomysłów, angażowanie się w działalność gospodarczą, kontrolowanie działań, udzielanie wsparcia społecznego, tworzenie dzieł*

---

[48] Ibidem.

[49] *The Cyber Security National System*, *The Government of Romania,* 2013, https://cyberwiser.eu/romania-ro#:~:text=The%202013%20strategy%20includes%20a,capabilities%2C%20increasing%20the%20resilience%20of [dostęp 01.09.2023 r.]. Zob.: https://sherloc.unodc.org/cld/uploads/res/lessons-learned/strategia-de-securitate-cibernetica-a-romaniei_html/STRATEGIA_de_securitate_cibernetic_a_Romanei.pdf [dostęp 01.09.2023 r.].

[50] *Cyber Strategy of Romania, The Government of Romania, 2013,* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Romania [dostęp 01.09.2021 r.].

[51] *French National Digital Security Strategy, The Government of France, 2015,* https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf [dostęp 01.09.2021 r.].

sztuki i mediów, uczestniczenie w dyskusjach politycznych i wiele wiele innych. Cyberprzestrzeń stała się pojęciem zbiorczym dla wszystkich rzeczy związanych z Internetem i dla różnych internetowych kultur. Wiele krajów uważa sieciowe technologie informacyjno-komunikacyjne i niezależne sieci działające za pośrednictwem tego medium jako elementy ich narodowych infrastruktur krytycznych"[52]. Zgodnie z powyższym, ponownie wskazuje się na istotną rolę Internetu jako fundamentu cyberprzestrzeni, a także na rozwojowy charakter tego terminu.

Ujęcie czeskie[53] skupia się na sferze informacyjnej: *„Cyberprzestrzeń oznacza środowisko cyfrowe, umożliwiające tworzenie, przetwarzanie i wymianę informacji, tworzone przez systemy i usługi informatyczne oraz sieci komunikacji elektronicznej"*[54]. Brak natomiast jasnej wzmianki dotyczącej użytkowników cyberprzestrzeni czy też relacji między nimi zachodzących. Nacisk na kwestie informacji zauważyć również można w dokumentach Litwinów[55]: *„Środowisko, w którym informacje elektroniczne są tworzone przy użyciu pojedynczych komputerów lub innych urządzeń informacyjno-komunikacyjnych i/lub przekazywane poprzez sieć elektroniczną do innych podłączonych komputerów lub innych urządzeń informacyjno-komunikacyjnych*[56]*".* Tożsame podejście prezentuje Grecja, opisując cyberprzestrzeń jako cyfrową domenę przetwarzania informacji[57].

Słowacja natomiast podkreśla znaczenie aterytorialności cyberprzestrzeni *„to wirtualna przestrzeń bez granic, składająca się z połączonych na całym świecie sieci sprzętu, oprogramowania i danych"*[58]. Cyberprzestrzeń nieposiadającą granic opisują również Holendrzy w *National Cyber Security Agenda. A cyber secure Netherlands*,

---

[52] *Austrian Cyber Security Strategy, The Government of Austria, 2013,* https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf [dostęp 01.09.2021 r.].

[53] *Strategy of the Czech Republic in the field of cybernetic security*, *The Government of Czech Republic,* 2015, https://nukib.gov.cz/en/cyber-security/strategy-action-plan/ [dostęp 01.09.2023 r.].

[54] *Act on Cyber Security, The Government of Czech Republic, 2015,* https://nukib.cz/download/publications_en/legislation/nbu_zkb_navrh_130723_senat_EN.pdf [dostęp 01.09.2021.].

[55] N*ational Cyber Security Strategy*, *The Government of The Republic of Lithuania,* 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf [dostęp 01.09.2023 r.].

[56]*The Cyber Security Environment in Lithuania, The Government of The Republic of Lithuania, 2018,* https://www.vkontrole.lt/failas.aspx?id=3504 – [dostęp 01.09.2021 r.].

[57] *National Cyber Security Strategy for Greece, The Government of the Hellenic Republic, 2020, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/GRNCSS_EN.pdf* [dostęp 01.09.2021 r.].

[58] *Cyber Security Concept of the Slovak Republic for 2015-2020, The Government of Slovak Republic,* 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 [dostęp 30.08.2021 r.].

gdzie wskazują na cyfrową domenę z danymi, połączeniami, podmiotami oraz Internetem[59]. Podobnie jest w przypadku Estonii[60].

W kontekście ograniczeń cyberprzestrzeni, możliwe jest wyróżnienie jej specyficznych obszarów. Poniższa tabela ocenia jak bardzo jeszcze cyberprzestrzeń jest sferą niedoprecyzowaną i zadaje pytanie czy kiedykolwiek stanie się możliwe jej dookreślenie?

Tab. 2.2

Obszary ograniczeń cyberprzestrzeni

L.p.	**Obszar**	**Charakterystyka**
1.	Przestrzeń	➢ brak granic geograficznych; ➢ brak granic przestrzennych; ➢ brak granic politycznych; ➢ brak granic doraźnych.
2.	Prawo	➢ niejasna odpowiedzialność za wykroczenia i czyny; ➢ brak narodowych jak i międzynarodowych kryteriów klasyfikacji i kwalifikacji czynów; ➢ mało precyzyjne określenia aktów kryminalnych; ➢ prawo niespójne, niejasne.
3.	Zagrożenia	➢ niewielkie koszty ataków; ➢ anonimowość sprawy; ➢ prosta, powszechnie dostępna technologia; ➢ wielość form cyberataków; ➢ skutek: „efekt domina”.
4.	Bezpieczeństwo	➢ wysokie koszty zabezpieczeń; ➢ brak szybkich rozwiązań zabezpieczających; ➢ mnogość obiektów ataków; ➢ zróżnicowana podatność obiektów; ➢ praktycznie zerowa przewidywalność źródeł zagrożeń.

Źródło: opracowanie własne na podstawie: P. Sienkiewicz, 2015, *Ontologia cyberprzestrzeni*, "Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 13, s. 94

[59] *National Cyber Security Agenda. A cyber secure Netherlands, The Government of the Netherlands*, *2018,* https://www.cyberwiser.eu/sites/default/files/NL_NCSS_2018_en%20%282%29.pdf [dostęp 06.09.2021 r.].

[60] *Cyber Security Strategy – Republic of Estonia, 2019-2022, The Government of Estonia, 2019,* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp 01.09.2021 r.].

Strategie Cyberbezpieczeństwa Zjednoczonego Królestwa w taki oto sposób definiują opisywane zjawisko: *„Cyberprzestrzeń obejmuje wszystkie formy działalności cyfrowej połączonej w sieć; obejmuje ona treści i działania prowadzone za pośrednictwem sieci cyfrowych*[61]*. Współzależna sieć infrastruktur technologii informacyjnych, która łączy Internet, sieci telekomunikacyjne, systemy komputerowe, urządzenia oraz wbudowane procesory i kontrolery. Może również odnosić się do wirtualnego świata lub domeny jako zjawiska lub abstrakcyjnej koncepcji"*[62]. Spojrzenie to w swoim zakresie posiada zarówno aspekty społeczne jak i techniczne cyberprzestrzeni. Podkreśla znaczenie ludzkiej aktywności i komunikacji przebiegającej w sieci. Poprzez użycie sformułowania „*wszystkie formy"* uzyskuje domniemanie, żeby do cyberprzestrzeni wpisać również telewizory, urządzenia AGD czy też konsole. Ponadto, bardzo ogólne opisanie jej jako „*abstrakcyjnej koncepcji"* rodzi zapytanie o szczegółowość, a raczej brak szczegółowości w definiowaniu cyberprzestrzeni. Pociąga to za sobą kolejne pytania i końcowy wniosek, iż definicja ta tak naprawdę nie stanowi podstawy do ścisłego rozróżnienia co można zaliczyć do cyberprzestrzeni, a czego nie.

Większość strategii cyberbezpieczeństwa przyjmuje całościowe spojrzenie na cyberprzestrzeń. Jednakże niemiecka wyraźnie stwierdza, że uwzględnia jedynie technologie informacyjno-komunikacyjne związane z Internetem. Australijskie, kanadyjskie, hiszpańskie i nowozelandzkie rozwiązania sugerują ten sam wąski pogląd na to, co składa się na cyberprzestrzeń. Strona holenderska wyraźnie stwierdza, że dotyczy ona pełnego zakresu *ICT*, który oprócz *ICT* podłączonych do Internetu, obejmuje na przykład karty chipowe, systemy samochodowe oraz nośniki przekazu informacji. Republika Czeska, Estonia, Francja i Republika Południowej Afryki zgadzają się z tym ostatnim poglądem. Pozostałe krajowe systemy statystyczne są mniej otwarte na ten temat, ale nie zawężają wyraźnie swojej uwagi do "tylko Internetu"[63]. Konkludując, cyberprzestrzeń opiera się na elementach społecznych, technologicznych oraz technicznych[64].

---

[61] *Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space, The Government of the United Kingdom, 2009,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 03.09.2021 r.].

[62] *National Cyber Security Strategy 2016-2021, The Government of the United Kingdom, 2016,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 05.09.2021 r.].

[63] https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies [dostęp 01.09.2021 r.].

[64] K. Dobrzyniecki, 2004, *Prawo a etos cyberprzestrzeni*, Wydawnictwo Adam Marszałek, Toruń, s.21.

Istnieje niedobór w kwestii ujednolicenia definicji cyberprzestrzeni na poziomie już regionalnym, czy nawet globalnym, rodzi to problem egzekwowania odpowiedzialności za czyny zabronione – popełniane w cyberprzestrzeni. W poszczególnych państwach kwalifikacje i klasyfikacje czynów różnią się, co powoduje brak zidentyfikowania danego cyberzagrożenia.

Powyższa analiza ilustruje brak jednej powszechnie zgodnej i uznawanej definicji terminu *„cyberprzestrzeń”*. Jak najbardziej we wszystkich wymienionych opisach możliwe jest znalezienie wspólnych mianowników, jednak nadal nie rozwiązuje to kwestii pełnego zrozumienia. Wynikać to może np. z różnego podejścia osób opracowujących takie terminy, zdania socjologów, politologów czy sekuritologów są odmienne już na wstępie. Taka konfrontacja definicji w jednym opracowaniu umożliwia dostrzeżenie podobieństw, ale i różnic, co okazać się może przydatne w przyszłości[65].

Zakres pojęciowy *„cyberprzestrzeni”* może skutkować poważnymi konsekwencjami podczas współpracy na arenie międzynarodowej. Dla przykładu, biorąc udział w ćwiczeniach z zakresu cyberbezpieczeństwa, znamienne są zawsze podstawy, jasne określenie kto, co, gdzie, kiedy, jak i w jakim celu? W analizowanym przypadku przysporzy to najprawdopodobniej wielu problemów.

2.1.1. Ujęcie cyberprzestrzeni w polskich regulacjach

Prawna analiza terminu *„cyberprzestrzeń”* przeprowadzona została w miarę możliwości i potrzeb zgodnie z hierarchią aktów prawa w Polsce:

- konstytucja,
- ratyfikowane umowy międzynarodowe,
- ustawy,
- rozporządzenia,
- akty prawa miejscowego,
- doktryny,
- strategie.

W tzw. ustawie zasadniczej, jaką jest Konstytucja RP ustawodawca nie używa określenia *„cyberprzestrzeń”*. Pierwszym europejskim prawem w zakresie cyberbezpieczeństwa jest ustanowiona w 2016 roku Dyrektywa Parlamentu Europejskiego i Ra-

[65] https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/11/6.pdf [dostęp 01.09.2021 r.].

dy (UE) tzw. Dyrektywa NIS (*Network and Information Systems Directive)*[66], jej polską implementację stanowi ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r.[67].

Niezwykle interesującym jest fakt, iż ustawa ta nie określa przedmiotowej definicji. Natomiast w art. 3 pkt. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[68] zawarte jest: *„jako cyberprzestrzeń rozumiana jest przestrzeń przetwarzania oraz wymiany informacji tworzona przez systemy teleinformatyczne, łącznie z powiązaniami między nimi i relacjami z użytkownikami”*. Wskazano jasno, aczkolwiek ogólnie czym jest cyberprzestrzeń oraz sprecyzowano wchodzące w jej skład podmioty, ponadto podkreślono znaczenie interakcji między użytkownikami. Cyberprzestrzeń stanowi wirtualne miejsce wymiany informacji, to miejsce dla ludzkiej aktywności pod kątem np. informacji czy komunikacji.

To samo tłumaczenie zawiera ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym […] [69].

Cytowana w poprzednich rozdziałach Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej z roku 2015 uwypukla znaczenie cyberprzestrzeni: *„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”*[70].

Odnosząc się do Strategii Cyberbezpieczeństwa RP na lata 2019-2024, *„Cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590), wraz z powiązaniami między nimi oraz*

[66] 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, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148 [dostęp 02.08.2021 r.].
[67] Zob. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560 z późn. zm.).
[68] Zob. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.).
[69] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323 z późn. zm.).
[70] Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s.7.

relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932)"[71]. Definicja systemów teleinformatycznych jest jednakowa, jak ta pochodząca z Doktryny Cyberbezpieczeństwa.

Analizując najważniejsze cechy definicji cyberprzestrzeni wyjętej z ustawy krajowej, należy wskazać, iż definicja ta wprowadza koncept jednej cyberprzestrzeni, będącej logicznie wydzielonym obszarem – cyfrową platformą przetwarzania i wymiany informacji. Przestrzeń ta mając charakter ponadnarodowy, jest tworzona poprzez systemy teleinformatyczne połączone przy pomocy sieci telekomunikacyjnych, w tym również sieci, których elementy zlokalizowane są na terenie innych państw czy podmiotów. Działania w cyberprzestrzeni nie ograniczają się jedynie do wymiany informacji. Dotyczyć mogą także samego ich wytwarzania, modyfikowania czy po prostu odczytywania. Tak więc również te operacje dokonywane są na gruncie cyfrowej domeny.

W definicji, wskazując na wzajemne relacje systemów z ich użytkownikami, zaznaczono pewnego rodzaju dwustronne powiązania działań w cyberprzestrzeni z działaniami w rzeczywistości, którą nazwać można „fizyczną" (rzeczywisty świat) i ich wzajemne konsekwencje[72].

Biorąc pod uwagę wszelkie wyżej wymienione określenia definicyjne oraz wnioski autora pracy dotyczące cyberprzestrzeni, uznać należy, iż cyberprzestrzeń:

- jest logicznie wyodrębnionym obszarem-cyfrową domeną wytwarzania, wymiany i przetwarzania informacji;
- ma charakter transgraniczny, globalny - jej składowe rozlokowane mogą być na całym świecie;
- przenika wszystkie sektory gospodarki i przez to wpływa na funkcjonowanie współczesnego państwa i społeczeństwa;
- można ją określić niezależną od granic, odległości, czasu czy też miejsca;
- w połączeniu i wykorzystaniu technologii informacyjno-komunikacyjnych wiąże ludzką działalność w świecie rzeczywistym.

[71]Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M.P. 2019 poz. 1037 z późn. zm.), s. 6.
[72] J. Wasilewski, 2013, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", 9, s. 228–231.

Cechą odróżniającą cyberprzestrzeń od innych nośników informacji powoduje fakt, iż dane w sieci kształtować może każdy użytkownik, stanowią przekaźnik interaktywny, w przeciwieństwie do przekazów nadawanych jednostronnie np. przy pomocy telewizji czy radia.

2.2. Cyberbezpieczeństwo – zakres pojęciowy, struktura

Analizując strategie cyberbezpieczeństwa wybranych państw, stwierdzić należy, iż np. Czechy, Hiszpania, Japonia, Litwa czy Luksemburg traktuje bezpieczeństwo cybernetyczne na poziomie strategicznym, w ogóle nie definiując tego pojęcia. Ponadto, rozumienie cyberbezpieczeństwa różni się znacznie wśród dziesięciu narodów, które zdefiniowały lub opisały to pojęcie. Niektóre kraje definiują cyberbezpieczeństwo w podejściu oddolnym, nadając mu niejako właściwości bezpieczeństwa informacji, które należy zabezpieczyć i zagwarantować. Inne kraje stosują holistyczne podejście odgórne i szukają ochrony przed zagrożeniami pochodzącymi z cyberprzestrzeni[73].

Na początku 2011 r. rosyjsko-amerykańska dwustronna grupa robocza działająca w ramach *East West Institute (EWI)* i Uniwersytetu Moskiewskiego opracowała międzynarodowe ramy terminologiczne dotyczące cyberterminologii. Zdefiniowali oni bezpieczeństwo cybernetyczne jako *"właściwość cyberprzestrzeni, która jest zdolna do przeciwstawiania się zamierzonym i niezamierzonym zagrożeniom oraz reagowania i odzyskiwania danych"*. Pomimo trwających dyskusji akademickich na temat większości definicji terminologicznych domeny cybernetycznej, definicja bezpieczeństwa cybernetycznego autorstwa Rauschera i Yashenko może zastąpić wiele narodowych definicji i sposobów rozumienia cyberbezpieczeństwa przedstawionych w Tabeli 2.3. Jednak pogląd Kanady na bezpieczeństwo cybernetyczne nie pokrywa się z definicją Rauschera i Yashenko, ponieważ Kanada zajmuje się tylko celowymi złośliwymi atakami cybernetycznymi. Dwa inne narody rozszerzają pogląd (Rauscher i Yashenko, 2011). Wielka Brytania uwzględnia w swojej definicji zagrożenia zakłóceniami fizycznymi i elektromagnetycznymi w cyberprzestrzeni w swojej definicji (CO, 2009, 2011). Niemcy włączają do swojej definicji pojęcie akceptacji ryzyka[74].

[73] https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies [dostęp 01.09.2021 r.].
[74] Ibidem.

Tab. 2.3

Rozumienie cyberbezpieczeństwa w wybranych państwach

L.p.	Nazwa państwa	Definicja
1.	Australia	Środki odnoszące się do poufności, dostępności i integralności informacji, które są przetwarzane, przechowywane i przekazywane za pomocą środków elektronicznych lub podobnych środków[75].
2.	Francja	System informatyczny mający odporność na prawdopodobne zdarzenia wynikające z cyberprzestrzeni, które mogą zagrozić dostępności, integralności lub poufności przechowywanych, przetwarzanych lub przekazywanych danych oraz związanych z nimi usług, które oferują systemy teleinformatyczne[76].
3.	Indie	Jest to działalność polegająca na ochronie informacji i systemów informatycznych (sieci, komputerów, baz danych, centrów danych i aplikacji) za pomocą odpowiednich proceduralnych i technologicznych środków bezpieczeństwa.
4.	Kanada	Ochrona cyfrowych informacji i infrastruktury. Odpowiedni poziom reakcji na ataki cybernetyczne i/lub łagodzenia ich skutków - celowy lub nieuprawniony dostęp, wykorzystywanie, manipulowanie, zakłócanie lub niszczenie (za pomocą środków elektronicznych) informacji elektronicznych i/lub infrastruktury elektronicznej i fizycznej wykorzystywanej do przetwarzania, przekazywania i/lub przechowywania tych informacji[77].
5.	Niderlandy / Holandia	Stan wolny od zagrożeń lub szkód spowodowanych zakłóceniem lub zniszczeniem *ICT (Information and Communication Technologies)*, lub z powodu nadużywania *ICT*[78].
6.	Niemcy	Jest pożądanym celem sytuacji bezpieczeństwa informatyczne-

[75] *Australian Government, List of glossary terms,* https://www.cyber.gov.au/learn-basics/view-resources/glossary/c [dostęp 01.09.2023 r.].
[76] *French White Paper, Defence and National Security, The Government of The Republic of France,* 2013, https://ccdcoe.org/uploads/2018/10/White-paper-on-defense-2013-1.pdf [dostęp 01.08.2024].
[77] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/2016-scrty-prsprty-en.pdf [dostęp 01.08.2024].
[78] *National Cyber Security Agenda. A cyber secure Netherlands, The Government of the Netherlands, 2018,* https://www.cyberwiser.eu/sites/default/files/NL_NCSS_2018_en%20%282%29.pdf [dostęp 01.09.2021 r.].

		go, w której ryzyko (globalne) w cyberprzestrzeni zostało ograniczone do akceptowalnego minimum[79].
7.	Nowa Zelandia	Jest to praktyka polegająca na uczynieniu sieci tworzących cyberprzestrzeń możliwie jak najbardziej bezpiecznych (odpornych) przed włamaniami, utrzymywanie poufności, dostępności i integralności informacji, wykrywanie włamań i incydentów oraz reagowanie na nie i przywracanie ich do stanu normalnego[80].
8.	Republika Południowej Afryki	Jest zbiorem narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, metod zarządzania ryzykiem, podejść do zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, gwarancji oraz technologii, które mogą być wykorzystane do ochrony środowiska cybernetycznego oraz organizacji i zasobów użytkownika.
9.	Rumunia	Normalność, prawidłowość wynikająca z zastosowania zestawu proaktywnych i reaktywnych środków, które zapewniają poufność, integralność, dostępność, autentyczność i niezaprzeczalność informacji elektronicznych, a także publicznych i prywatnych zasobów i usług w cyberprzestrzeni[81].
10.	Uganda	Odniesienia do "bezpieczeństwa informacji": ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem[82].

[79] *Cyber Strategy for Germany, 2011, Federal Minister of the Interior and Community,* https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 [dostęp 02.09.2021 r.].

[80] *New Zeland's Cyber Security Strategy, The Government of New Zeland, 2015,* https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf [dostęp 01.09.2021].

[81] *The Cyber Security National System*, *The Government of Romania,* 2013, https://cyberwiser.eu/romania-ro#:~:text=The%202013%20strategy%20includes%20a,capabilities%2C%20increasing%20the%20resilience%20of [dostęp 01.09.2023 r.]. Zob.: https://sherloc.unodc.org/cld/uploads/res/lessons-learned/strategia-de-securitate-cibernetica-a-romaniei_html/STRATEGIA_de_securitate_cibernetic_a_Romanei.pdf [dostęp 01.09.2021 r.].

[82] *National Infromation Security Strategy, The Government of Uganda, 2011,* https://www.cert.ug/sites/default/files/2022-05/National%20Information%20Security%20Strategy%202011.pdf [dostęp 01.09.2021].

11.	Wielka Brytania	Obejmuje zarówno ochronę interesów narodowych w cyberprzestrzeni, jak i dążenie do realizacji szerszej polityki bezpieczeństwa narodowego poprzez wykorzystywanie wielu możliwości, jakie oferuje cyberprzestrzeń[83].

Źródło: opracowanie własne na podstawie: E. Luiijf, K. Besseling, P. De Graff, 2013, *Nineteen national cyber security strategies, International Journal of Critical Infrastructures, vol. 9, ½,* https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies [dostęp 01.09.2021 r.]

Nie wszystkie państwa mają precyzyjnie określone definicje cyberbezpieczeństwa. Niektóre wynikają jedynie z opisu, z tekstu, co wymaga analizy. Powodować to może nieporozumienia już na poziomie krajowym, ale i międzynarodowym. Dlatego też, taki stan rzeczy nie zaowocuje w kwestii wspólnego rozwiązywania globalnych zagrożeń w cyberprzestrzeni. Poszczególne kraje w zakresie bezpieczeństwa cybernetycznego odwołują się jedynie do systemów podłączonych do Internetu bądź do całości technologii informatyczno-komunikacyjnej. To pierwsze podejście wydaje się być szkodliwe, ze względu na fakt, iż niektóre systemy nie są podłączone do sieci. Przykład mogą stanowić systemy kontroli procesów w infrastrukturze informacyjnej bądź nieinformacyjnej.

„Art. 5. Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju"[84]. Pierwszy dokument, ustawa zasadnicza – wskazuje na bezpieczeństwo obywateli. Cyberbezpieczeństwo jest obszarem, składową całego bezpieczeństwa państwa czy narodu.

Nadrzędna ustawa sfery cyberbezpieczeństwa, wspomniana już wyżej określa cyberbezpieczeństwo jako: *„odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"*[85].

W Doktrynie Cyberbezpieczeństwa, przyjętej w 2015 roku, (de facto będącej już dokumentem historycznym, wykonawczym do Strategii Bezpieczeństwa Narodowego

[83] *Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space, The Government of the United Kingdom, 2009,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 01.09.2021 r.].
[84] Konstytucja RP…, op. cit.
[85] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560 z późn. zm.).

z 2014 r.) pojęcia *„cyberbezpieczeństwo RP”* tożsame jest z określeniem *„bezpieczeństwa RP w cyberprzestrzeni”* i oznacza: *„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”*[86]. Ponadto, w dokumencie tym zawarto określenie *„bezpieczeństwo cyberprzestrzeni RP”* jako części 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”*[87].

Bardzo zbliżony opis cyberbezpieczeństwa w stosunku do ustawy, ujęto w Strategii Cyberbezpieczeństwa RP na lata 2017-2022 (późniejsza strategia na lata 2019-2024 niestety nie zawiera dosłownej definicji). Pierwsza strategia postrzega *„cyberbezpieczeństwo”* na równi z *„bezpieczeństwem sieci i systemów informatycznych”* oraz *„bezpieczeństwa teleinformatycznego”*. *„Oznacza odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne”*[88]. Charakterystyka ta zbliżona jest do tej ujętej w ustawie o krajowym systemie cyberbezpieczeństwa, podkreśla się odporność systemów teleinformatycznych na różnego rodzaju działania w nie godzące.

Najbardziej aktualne w przepisach prawnych określenie pojęcia *cyberbezpieczeństwo*, ujęto w europejskim Akcie o cyberbezpieczeństwie z 2019 r. *„Cyberbezpieczeństwo obejmuje wszystkie działania niezbędne do ochrony przed cyberzagrożeniami sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą”*[89]. Wskazana definicja w sposób jak najbardziej pełny obejmuje bezpieczeń-

[86] Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s.7-8.
[87] Ibidem.
[88] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa 2017, (M.P. 2017 poz. 52 z późn. zm.), s. 28.
[89] 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), art. 2.

stwo zarówno systemów informatycznych, jak i zwraca uwagę również na czynnik społeczny- na bezpieczeństwo człowieka.

2.3. „Bezpieczna, globalna wioska" w kontekście sieci wzajemnych połączeń

Całkowite zanurzenie użytkowników w wirtualny świat nowych technologii stało się konsekwencją czasu. Można sięgnąć po przykład sposobu użytkowania telefonów komórkowych. Bardzo intuicyjna stała się ich obsługa, bez konieczności korzystania z instrukcji, jest to obecnie wręcz machinalne, naturalne, jednolicie zintegrowane z jakąkolwiek aktywnością człowieka. Podobnie, w przypadku zegarków, które już w latach 30. XX wieku stanowiły atrybut każdego człowieka, pozwalając sprawdzać czas i nie przerywając aktualnie wykonywanych czynności. Analogicznie, obecnie telefon komórkowy jest już znacznie częściej używany aniżeli zegarek. W kwestii Internetu, ten w 1995 r. był jeszcze czymś niezwykłym *„uwaga… teraz włączę Internet"*. Dziś można stwierdzić, że w Internecie raczej się *„jest"*, automatycznie, wręcz stale, zaś *„surfowanie"* po nim to naturalna, oczywista i bezproblemowa już czynność[90]. Można posłużyć się badaniami firm *Sapio Research i DoubleVerify*, według których w czasie pandemii wywołanej wirusem *SARS-CoV-2* (lata 2020-2023) człowiek spędzał jedną trzecią swojego dnia w Internecie. Konkretnie, przeciętny mieszkaniec Stanów Zjednoczonych lub Europy spędzał przed ekranem komputera bądź smartfona blisko siedem godzin dziennie. Dodając do tego osiem godzin pracy zdalnej, na sen i inne aktywności niezwiązane z siecią pozostaje jedynie nieco ponad dziewięć godzin[91]. Te wszystkie dane prezentują jak stopniowo coraz bardziej społeczeństwo przenosi swoje życie do Internetu i ekranów monitora.

Rozpatrując znaczenie globalnej wioski, zacząć należy od definicji *„globalizacji".* Są to bowiem charakterystyczne i dominujące pod koniec XX wieku i na początku XXI wieku tendencje w światowej polityce, ekonomii, demografii, życiu społecznym oraz kulturze, polegające na rozpowszechnianiu się zjawisk, bez zależności w kontekście geograficznym i gospodarczym zaawansowaniu danego obszaru na świecie. Wynikiem globalizacji jest ujednolicanie się obrazu świata stanowiącego homogeniczną całość wzajemnie ze sobą powiązanych elementów kultury jak i gospodarki[92]. Z globali-

[90] D. Lombard, 2008, *Globalna wioska cyfrowa. Drugie życie sieci*, Wydawnictwo MT Biznes, Warszawa, s. 95-96.

[91] https://www.benchmark.pl/aktualnosci/ile-czasu-spedzamy-przed-ekranami-w-erze-pandemii.html [dostęp 06.01.2022 r.].

[92] https://encyklopedia.pwn.pl/haslo/3905881/globalizacja.html%20target= [dostęp 29.11.2021 r.].

zacją wiążą się liczne korzyści, m.in. wzrost jakości usług i produktów, wzrost gospodarczy, zanikanie barier we współpracy międzynarodowej, łatwiejszy dostęp do różnych kultur. W kwestii zagrożeń mogą to być: nasilenie się migracji ludności, utrata suwerenności państwowych czy konflikty związane ze zmniejszaniem się zasobów energetycznych (surowcowych).

W roku 1962 M. MacLuhan[93] scharakteryzował termin *„globalnej wioski"*. Według niego jest to świat, w którym rozwój w dziedzinie komunikacji elektronicznej nie ma jakichkolwiek ograniczeń czasowych i dostępu do informacji. W wieku XX głos ten był dość kontrowersyjnym, jednak z biegiem lat uzyskał aprobatę. Poprzez Internet pokonywać można wszelkie granice[94].

Globalną wioskę porównać można do społeczeństwa informacyjnego, które warunkowane jest współczesnymi rozwiązaniami technicznymi. Wszelkie połączenie internetowe, sieciowe czy telefonicznie jakoby oplatają ziemię dookoła, co sprawia, że świat w pewnym sensie się zmniejszył. Nie ma już bariery czasu czy przestrzeni, co pozwala na szybszy i sprawniejszy kontakt, jak w *„małej wiosce"*.

Wyróżnia się cztery zasadnicze rodzaje społeczeństw. Pierwsze to społeczeństwo pierwotne (tradycyjne), które rozwijało się przed powstaniem państwa w dzisiejszym rozumieniu (wskazują na to źródła archeologiczne). Podstawą takiej komórki były małe grupy plemienne, zaś cechy charakterystyczne to: łowiectwo, rybołówstwo, zbieractwo. Takie formy nadal występują w Afryce, Nowej Gwinei oraz dżungli brazylijskiej (0,001% światowej populacji). Drugie – przemysłowe, mające u źródła motywacji działań gospodarczych – dążenie do zysku. Wyznacznikiem miejsca człowieka w społeczeństwie staje się pieniądz. Charakterystyczne dla kolejnego rodzaju, społeczeństwa poprzemysłowego jest przemieszczenie aktywności gospodarczej (większości) ze sfery produkcyjnej dóbr materialnych do sfery usługowej. W końcu, społeczeństwo informacyjne stanowiące o zależności produkcji towarów i realizowaniu usług poprzez przekazywanie odpowiedniej informacji. Rozwój technik i technologii telekomunikacyjnych oraz szybkie komputery umożliwiają wytwarzanie i przetwarzanie ogromnych ilości informacji. Informacja natomiast uznawana jest za najcenniejszy zasób we wszystkich dziedzinach i obszarach życia[95].

[93] Teoretyk komunikacji, urodzony w Kanadzie.
[94] https://eskamedia.pl/2020/05/04/swiat-to-globalna-wioska/ [dostęp 20.11.2021 r.].
[95] M. Szyłkowska, 2020, *wykład z przedmiotu: Wybrane problemy społeczeństwa informacyjnego*- materiał w zbiorach autora, WAT, Warszawa.

Potwierdzenie powyższych twierdzeń znaleźć można w artykule S. Gwoździewicz i M. Cieślikowskiej, które podkreślają znaczenie informacji: „*Informacja oraz wiedza stają się produktem przeznaczonym na sprzedaż, a jej rosnąca wartość jest siłą napędową rozwoju cywilizacji"*[96].

Pojęcie informacji jest trudne do jednoznacznego określenia: *„Próbom zdefiniowania informacji zawsze towarzyszy niedookreśloność, uzupełniona akcentem ważnej dla konretnej dziedziny wiedzy"* (J. Jackowski). Uogólniając można założyć, iż informacja jest wynikiem uporządkowanych danych (surowych, niepoddanych analizie liczb oraz faktów dotyczących wydarzeń czy zjawisk)[97]. Informacja nie jest wynikiem oceny, jest to *„suchy"* fakt i stanowi nowość dla odbiorcy.

Najprawdopodobniej po raz pierwszy określenia *„społeczeństwo informacyjne"* użył w roku 1963 Japończyk Umesao Tadeo, który opisał je jako społeczność komunikującą się przy użyciu komputerów. Inni podają, iż historia tego typu społeczeństwa rozpoczęła się w roku 1979, wówczas to Akademia Nauk Stanów Zjednoczonych w swoim raporcie zasygnalizowała nadejście całkowicie nowej ery informacyjnej, opartej na rozwoju technik cyfrowych[98].

Społeczeństwo informacyjne nasycone jest wieloma cechami tradycyjnych typów społeczeństw, ma jednak również wiele nowych, własnych. Można więc wyróżnić następujące czynniki[99]:

- znaczenie wiedzy teoretycznej wzrosło w obszarze znaczenia innowacji w różnych sektorach życia;
- technologie intelektualne przybierają na znaczeniu, bazy danych są pomocne w podejmowaniu decyzji politycznych, gospodarczych czy społecznych;
- szybkie, natychmiastowe przekazywanie informacji powoduje zanik związku między odległością a czasem powstania kontaktu;
- cyfrowy obieg informacji determinuje życie społeczne, gospodarcze, a nawet polityczne i kulturowe;

---

[96] S. Gwoździewicz, M. Cieślikowska, 2020, *Determinants of Social Development. About the Power of Expansion of (New) Technologies*. International Journal of New Economics And Social Sciences (IJONESS), p.120.

[97] Ibidem.

[98] M. Wilk, 2000, *Państwo w dobie społeczeństwa informacyjnego – perspektywa strategicznych zmian,* [w:] *Internet 2000. Prawo – ekonomia – kultura*, R. Skubisz (red.), Wydawnictwo Oficyna Wydawnicza Verba, Lublin, s. 194.

[99] http://repozytorium.amu.edu.pl:8080/bitstream/10593/5615/1/19_Marian_Golka_Czym%20jest%20spo%C5%82ecze%C5%84stwo%20informacyjne_253-265.pdf [dostęp 20.11.2021 r.].

- informacyjne technologie cyfrowe przenikają do niemal wszystkich dziedzin życia (życie codzienne, nauka, sztuka, gospodarka itp.) i uzależniają bezpowrotnie ich funkcjonowanie od komputerów;
- zacierają się granice między sferą prywatną i publiczną powodowane przez trudności w określeniu, co jest prywatne, co publiczne;
- zmiany w komunikacji między ludźmi wpływają na zmiany w tworzeniu i funkcjonowaniu więzi społecznych;
- zmieniające się urządzenia cyfrowe wprowadzają konieczność nieustannego dokształcania się w zakresie ich obsługi;
- różnorodność źródeł informacji i kwestie ograniczeń bezwładności informacji (informacja raz dostarczona do sieci jest natychmiast dostępna dla każdego użytkownika) powoduje częstokroć sytuacje nieporozumień;
- obecność zniekształconych informacji bądź wręcz manipulowanych sprawia problemy w weryfikacji prawdziwości i rzetelności informacji; podobnie w przypadku nadmiaru informacji i nieumiejętności ich selekcji, krytycznego podejścia.

Internet spowodował masowe wprowadzenie w rzeczywistość sieci telekomunikacyjnych tzw. *„ideał darmowości”*. Od początku bowiem stanowił przestrzeń otwartą, wolną dla każdego jak i darmową. Internet przyniósł więc pojęcie otwartości *(„openness”)* – każda osoba może mieć nieograniczony dostęp do treści, informacji czy aplikacji obecnych w sieci, z czasem również możliwa była ich modyfikacja. Stworzony na potrzeby militarne, Internet stał się narzędziem pomocnym w realizacji badań naukowych. Badacze najczęściej dzielili się swoimi pracami w środowiskach naukowych całego świata, nieskrępowany zaś przepływ informacji to zasada fundamentalna. Zwyczajne więc stało się komunikowanie poprzez konferencje czy specjalistyczne publikacje. Celem było szerokie rozpowszechnienie stworzonych prac i związane z tym budowanie własnego portfolio i reputacji. O ile Internet nie ma już czysto akademickiego charakteru, to nadal pozostaje żywa idea współpracy, dwustronnej wymiany wiedzy oraz zasobów. W taki oto sposób każdy użytkownik może zyskać dostęp do nieograniczonej ilości treści dostarczanej każdego dnia przez innych użytkowników, dorzucając tym samym własną twórczość i powiększając istniejącą już bazę[100]. Ponadto, coraz więcej szkół wyższych oferuje kształcenie online, tzw. kształcenie na odległość bez wymogu uczestnictwa stacjonarnego. Z pewnością dla wielu osób stanowi to niespotykaną

[100] D. Lombard, *Globalna wioska…,* op. cit., s. 133-135.

wcześniej możliwość poszerzenia swojej wiedzy bez utraty częstokroć czasu, pieniędzy na dojazdy i innych.

Procesy i wydarzenia zachodzące na całym świecie mają coraz większy wpływ na życie każdego obywatela. Rozwój systemów komunikacji sprawił zwiększenie tempa rozpowszechniania informacji praktycznie na całym świecie. Życie jest więc ze sobą powiązane. Użytkownicy działają w sieci wzajemności, która powoduje wielostronne interakcje. Cokolwiek dotyka kogoś innego bezpośrednio, wpływa pośrednio na nas samych. Zapewne na co dzień nikt nie zastanawia się, iż każdy z nas korzysta z dorobku wielu kultur i narodów. A tak właśnie dzieje się całkiem naturalnie. Czyni to ze świata wspólną globalną wioskę z niezliczoną ilością połączeń. Inną kwestią jest jej bezpieczeństwo. Bezpieczeństwo, do którego dążyć powinien każdy naród i każde państwo, chcące rozwijać swoje umiejętności w sposób zrównoważony i niezakłócony.

Zdaniem autora *„bezpieczna, globalna wioska"* to przestrzeń świata oparta na elektronicznym przekazie informacji, w której następuje stopniowa uniformizacja społeczeństw z zachowaniem dążenia do niezachwianego rozwoju. Rozwoju, który nie jest ograniczany przez np. ataki hakerskie dzięki właśnie odpowiednim zabezpieczeniom. Przykładem takiej uniformizacji jest bez wątpienia obecność języka angielskiego, który to staje się coraz bardziej dominującym językiem na świecie. Obecność w mass-mediach, informatyce, polityce, kulturze czy transporcie ułatwia międzynarodowy przekaz i jasność komunikacji. Oczywiście tak silna obecność obcego języka może powodować trudności dla osób starszych, które prawdopodobnie czuć będą się nieco wyobcowane nie znając nowego języka.

2.4. Wnioski

Obszerny zakres definicji cyberprzestrzeni w krajowych - polskich dokumentach strategicznych, stwarza pewne nieścisłości i niejasności prawno-instytucjonalne. Te uchybienia powodować mogą powstawanie zagrożeń tak dla państwa, jak i społeczeństwa, w sferze militarnej i cywilnej. Tak samo w przypadku sektora teleinformatycznego, bankowego czy infrastruktury krytycznej[101].

Cyberprzestrzeń nie jest jedynie sumą składników fizycznych tj. oprogramowania, sieci, systemów. Nie należy zapominać o zagadnieniu społecznym, które jest zna-

[101] A. Waloch, 2019*, Annales Universitatis Paedagogicae Cracoviensis*, https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/11/11.pdf [dostęp 01.09.2021 r.].

czącym elementem cyberprzestrzeni. Internet objętościowo stanowi najbardziej istotny składnik cyberprzestrzeni, ale z pewnością nie jest jej całością. Sens cyberprzestrzeni oddaje nowy wymiar ludzkich działań, który nie jest możliwy do schematycznego opisania[102]. Jakikolwiek ruch w cyberprzestrzeni ma swoje źródło w działaniu człowieka i wytworze jego zamiaru.

Z pewnością precyzyjne określenie cyberprzestrzeni stanowi rzeczywiście ogromne wyzwanie. Opierając się na oficjalnych dokumentach należy przyjąć, iż jest to przestrzeń tworzona przez urządzenia i programy informatyczne, które komunikują się między sobą i użytkownikami.

Rozwiązanie autorskie definicji cyberprzestrzeni - wirtualna przestrzeń organizowania informacji, której podstawę stanowią systemy teleinformatyczne oraz ich wzajemnie na siebie oddziałujący - użytkownicy.

Podobnie, brak wspólnych, zharmonizowanych definicji dotyczących cyberbezpieczeństwa w różnych krajach może być przyczyną nieporozumień między narodami podczas omawiania międzynarodowych podejść do globalnych zagrożeń cyberprzestrzeni.

Jak wiele sytuacji, zdarzeń, problemów czy procesów, tak globalizacja ma swoje pozytywne i negatywne skutki. Bez wątpienia postęp techniczny ułatwia życie, czyni je przyjemniejszym w egzystencji. Sprawia jednak również, że pojawiają się coraz to nowe zagrożenia, przyzwyczajenia czy choroby cywilizacyjne np. uzależnienie od sieci, wyobcowanie lub erotomania internetowa.

P. Bosmans stwierdza, iż postęp naukowo-techniczny i duchowy rozwój człowieka całkowicie się rozminęły. Ludzie zajęli się swoim materialnym postępem i stali się ofiarami własnej twórczości, zostali zaprogramowani, zmanipulowani i wręcz zdegenerowani[103]. Faktem jest, iż to człowiek tworzył i stale tworzy globalny świat, jest za niego odpowiedzialny i powinien ponosić wszelkie jego konsekwencje. Powstaje pytanie co dalej, w którym kierunku proces globalizacji będzie zmierzał? Czy globalna wioska stanie się bezpieczniejsza, czy wręcz przeciwnie?

Niektórzy badacze używają już określenia *homo informaticus*, jako nowego typu człowieka funkcjonującego w społeczeństwie informacyjnym (czy też społeczności wirtualnej). Podkreślają jego przesadną świadomość znaczenia i skutków obiegu informa-

[102] J. Wasilewski, *Zarys definicyjny…,* op. cit., s. 231-232.
[103] C. Banach, 2002, *Człowiek wobec wyzwań globalizacji i transformacji ustrojowej w Polsce,* [w:] *Pedagogika wobec zagrożeń, kryzysów i nadziei*, T. Borowska (red.), Wydawnictwo Oficyna Wydawnicza Impuls, Kraków, s. 16-18.

cji, również w życiu codziennym. W kontekście całego systemu cyberbezpieczeństwa oprócz warstwy technicznej czy podmiotowej, szczególne znaczenie odgrywa warstwa społeczna, czyli pojedynczy użytkownik, który de facto również stanowi część systemu. To bowiem on, jako element globalnej cyfrowej wioski, może wpływać na całokształt systemu, zarówno pozytywnie, ale i negatywnie (np. będąc cybertetrrorystą).

3. Dokumenty strategiczne i regulacje prawne w obszarze cyberbezpieczeństwa

3.1. Krajowe i międzynarodowe dokumenty strategiczne

Celem kolejnego podrozdziału jest określenie istotnych dokumentów strategicznych, które wyznaczały pewne początkowe kierunki w rozwoju cyberbezpieczeństwa. Nawiązanie do historycznych już momentów jest szczególnie ważne w zakresie wskazania sposobów kształtowania się określonych cech i podejść do opisywanego obszaru. Ponadto, zawarto analizę najnowszych, obowiązujących regulacji.

Mimo, że *Polityka Ochrony Cyberprzestrzeni RP z 2013 roku*[104] została już wyparta przez nowsze opracowanie (w 2017 roku opracowano *Krajowe Ramy Polityki Cyberbezpieczeństwa RP*[105]), to podanie jej założeń jest istotne ze względu na opisywaną tematykę oraz ze względu na aktualność podjętych w niej zagadnień. Cele szczegółowe polityki zostały ujęte w następujący sposób:

- zwiększenie poziomu bezpieczeństwa teleinformatycznej infrastruktury państwa;
- zwiększenie zdolności zapobiegania oraz zwalczania zagrożeń w cyberprzestrzeni;
- zmniejszenie skutków i skali oddziaływania incydentów;
- wskazanie kompetencji podmiotów zaangażowanych w bezpieczeństwo cyberprzestrzeni;
- utworzenie i realizacji spójnego systemu zarządzania bezpieczeństwem cyberprzestrzeni i ustanowienie wytycznych dla podmiotów niepublicznych;
- stworzenie trwałego i silnego systemu koordynacji i wymiany informacji między podmiotami oraz użytkownikami;
- zwiększenie świadomości użytkowników cyberprzestrzeni w obszarze środków i metod bezpieczeństwa w cyberprzestrzeni[106].

Wzmianki dotyczące budowania świadomości w zakresie cyberbezpieczeństwa znajdują się w podrozdziale 3.5 zatytułowanym *„Założenia dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa”*, uwagę przykuwa kampania społeczna o charakterze prewencyjno-edukacyjnym. Skierowana w szczególności do dzieci i młodzieży, którzy jako grupy młodych osób są najbardziej podatne na wpływy. Edukacja winna zaczynać się już od najmłodszych lat, tak by właściwie ukształtować nawyki chroniące przez zagrożeniami sieci (np. przed *cyberbullyingiem*, czyli nękaniem

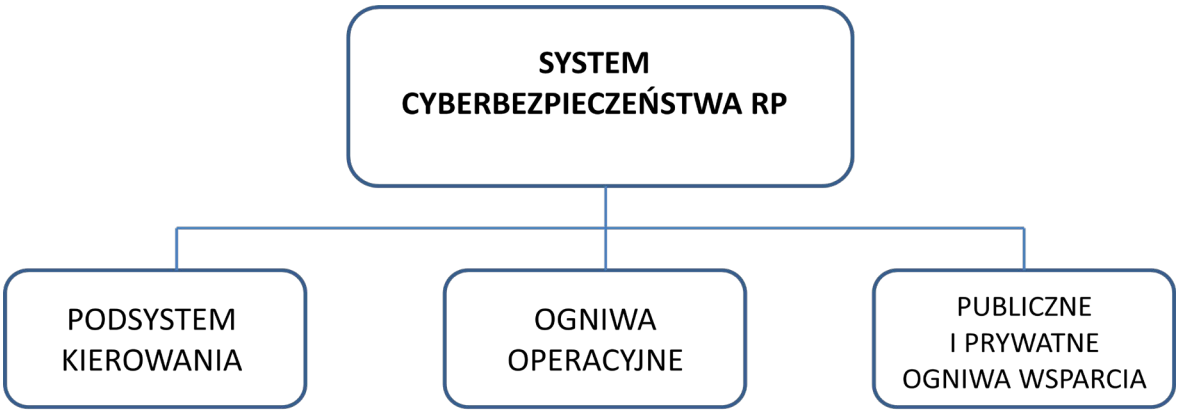
[104] Zob. Polityka Ochrony Cyberprzestrzeni RP, Warszawa 2013 (M.P. 2013 poz. 111 z późn. zm.).
[105] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017, s. 15.
[106] Ibidem.

w sieci, poznawaniem przypadkowych osób, piractwem czy uzależnieniem od Internetu). Wiedzę na tematy związane z cyberzagrożeniami dziecko powinno zdobywać przede wszystkim w szkole na wszystkich poziomach edukacji. Kolejnym odbiorcą tejże kampanii powinni być rodzice, jako odpowiedzialni za wychowanie następnych pokoleń. To na nich spoczywa ogromny obowiązek za przygotowanie dzieci do funkcjonowania w społeczeństwie informacyjnym. W zakresie nauczycieli, ich standard kształcenia opiera się na podstawowej wiedzy z technologii informacyjnej, w tym świadomego i bezpiecznego korzystania z sieci i systemów teleinformatycznych[107].

Polityka Ochrony Cyberprzestrzeni RP jest pierwszym dokumentem strategicznym w zakresie cyberbezpieczeństwa w Polsce. Już w 2013 r. za jeden z celów szczegółowych uznano budowanie świadomości użytkowników, co było już wówczas bardzo dobrym krokiem ku budowaniu efektywnego systemu cyberbezpieczeństwa. Powszechność korzystania z systemów dołączonych do sieci i zwiększające się znaczenie usług cyfrowych wymusiło konieczność podnoszenia świadomości obywateli, a także uwrażliwienia ich na pojawiające się cyberzagrożenia.

Doktryna Cyberbezpieczeństwa z 2015 r. jako strategiczny cel określa zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni. Cel strategiczny osiągnąć można poprzez realizację zadań prowadzących do wypełnienia celów o charakterze operacyjnym oraz preparacyjnym. Do celów operacyjnych zaliczono: ocenę warunków cyberbezpieczeństwa – rozpoznawanie zagrożeń, szacowanie ryzyka i identyfikację szans; przeciwdziałanie zagrożeniom, wykorzystywanie szans i redukowanie ryzyka; obronę i ochronę własnych systemów i zasobów; zwalczanie źródeł zagrożeń poprzez aktywną obronę i działania ofensywne; po ewentualnym zdarzeniu bądź ataku – odtwarzanie funkcjonalności i sprawności systemów cyberprzestrzeni. Tak, by osiągnąć cele operacyjne, należy w wymiarze preparacyjnym zbudować, utrzymywać i stale doskonalić zintegrowany system cyberbezpieczeństwa, obejmujący elementy jak na poniższym rysunku.

[107] Ibidem.



Rys. 3.1. System cyberbezpieczeństwa RP wg koncepcji historycznej z roku 2015
(źródło: opracowanie własne na podstawie: Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s. 9)

Podsystem kierowania zdolny do organizacji i koordynacji działań podmiotów rządowych oraz pozarządowych, które realizują zadania w zakresie cyberbezpieczeństwa. Podsystemy operacyjne i wsparcia – zdolne do przeprowadzania działań defensywnych (tj. obronnych i ochronnych), a także ofensywnych operacji cyber i udzielania wsparcia w ramach sojuszniczych działań.

Doktryna ta wskazuje zadania sektora publicznego m.in. działania informacyjne i edukacyjne ukierunkowane na społeczeństwo w zakresie bezpiecznego korzystania z cyberprzestrzeni i informowanie o zagrożeniach. Spośród zadań obywatelskich wyróżnia się:

- pomoc państwu w zapewnieniu bezpieczeństwa poprzez dbałość o użytkowane systemu i urządzenia informatyczne;
- samokształcenie w zakresie cyberbezpieczeństwa;
- monitorowanie zmian prawnych i organizacyjnych i składanie propozycji zmian w celu ochrony praw człowieka (w tym także prawa do prywatności w sieci);
- udział w inicjatywach społecznych wzmacniających cyberbezpieczeństwo (np. wolontariat dla cyberbezpieczeństwa).

„Dla przygotowania i realizowania efektywnego systemu cyberbezpieczeństwa istotne będzie opracowanie systemowych podstaw wykorzystania potencjału obywateli. Ważne jest prowadzenie czynności informacyjnych i edukacyjnych o charakterze profilaktycznym - zapobiegawczym w zakresie przygotowania obywateli do ich ochrony (również samoochrony) przed zagrożeniami w cyberprzestrzeni. Należy

uznać użytkowników indywidualnych, ich umiejętności i także świadomość bezpieczeństwa, za jeden z filarów cyberbezpieczeństwa państwa"[108].

Równie istotnym dokumentem jest *Strategia Bezpieczeństwa Narodowego z 2020 r.*[109]. Wyróżnia kilka filarów bezpieczeństwa i wartości państwa. Filar I Bezpieczeństwo państwa i obywateli; Filar II Polska w systemie bezpieczeństwa międzynarodowego; Filar III Tożsamość i dziedzictwo narodowe; Filar IV Rozwój społeczny i gospodarczy, ochrona środowiska. W ramach filaru pierwszego uwagę zwrócono na cyberbezpieczeństwo. Wskazano na podniesienie i wzmocnienie ochrony jak i odporności na cyberzagrożenia. Zwiększenie poziomu ochrony informacji w sektorach: publicznym, prywatnym, militarnym. Podkreślono promowanie wiedzy i dobrych praktyk umożliwiających użytkownikom lepszą ochronę ich informacji, ponadto rozwój prac badawczo-rozwojowych ukierunkowanych na m. in. Internet Rzeczy, szerokopasmową sieć łączności mobilnej i stacjonarnej, czyli 5G i wyższych oraz współpracę z uczelniami i instytucjami naukowymi. Strategia wyznacza kierunek rozwoju kompetencji, wiedzy i świadomości zagrożeń jak i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w zakresie cyberbezpieczeństwa[110]. Nie zabrakło miejsca na wpis dotyczący uzyskania zdolności do prowadzenia działań militarnych w cyberprzestrzeni, co obecnie bardzo mocno nabiera na znaczeniu.

W *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022* za nadrzędny cel ujęto zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, prywatnego oraz obywateli w obszarze świadczenia lub korzystania z usług cyfrowych oraz usług kluczowych. Kwestia stworzenia warunków do bezpiecznego korzystania z cyberprzestrzeni przez wszystkich obywateli wybrzmiała równie mocno jak cel nadrzędny.

Realizację postanowień ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r.[111] stanowi *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, która wskazuje najważniejsze zadania: uzyskanie wysokiego poziomu cyberbezpieczeństwa – głównie odporności systemów informacyjnych, operatorów infrastruktury krytycznej, operatorów usług kluczowych, dostawców usług cyfrowych. Strategia określa cele strategiczne i środki polityczne, regulacyjne, mające na celu zyskanie

[108] Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.
[109] Strategia Bezpieczeństwa Narodowego, Warszawa 2020, (M.P. 2020 poz. 413 z późn. zm.).
[110] Zob. Strategia Bezpieczeństwa Narodowego, Warszawa 2020, (M.P. 2020 poz. 413 z późn. zm.).
[111] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.
(Dz.U. 2018 poz. 1560 z późn. zm.).

i utrzymywanie wysokiego poziomu cyberbezpieczeństwa. Obejmuje sektory usług kluczowych, cyfrowych oraz podmioty publiczne. W dokumencie tym określa się w szczególności: priorytety i cele w zakresie cyber; podmioty zaangażowane w realizację Strategii; środki do realizacji wyznaczonych celów; środki w zakresie reagowania na przywracanie stanu cyberbezpieczeństwa; zasady współpracy w sektorach publicznym i prywatnym; ocenę ryzyka; programy szkoleniowe, informacyjne i edukacyjne, a także działania mające wpływ na plany badawczo-rozwojowe w zakresie cyberbezpieczeństwa. Strategia opracowywana i przeznaczana jest na pół dekady. Obowiązkowi przeglądu Strategii co dwa lata podlegają minister właściwy ds. informatyzacji i Pełnomocnik Rządu ds. Cyberbezpieczeństwa wraz z innymi ministrami i właściwymi kierownikami centralnych urzędów. Ponadto, niezmiennie zapewnienie warunków do bezpiecznego korzystania z cyberprzestrzeni dla obywateli. W związku z tym ostatnim celem, pojawił się poboczny, aczkolwiek niezwykle poważny: rozwijanie społecznej świadomości w kierunku bezpiecznego korzystania i poruszania się w cyberprzestrzeni[112].

Głównymi priorytetami w Strategii są:

- rozwój krajowego systemu cyberbezpieczeństwa;
- zwiększenie poziomu odporności systemów informacyjnych sektora prywatnego oraz administracji publicznej;
- osiągnięcie pełnej zdolności do zapobiegania i reagowania na incydenty;
- wzmocnienie potencjału narodowego w obszarze cyberbezpieczeństwa;
- budowanie i kształtowanie świadomości i kompetencji społecznych w zakresie bezpieczeństwa w cyberprzestrzeni;
- zbudowanie trwałej i silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Jednym z celów szczegółowych Strategii jest wspomniane budowanie i kształtowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. Zakłada się, iż edukacja w cyberprzestrzeni powinna zaczynać się od jak najwcześniejszego etapu nauki dzieci i młodzieży, najlepiej przed wejściem w świat cyfrowy, w praktyce zapewne już na etapie edukacji wczesnoszkolnej. Zgodnie z zapisami, planowane jest wsparcie nauczycieli w realizacji podstawy programowej, a w szczególności w obszarach wymagających aktualnej wiedzy nt. bezpiecznego poruszania się w świecie nowych technologii. Podaje się ponadto realizację działań wspierających ciągły rozwój

[112] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Warszawa 2019 (M.P. 2019 poz. 1037 z późn. zm.).

kadry nauczycielskiej w obszarze nowych technologii, z jednoczesnym uwzględnieniem potrzeb danej szkoły czy placówki. Dokument ten podkreśla znaczenie rozwijania świadomości społecznej w kierunku cyberbezpieczeństwa (bezpiecznego i niezagrożonego korzystania z cyberprzestrzeni). Administracja publiczna zamierza wraz z organizacjami pozarządowymi, ośrodkami akademickimi i sektorem prywatnym, kontynuować działania uwrażliwiające społeczność na cyberzagrożenia i poszanowanie praw i wolności w świecie cyfrowym. Kampanie społeczne skierowane docelowo do różnych grup (seniorów, rodziców czy dzieci) to część tych przedsięwzięć. Strategia zwraca uwagę na coraz liczniej występujące zagrożenia mające na celu wywarcie określonego wpływu i działania ludzi. Twórcy są świadomi konsekwencji celowego wykorzystania narzędzi inżynierii społecznej do działań manipulacyjnych, stąd istnieje potrzeba systemowego podejścia do tego zagadnienia i rozwijania świadomości obywateli w obszarze weryfikacji autentyczności przyjmowanych informacji[113].

Dość bezpośrednio można opisać ogólny cel doktryny, gdyż powinna ona odpowiadać na pytanie – co należy wykonać? Zaś strategia – w jaki sposób to zrealizować? Biorąc pod uwagę powyższe informacje, można mieć obiekcje co do precyzyjności ujętych w ww. dokumentach informacji. Zdaniem autora istnieje zbyt mało szczegółowych danych i wytycznych, które miałyby powodować skuteczne zwiększanie świadomości cyfrowej użytkowników.

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 już nie obowiązują[114]. Dokument zastąpiono *Strategią Cyberbezpieczeństwa*[115]. Do celów nadrzędnych *Krajowych Ram […]* zaliczono stworzenie systemu ostrzegania użytkowników, systemu bieżącego zarządzania cyberprzestrzenią oraz dodatkowego systemu informacyjnego – jedynie dla obywateli.

Bardzo interesujące, ponieważ w zarówno *Strategii Cyberbezpieczeństwa RP na lata 2019-2024*, jak i *Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-2022* zawarto ten sam podrozdział w swojej treści, dotyczący stworzenia warunków do bezpiecznego korzystania przez obywateli z cyberprzestrzeni. Założenie jest niezmienne, edukacja w zakresie cyber powinna zaczynać się już podczas edukacji wczesnoszkolnej. Planowane są zmiany w podstawach programowych nauczania i w kształceniu podyplomowym. Co więcej, wskazuje się również na współpracę

[113] Ibidem.
[114] Krajowe Ramy Polityki Cyberbezpieczeństwa…, op. cit.
[115] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Warszawa 2019 (M.P. 2019 poz. 1037 z późn. zm.).

z ośrodkami akademickimi i organizacjami pozarządowymi. Informacja o kampaniach społecznych kierowanych do różnych grup odbiorców jest również taka sama, jednolita w obu regulacjach. Może nieco zastanawiać, iż katalog wytycznych ujęty w Strategii jest nie tyle co zbieżny, a wprost identyczny jak ten w *Krajowych Ramach […]*.

Warto przytoczyć część podrozdziału 5.8 z *Krajowych Ram […]* noszącego nazwę *Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń*. Kluczowe znaczenie ma stworzenie warunków bezpieczeństwa systemów teleinformatycznych, które zapewnić miałby dostęp do informacji o zagrożeniach i dzielenie się tymi informacjami z użytkownikami. Dokument zakładał stworzenie systemu bieżącego zarządzania bezpieczeństwem cyberprzestrzeni. System ten miałby umożliwiać zgłaszanie danych o podatnościach i zagrożeniach. Zgodnie z przeprowadzonymi analizami, do zainteresowanych stron kierowane byłyby ostrzeżenia na temat cyberzagrożeń. Ponadto, celem ochrony użytkowników przed skutkami zagrożeń planowano utworzyć dodatkowy system informacyjny – jedynie dla obywateli[116].

Na poziomie europejskim, pierwszym dokumentem strategicznym w zakresie cyberbezpieczeństwa jest *Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP))*[117]. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej wyznacza pięć priorytetowych kierunków działań, mających zwiększyć poziom cyberbezpieczeństwa wszystkich krajów członkowskich:

- osiągnięcie wymaganego poziomu odporności na zagrożenia cybernetyczne;
- znaczące ograniczenie cyberprzestępczości;
- opracowanie i wdrożenie polityki obronnej i rozbudowa zdolności cyberbezpieczeństwa wraz ze Wspólną Polityką Bezpieczeństwa i Obrony UE;
- stała rozbudowa zasobów technologicznych i przemysłowych w ramach bezpieczeństwa w cyberprzestrzeni;
- wdrożenie wspólnej i spójnej polityki międzynarodowej w zakresie cyberprzestrzeni dla państw UE i promowanie podstawowych wartości.

[116] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017, s. 15.
[117] Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP)), (Dz.U.UE C z dnia 9 marca 2016 r.) z późn. zm.).

Współpraca na arenie międzynarodowej ma na celu ujednolicanie założeń i postulatów, tak aby działania w zakresie cyberbezpieczeństwa były jak najbardziej skoordynowane i nie wymagały skomplikowanych uzgodnień. Wspólne działanie państw w ramach UE przyczynia się do powstania możliwości prowadzenia szkoleń na większą skalę, co jest bardziej korzystne aniżeli dla państw organizujących szkolenia w tzw. „pojedynkę". To wszystko sprzyja wymianie doświadczeń w kwestii tworzenia czy analizy istniejących już zabezpieczeń.

W grudniu 2020 roku Unia Europejska przyjęła *Strategię UE w zakresie cyberbezpieczeństwa na cyfrową dekadę*[118]. Szczególne znaczenie cyberbezpieczeństwa opisano już we wprowadzeniu, gdzie wskazano, że sfera ta jest obecna podczas codziennego życia, tj. wizyt w banku, lotu samolotem, korzystania z usług administracyjnych, pobytu w szpitalu. Cyberbezpieczeństwo stanowi o ogromnej roli w budowaniu cyfrowej, odpornej i ekologicznej Europy. Celem strategii jest ochrona globalnego Internetu, co związane jest z ulepszeniem i wykorzystaniem wszystkich narzędzi w zapewnianiu bezpieczeństwa i ochrony praw europejskich wszystkich ludzi.

Wskazane w strategii inicjatywy[119]:

- ogólnoeuropejska tarcza przed zagrożeniami cyber, złożona z centrów monitorowania bezpieczeństwa wykorzystujących sztuczną inteligencję i uczenie się maszyn celem wykrywania wczesnych sygnałów cyberataków i umożliwiających podjęcie działań przed szkodami;
- wspólna jednostka ds. cyberprzestrzeni, skupiająca wszystkie środowiska zajmujące się cyberbezpieczeństwem, aby świadomość na temat zagrożeń była coraz większa oraz aby umożliwić reagowanie- wspólnie na incydenty i zagrożenia;
- europejskie rozwiązania w ramach poprawy bezpieczeństwa internetu na świecie, w tym także publiczny unijny dostawca usługi rozpoznawania *DNS*;
- lepszy unijne narzędzia dla dyplomacji cyfrowej celem zapobiegania cyberatakom, powstrzymywania ich i reagowania na nie;
- rozporządzenie mające na celu wsparcie i zabezpieczenie internetu rzeczy zabezpieczonych;
- bliższa współpraca w zakresie cyberobrony, w szczególności poprzez przegląd ram polityki w ramach cyberobrony;

[118] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020JC0018 [dostęp 03.05.2024 r.].
[119] https://ec.europa.eu/commission/presscorner/detail/pl/QANDA_20_2392 [dostęp 03.05.2024 r.].

- bardziej intensywne dialogi w kwestiach cyberprzestrzeni z państwami trzecimi i organizacjami regionalnymi oraz międzynarodowymi, w tym NATO;
- program działań w ramach Organizacji Narodów Zjednoczonych dotyczący bezpieczeństwa międzynarodowego w cyberprzestrzeni;
- program na rzecz zdolności cyfrowych UE i unijna międzyinstytucjonalna tzw. Rada ds. Budowania Zdolności Cyfrowych – celem zwiększenia skuteczności oraz wydajności budowania zdolności cyfrowych UE.

Podatność na działania hybrydowe ze strony Rosji – dezinformacje i cyberataki w najbliższym sąsiedztwie – ma negatywny wpływ na bezpieczeństwo wewnątrz UE. Tak więc Polska odegrać może aktywną rolę w procesie rozbudowy cyberodporności UE, wysuwając propozycje programów dla państw stowarzyszonych Bałkanów Zachodnich i Partnerstwa Wschodniego, a następnie implementując powyższe. Ważnym elementem będzie również podtrzymanie polskiego zaangażowania w rozwój projektu śledzenia i obserwacji przestrzeni kosmicznej, który zapewni bezpieczne, a także stabilne funkcjonowanie technologii, które wykorzystują dane satelitarne.

3.2. Wybrane regulacje prawne Unii Europejskiej i krajowe

W podrozdziale 3.2. zostaną przeanalizowane źródła prawa UE pod kątem *Dyrektywy NIS z 2016 r.*, *Rozporządzenia ENISA z 2019 r.*, *Dyrektywy NIS 2 z 2022 r.*, aktu o usługach cyfrowych z 2024 r. oraz regulacji państwowych. Celem tej części dysertacji będzie wskazanie kluczowych rozwiązań prawnych w obszarze cyberbezpieczeństwa i ich implikacji dla poszczególnych podmiotów.

Pierwsze europejskie prawo w zakresie cyberbezpieczeństwa stanowi wprowadzona w 2016 roku tzw. *Dyrektywa NIS (Network and Information Systems Directive)*[120]. Dokument ten nakłada na państwa członkowskie szereg obowiązków, obliguje je do stworzenia konkretnych instytucji i wprowadza określone mechanizmy współpracy. Pomysł dyrektywy zakładał stan faktyczny, iż kraje UE różnią się od siebie względem poziomu bezpieczeństwa sieci oraz systemów informatycznych, co przekłada się na ogólny poziom cyberbezpieczeństwa całej Unii.

Jednym z obowiązków państw członkowskich jest przyjęcie krajowej strategii cyberbezpieczeństwa, w której winny być zawarte strategiczne cele i właściwe środki

[120] 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.

polityczne (i regulacyjne) ukierunkowane na utrzymanie bądź podwyższenie obecnego poziomu bezpieczeństwa systemów informatycznych. Kolejnym zadaniem jest wyznaczenie organu lub kilku organów odpowiedzialnych za monitorowanie stosowania przepisów krajowych – wdrażających ten dokument we wskazanych sektorach. Jeśli państwo członkowskie wyznaczy więcej niż jeden organ właściwy, wówczas ma obowiązek ustanowienie Pojedynczego Punktu Kontaktowego (PPK). Jeśli natomiast organ właściwy jest tylko jeden, wówczas to on jednocześnie sprawuje funkcję PPK, którego przeznaczeniem jest m.in. zapewnienie transgranicznej współpracy organów krajów członkowskich i odpowiednich organów innych państw w ramach UE, a także z Grupą Współpracy i *CSIRT*. Najważniejsze zadanie PPK stanowi gromadzenie danych i informacji o incydentach na szczeblu krajowym, następnie ich wymiana z odpowiednikami z zagranicy[121].

Co więcej, każde państwo zobligowane jest do stworzenia jednego lub kilku Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego *(Computer Security Incident Response Team),* zwanych również Zespołami Reagowania na Zagrożenia Komputerowe *(Computer Emergency Response Team)*[122]. Oczywistym jest, że powyższe kategorie instytucji, tj. organ właściwy, PPK oraz *CSIRT,* jeżeli są oddzielne, mają obowiązek wymiany informacji i współpracy w zakresie obowiązków określonych dyrektywą.

Przedstawiciele państw członkowskich tworzą tzw. Grupę Współpracy. Cel jaki przyświecał jej tworzeniu to ulepszenie poziomu przepływu informacji, wzajemne wsparcie oraz wzmocnienie zaufania międzynarodowego. Do nadrzędnych zadań Grupy należą[123]:

- udzielanie wskazówek w obszarze działania *CSIRT*;
- wymiana tzw. *leassons learned* dotyczących zgłaszania incydentów;
- podnoszenie świadomości cyberzagrożeń i organizacja szkoleń wraz z rozwojem badań bezpieczeństwa sieci i systemów teleinformatycznych;
- identyfikowanie i wskazywanie operatorów usług kluczowych;

[121] C. Banasiński (red. nauk.), 2018, *Cyberbezpieczeństwo. Zarys wykładu,* Wydawnictwo Wolters Kluwer Polska, Warszawa, s. 155-156.
[122] Prawo europejskie używa terminu *CSIRT*, gdyż termin *CERT* zarejestrowany jest przez Centrum Koordynacji *CERT (CERT/CC)* w Stanach Zjednoczonych; niemniej jednak w Dyrektywie NIS skróty te stosowane są przemiennie. Pojawia się również *IRT (Incident Response Team)* lub *CIRT (Computer Incident Response Team).*
[123] 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, s. 18.

- wymiana pozostałych istotnych informacji w zakresie bezpieczeństwa sieci i systemów teleinformatycznych z właściwymi instytucjami i agencjami UE.

Na sieć krajowych *CSIRT* składają się przedstawiciele *CSIRT* państw członkowskich oraz *CERT-EU*. Komisja jest uczestnikiem sieci *CSIRT*, ale jedynie jako obserwator. Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji - *ENISA (European Network and Information Security Agency)* zapewnia sekretariat i stanowi wsparcie *CSIRTów* państw członkowskich. W katalog zadań zespołów właczono: wymianę i udostępnienie na zasadzie dobrowolności danych – informacji dotyczących operacji, usług, zdolności współpracy *CSIRT* i poszczególnych incydentów. Tak więc *CSIRT* jest siecią nieformalną i państwo członkowskie może odmówić udziału w dyskusji w ramach danego incydentu, jeśli uzna to za ryzyko szkody. Nie jest możliwe zmuszenie członków do działania w inny, określony sposób. Bez wątpienia, konstruktywny i logiczny charakter dyskusji może pomóc przy rozwiązywaniu wielu problemów w obszarze bezpieczeństwa cybernetycznego.

Zakres podmiotowy *Dyrektywy NIS* obejmuje dostawców usług cyfrowych oraz operatorów usług kluczowych.

Za dostawcę usług cyfrowych uznaje się jakąkolwiek osobę prawną świadczącą usługę cyfrową – każdą usługę świadczoną z reguły na odległość, za wynagrodzeniem, drogą elektroniczną i z powodu indywidualnego żądania odbiorcy usługi. Usługa ta musi mieścić się w załączniku nr III *Dyrektywy NIS*, zgodnie z którym wyszczególniono internetowe platformy handlowe (zakupy online), wyszukiwarki internetowe i usługi chmury obliczeniowej. Przez internetową platformę handlową rozumie się usługę cyfrową umożliwiającą przedsiębiorcom lub konsumentom zawieranie umów online. Wyszukiwarka internetowa jest usługą cyfrową, która daje możliwość użytkownikowi wyszukiwanie jakichkolwiek stron internetowych w danym języku przy użyciu zapytania (słowo kluczowe), wyrażenie lub wskazanie innej wejściowej wartości. Ostatnią wskazaną usługą cyfrową jest usługa przetwarzania w chmurze, której atrybutem jest dostęp do elastycznego i skalowalnego zbioru zasobów obliczeniowych do wielopólnego zastosowania.

W kwestii operatora usług kluczowych – jest to podmiot prywatny lub publiczny, który należy do jednego z rodzajów sektorów (wskazanych w załączniku II ustawy), czyli energii, bankowości, transportu, służby zdrowia, infrastruktury usług finansowych, infrastruktury cyfrowej, zaopatrzenia w wodę pitną i jej dystrybuowania, podmiotów zarządzających i dokonujących rejestracji internetowych nazw domen, a także dostaw-

ców punktów wymiany ruchu internetowego. Podmiotom tym stawiane są określone kryteria, o czym na kolejnych stronach dysertacji[124].

Każde z sygnatariuszy *Dyrektywy NIS* są zobowiązane zidentyfikować operatorów usług kluczowych – na swoim terytorium, w sektorach ujętych w załączniku II. W sytuacji, gdy dany operator świadczy usługę kluczową nie tylko w jednym państwie, zaś w większej ilości państw członkowskich, wówczas decyzję o identyfikacji poprzedza się konsultacjami tych wybranych państw. Identyfikację tą oparto na trzech faktorach, które spełnione powinny być łącznie[125]:

- świadczenie przez wskazany podmiot usługi mającej kluczowe znaczenie dla utrzymywania krytycznej działalności gospodarczej bądź społecznej;
- od systemów informatycznych i sieci zależy świadczenie danej usługi;
- jakikolwiek incydent miałby znaczący skutek zakłócający świadczenie danej usługi.

Istotne dla dalszych rozważań jest zanalizowanie terminu incydent. Bowiem jak wskazano w dyrektywie, incydent zwykły to każde zdarzenie mające niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Rozróżnia się kilka rodzajów incydentów, w zależności od podmiotu zgłaszającego i stopnia ich oddziaływania. Incydent krytyczny skutkuje znaczną szkodą dla porządku publicznego, bezpieczeństwa lub działania instytucji publicznych, może wpływać na interesy gospodarcze państwa. Incydent poważny związany jest z przerwaniem ciągłości świadczenia kluczowej usługi lub znacznym obniżeniem jej jakości. Incydent istotny musi mieć istotny wpływ na świadczenie usługi cyfrowej. Jeszcze innym typem jest incydent w podmiocie publicznym, powodujący lub mogący spowodować obniżenie jakości albo przerwanie realizacji zadania publicznego. Co wpływa na ocenę, iż incydent jest rzeczywiście skutkiem zakłócającym[126]?

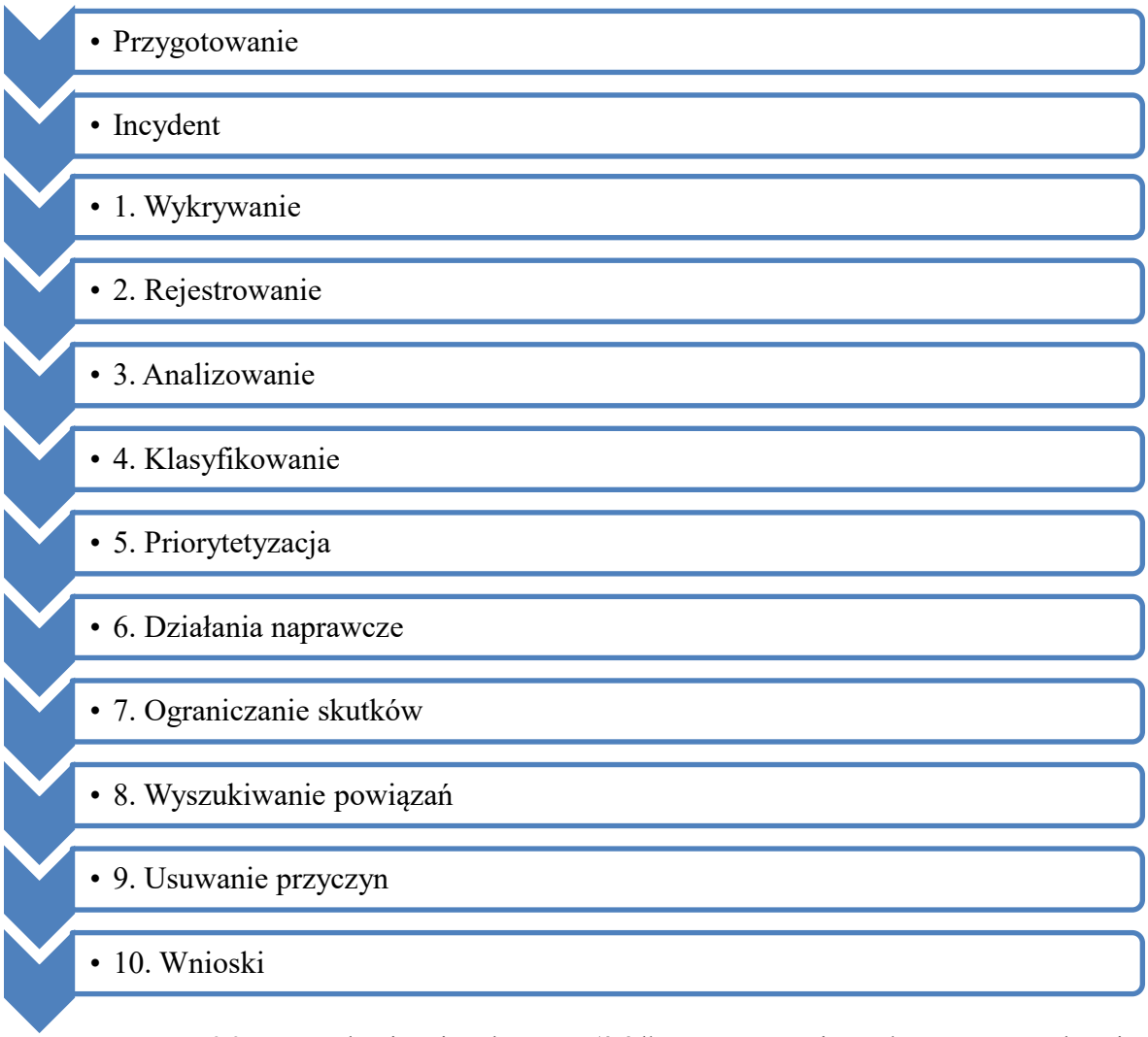
- liczba użytkowników zależnych od usługi świadczonej przez określony podmiot;
- uzależnienie pozostałych sektorów (załącznik II ustawy) od usługi świadczonej przez określony podmiot;
- poziom wpływu, jaki incydent biorąc pod uwagę skalę i czas trwania, mógłby mieć na bezpieczeństwo publiczne, działalność społeczną bądź gospodarczą;

[124] C. Banasiński (red. nauk.), 2018, *Cyberbezpieczeństwo…,* op. cit., s. 157.
[125] 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, s. 14-15.
[126] 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, s. 15.

- udział danego podmiotu w rynku;
- obszar i zasięg geograficzny, jakiego dotknąć mógłby incydent;
- znaczenie podmiotu w zapewnianiu wystarczającego poziomu usługi biorąc pod uwagę dostępność alternatywne sposoby świadczenia tej usługi.

Wymogi, którym sprostać muszą operatorzy podzielono na trzy zasadnicze kategorie: wymogi dotyczące szacowania ryzyka; wymogi dotyczące zgłaszania incydentów oraz pozostałe wymogi. W pierwszej grupie zawiera się m.in. stałe prowadzenie szacowania ryzyka wystąpienia incydentu, zbieranie informacji o zagrożeniach cyberbezpieczeństwa oraz stosowanie środków zapobiegających. Do drugiej grupy zaliczany jest obowiązek zarządzania incydentami i ich obsługę. Znacząca jest różnica między zarządzaniem incydentem – *incident management* i obsługą – *incident handling*. Obsługa incydentu jest pojęciem węższym, obejmującym działania przedstawione na poniższym rysunku (nr 1-7), zaś zarządzanie incydentem obejmuje oprócz wymienionych ponadto nr 8-10. Przygotowanie i planowanie to faza nieopisana jako element obsługi czy zarządzania. Jest wskazana jako etap niezbędny wg normy ISO/IEC/27035[127].

[127] ISO/IEC/27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principle of incident management.

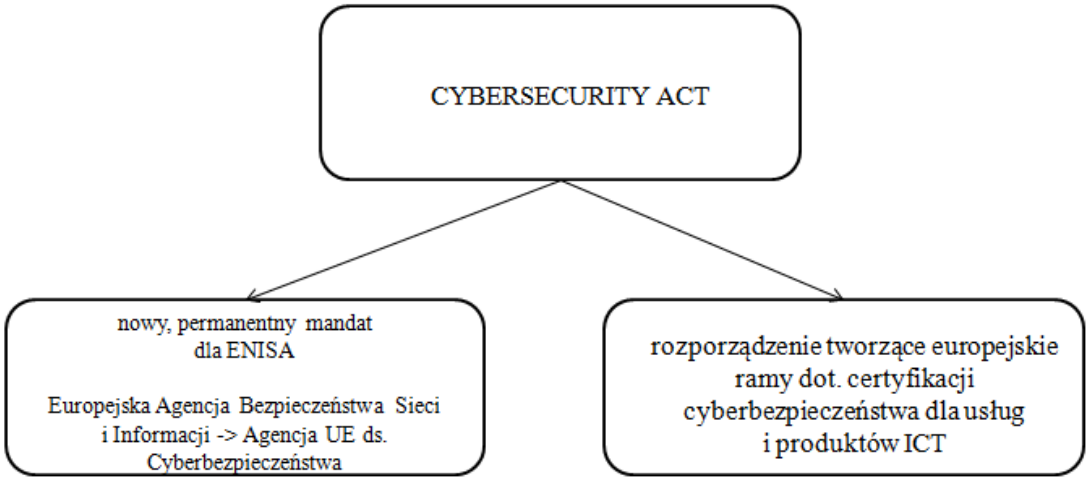


Rys. 3.2. Zarządzanie incydentem (źródło: opracowanie własne na podstawie: J. Dysarz, 2018, *Zarys działania krajowego systemu cyberbezpieczeństwa w Polsce*, [w:] *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni. Wymiar teoretyczny i praktyczny*, S. Topolewski (red.), Gdynia, s. 30)

Implementację zapisów i postanowień dyrektywy NIS, stanowi ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[128], która jest jednocześnie podstawą do rozważań dotyczących systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej, o czym w kolejnych podrozdziałach.

Od 27 czerwca 2019 r. obowiązuje *Cybersecurity Act*, co stanowi drugą regulację na poziomie europejskim w dziedzinie cyberbezpieczeństwa. *CA* składa się z dwóch części, co prezentuje poniższy rysunek.

[128] Zob. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560 z późn. zm.).



Rys. 3.3. Składowe *Cybersecurity ACT*[129] (źródło: opracowanie własne na podstawie: 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), art. 3, art. 8

Szczegółowy opis wzmocnienia *ENISA*, nie tylko poprzez permanentny mandat, ale również szereg nowych obowiązków znajduje się na końcu rozdziału. Natomiast, regulacja tworząca europejskie ramy certyfikacji to bardzo istotna regulacja, która zmieni w sposób znaczący obecny system certyfikacji, zdominowany przez *SOG-IS* (*Senior Official Group Information Security Systems)*.

W zakresie certyfikacji kilka najważniejszych zmian, jakie wprowadza *Cybersecurity Act*, przedstawia się następująco[130]:

- dobrowolna certyfikacja usług, procesów, produktów *ICT*;
- możliwość obowiązkowej certyfikacji dla konkretnych usług, procesów, produktów *ICT*;
- trzy poziomy bezpieczeństwa;
- obowiązek utworzenia przez państwa członkowskie krajowych organów ds. certyfikacji cyberbezpieczeństwa;
- powołanie Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa;
- wymóg zmian prawnych w Polsce (w szczególności w ustawie o krajowym systemie cyberbezpieczeństwa).

Akt o cyberbezpieczeństwie wskazuje trzy poziomy certyfikatów, tj. wysoki, istotny oraz podstawowy. Dzięki obranej metodologii np. przedsiębiorcy mogli będą łatwiej i szybciej dobrać certyfikat do indywidualnych potrzeb. W związku z tym, jeśli ocenią, iż do przeciwdziałania podstawowym zagrożeniem właściwy będzie poziom

[129] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R0881 [dostęp 03.11.2021 r.].
[130] https://cyberpolicy.nask.pl/akt-o-cyberbepzieczenstwie-certyfikacja-cyberbezpieczenstwa/ [dostęp 10.06.2021 r.].

najniższy, mają taką możliwość. Środkowy poziom pozwala na skuteczną ochroną przed atakami z ograniczonymi możliwościami. Najwyższy poziom ochrony wskazuje, iż produkt powinien być odporny na ataki sprawców o znaczących możliwościach i środkach (tak np. przed zorganizowanymi grupami dyponującymi ogromnymi funduszami)[131].

Przechodząc na polski grunt, pojawienie się cyberprzestrzeni wymusiło potrzeby zmian niektórych dokumentów, tak by stały się one kompatybilne i koherentne z innymi regulacjami.

Pierwszy, jakże znaczący zapis w zakresie bezpieczeństwa państwa (ściślej: bezpieczeństwa cyberprzestrzeni) ujęto w art. 228. Konstytucji RP, który stanowi: „*W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej"*[132].

Wdrożenie sfery cyber do stanów nadzwyczajnych ujęto w ustawie z dnia 30.08.2011 r. o zmianie ustawy o stanie wojennym […][133].

„W razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa"[134]. Przez zagrożenia zewnętrzne określa się działania godzące w niepodległość, niepodzielność terytorium państwa zmierzające do zakłócenia jego funkcjonowania, podejmowana przez podmioty zewnętrzne. Wydaje się, iż definicja ta może być zbyt mocno zawężona, co rodzi pewne wątpliwości. Warto zastanowić się, czy termin ten został „zarezerwowany" jedynie dla zagrożeń wojennych – pochodzących od obcego państwa? Zatem co w sytuacji wystąpienia działań terrorystycznych czy działań w cyberprzestrzeni? Czy niepaństwowy podmiot lub niezidentyfikowana jednostka byłaby podstawą do wprowadzenia stanu wojennego?

„W sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami

[131] https://www.gov.pl/web/cyfryzacja/akt-o-cyberbezpieczenstwie [dostęp 10.06.2021 r.].
[132] Konstytucja RP…, op. cit.
[133] Zob. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2002 nr 156 poz. 1301 z późn. zm.).
[134] Ibidem.

o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego"[135]. Co oznacza „bezpieczeństwo obywateli lub porządku publicznego"? W tym miejscu należy przytoczyć wyrok TK, w którym wskazano: „przesłanka ochrony porządku publicznego mieści w sobie postulat stanu faktycznego wewnątrz państwa, jaki pozwala na normalne współżycie jednostek w państwie. Podczas ograniczenia konkretnego prawa bądź wolności, ustawodawca kieruje się troską o harmonijne i należyte współżycie członków społeczeństwa, w czym zawiera się ochrona interesów poszczególnych osób oraz dóbr społecznych jak i mienia publicznego"[136]. Definicje bezpieczeństwa obywateli wskazują, że jest to stan niezagrożenia zdrowia i życia danej społeczności. Tak więc w kontekście stanu wyjątkowego, działania w cyberprzestrzeni powinny wywoływać pewne skutki, ponieważ same w sobie działania w cyberprzestrzeni prawdopodobnie nie byłyby podstawą do wprowadzenia tego stanu nadzwyczajnego. Reasumując, należy mieć na uwadze zasady stanów nadzwyczajnych[137].

Dzięki powyższym zapisom, kategoria cyberprzestrzeni dość szybko i sprawnie znalazła się w obiegu prawnym, nie pozwalając państwom NATO-wskim na ucieczkę w tym zakresie. Poprzez te działania struktury RP mogły przejść do kolejnych praktycznych czynności planistycznych i organizacyjnych. Konieczność podejścia jest wynikiem sieciowego charakteru środowiska bezpieczeństwa. Warto zauważyć, iż jest to sytuacja analogiczna do zagrożeń tworzonych przez siatki terrorystyczne np. atak na Stany Zjednoczone w dniu 11 września 2001 r. Atak uznano za atak zewnętrzny, wykonała go *Al.-Kaida*, mimo, że został wyprowadzony z terytorium USA i wykonany przy użyciu środków amerykańskich. Tak więc doprecyzowane rozumienie zewnętrzne (w przypadku ustawy o stanie wojennym) ma swoje logiczne, ale i praktyczne uzasadnienie.

[135] Ibidem.
[136] Wyrok Trybunału Konstytucyjnego z dnia 12 stycznia 1999 r., sygn. P. 2/98, (Dz. U. 1999, nr 3, poz. 30).
[137] M. E. Kołodziejczyk, 2021, *Wprowadzenie stanów nadzwyczajnych w Rzeczypospolitej Polskiej w przypadku działań w cyberprzestrzeni*, [w:] *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP,* K. Chałubińska-Jentkiewicz, A. Brzostek (red.), Warszawa, s. 233.

”Katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym”[138]. Takie ujęcie jest podstawą decyzji o ewentualnym wprowadzeniu stanu nadzwyczajnego do realnie możliwie istniejących przesłanek, ponadto jest to także impuls do przeglądu i aktualizacji planów kryzysowych czy planów operacyjnych z uwzględnieniem tych sytuacji warunkujących działania w cyberprzestrzeni[139].

Kolejna znowelizowana już ustawa stanowi, iż którykolwiek ze stanów nadzwyczajnych może zostać wprowadzony w związku z działaniami w cyberprzestrzeni.

O ile występuje już podstawa prawna, to występuje także wiele wątpliwości natury organizacyjno-prawnej odnośnie wprowadzania któregoś ze stanów. W szczególności, rozpatrując stan wojenny należy zdefiniować „zewnętrzny podmiot” (czy uwzględniona zostałaby grupa hakerska? Organizacja terrorystyczna?), „napaść” (na kogo? Na co?) oraz cel (działania godzące w niepodległość / niepodzielność RP). Może jeszcze bardziej istotny będzie skutek, zasięg i wymiar takiego działania. Wymienione elementy nie zostały uregulowane, stąd wprowadzenie stanów nadzwyczajnych w związku z działaniami w cyberprzestrzeni nie jest do końca aktem praktycznym[140]. Tak więc kwestia stanów nadzwyczajnych pozostaje nierozwiązana. Należałoby zastanowić się nad skróceniem całego procesu wprowadzania danego stanu nadzwyczajnego mając na uwadze jakże szybko zmieniające się warunki działań w cyberprzestrzeni. Ponadto, zasadnym byłoby nawiązanie do kategorii incydentów i wówczas uruchomienie któregoś ze stanów – np. w sytuacji wystąpienia incydentu krytycznego, poważnego czy istotnego.

Niezwykle dynamicznie zmieniające się środowisko cyberprzestrzeni wymusiło kolejne zmiany w regulacjach prawnych. W grudniu 2022 r. UE opublikowała nową dyrektywę na rzecz wysokiego wspólnego poziomu bezpieczeństwa cybernetycznego w Unii tzw. *Dyrektywa NIS 2*[141]. Weszła w życie w styczniu 2023 r. jednocześnie zastępując *Dyrektywę NIS* z 2016 r.

---

[138] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. 2002 nr 156 poz. 1301 z późn. zm.).

[139] https://www.bbn.gov.pl/pl/wolnytekst/3237,Cyberprzestrzen-w-ustawach-ostanach-nadzwyczajnych.html [dostęp 15.05.2022 r.].

[140] M. E. Kołodziejczyk, *Wprowadzenie…,* op. cit., s. 247-248.

[141] 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) 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2), art. 16.

Szczególnie w czasach po pandemii *COVID-19,* zwiększona zależność od infrastruktury cyfrowej spowodowała wzrost liczby ataków cybernetycznych na dużą skalę, przestojów i wycieków, co doprowadziło zarówno do szkód materialnych, jak i utraty reputacji, ale także do znacznych szkód gospodarczych i skutków społecznych, zaś trend ten został jeszcze bardziej przyspieszony na skutek wojny na Ukrainie. Ewoluujący krajobraz cyfrowy oraz nowe zagrożenia dla odpowiednich systemów wymagają zaktualizowanego, zmodyfikowanego systemu w celu poprawy odporności, integralności, poufności oraz dostępności. Proces przeglądu *Dyrektywy NIS 2016* ujawnił także rozbieżności w stosowaniu jej wymogów w państwach UE, co zwiększyło wymóg bardziej zharmonizowanej regulacji na europejskim poziomie[142].

Najistotniejsza różnica pomiędzy wcześniejszą *NIS*, a *NIS 2* sprowadza się do rozszerzenia zakresu zobowiązanych podmiotów i ich podziału na podmioty istotne oraz kluczowe. To nowy podział, który zastępuje dotychczasowy – na operatorów usług kluczowych i dostawców usług cyfrowych. Jako podmioty kluczowe, oprócz podmiotów z sektora bankowego, energetycznego, transportowego, zdrowotnego, czy finansowego, uznano m.in.: dostawców usług przetwarzania w chmurze – wcześniej należących do „niższej" kategorii dostawców usług cyfrowych: dostawców usług centrów danych – (nieistniejąca wcześniej kategoria), obejmującej w szczególności usługi scentralizowanego przetwarzania, przechowywania i transportu danych wraz z zapewnieniem wszelkich niezbędnych narzędzi (np. infrastruktury i obiektów), a także środków (np. dostaw energii); dostawców usług *CDN* (*content delivery network providers*) – również nowej kategorii usług, która polega na udostępnianiu sieci serwerów celem zapewnienia opcji dalszego udostępniania użytkownikom internetowych treści; dostawców publicznych sieci łączności elektronicznej i usług łączności elektronicznej; dostawców usług zaufania; jednostek administracji rządowej. Zatem widać wyraźne rozszerzenie zakresu podmiotów kluczowych porównując do katalogu operatorów usług kluczowych wg jeszcze pierwszej *Dyrektywy NIS*[143].

Z definicji *NIS 2* do podmiotów istotnych zalicza się m.in. dostawców wyszukiwarek internetowych, dostawców platform handlowych, dostawców serwisów społecznościowych i dostawców usług kurierskich – te dwa ostatnie to nowa grupa, wcześniej

[142] https://www.klgates.com/Happy-NIS-Year-Everyone-A-New-Common-Cybersecurity-Framework-for-the-European-Union-1-13-2023 [dostęp 11.02.2023 r.].
[143] https://kicb.pl/rada-ue-przyjela-nis-2/ [dostęp 11.02.2023 r.].

nie ujęta w dyrektywie. Oprócz wymienionych, kategoria podmiotów istotnych obejmuje także podmioty produkcji i dystrybucji chemikaliów, produkcji i dystrybucji żywności czy zarządzania odpadami. Zadaniem wskazanych podmiotów będzie przygotowanie i wdrożenie stosownych procedur w zakresie cyberbezpieczeństwa i zgłaszanie naruszeń, incydentów oraz cyberzagrożeń. Co szczególnie ważne, nowa dyrektywa nie pozostawia krajowym ustawodawcom możliwości zadecydowania, które podmioty uznać za istotne a które za kluczowe. Podział ten narzucono z góry i opisano w załącznikach *Dyrektywy NIS 2* oznacza bardziej rygorystyczne środki nadzorcze dla krajowych organów i bardziej rygorystyczne wymogi w zakresie kontroli i egzekwowania prawa. Odpowiedzialność za zapewnienie cyberbezpieczeństwa spoczywać będzie także na osobach, które zarządzają podmiotami zobowiązanymi przez dyrektywę[144].

Dyrektywa NIS 2 powołuje nowy europejski organ cyberbezpieczeństwa – *EU-CyCLONE* tj. europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa. Jej głównym zadaniem będzie koordynowanie zarządzania na szczeblu operacyjnym incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie w dużej skali, a także zapewnienie regularnej wymiany informacji pomiędzy państwami członkowskimi a organami, instytucjami, urzędami i agencjami Unii. W katalogu obowiązków ujęto m.in. rozwijanie świadomości sytuacyjnej w obszarze zarządzania incydentami; ocenę wpływu incydentów na dużą skalę i wspieranie procesu decyzyjnego na szczeblu politycznym[145]. Regulacja ta ustanawia również bardziej rygorystyczne zadania i obowiązki w zakresie bezpieczeństwa cybernetycznego dla państw UE w obszarze nadzoru. Poprawia ona ich egzekwowanie przez harmonizację sankcji w państwach UE. Zmierza również do poprawy współpracy między narodami, w tym w szczególności w przypadku incydentów na dużą skalę, pod patronatem europejskiej agencji cyberbezpieczeństwa, *ENISA*.

Od 16 lutego 2024 r. obowiązuje na terenie państw UE akt o usługach cyfrowych *(Digital Services Act)*[146]. Stanowi on zbiór ogólnounijnych przepisów w obszarze usług cyfrowych działających w linii pośrednik – konsument. Usługi cyfrowe obejmują usługi pośrednie takie jak dostawca usługi hostingowej, internetowa platforma handlowa czy sieć mediów społecznościowych. Cel *DSA* jest jasno określony: budowa bez-

[144] Ibidem.
[145] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555…, op. cit.
[146] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).

pieczniejszego i sprawiedliwego świata online. Przepisy mają chronić w równym stopniu użytkowników w UE, w zakresie nielegalnych usług, treści czy towarów oraz ich podstawowych praw[147].

Akt ma zastosowanie jak już wspomniano, do platform handlowych, social media, sklepów z aplikacjami, internetowych platform zakwaterowania oraz podróży. Mikro i małe przedsiębiorstwa zwolnione są z niektórych przepisów. Bardzo duże platformy internetowe oraz wyszukiwarki –*Very Large Online Platforms (VLOP), Very Large Online Search Engines (VLOS* - przeciętni użytkownicy sięgają lub przekraczają 10% ludności UE, czyli ok. 45 mln. użytkowników obarczone są dodatkowymi obowiązkami. Komisja dotychczas wyznaczyła następujące serwisy *VLOP* (m.in.): *Alibaba AliExpress, Sklep Amazon, Mapy Google, Facebook, Instagram, Pornhub, YouTube* czy Zalando. *VLOSE: Bing* oraz *Wyszukiwarka Google.* W zakres obowiązków platform i wyszukiwarek dopisano przeprowadzanie ocen ryzyka, zapewnienie łatwiejszego dostępu do odczytania wielojęzycznej wersji warunków, wdrażanie środków ograniczających ryzyko; budowa i aktualizowanie mechanizmu reagowania kryzysowego[148].

Zdaniem specjalistów jest to przełomowa zmiana, która pozwoli użytkownikom sieci być lepiej chronionymi przed treściami nielegalnymi, zaś ich prawa będą znacznie ściślej przestrzegane. Są także osoby wyrażające swoje obawy, iż akt ten może zostać wykorzystywany jako narzędzie do cenzurowania pod pretekstem przeciwdziałania tzw. mowie nienawiści w sieci.

DSA zapewnia[149]:

- łatwiejszy sposób zgłaszania nielegalnych treści, usług bądź towarów;
- silniejszę ochronę osób, które są ofiarami nękania w internecie;
- w zakresie reklamy – jej przejrzystość;
- zakazuje stosowania pewnych rodzajów reklamy ukierunkowanej, jak np. reklamy wykorzystujące dane małoletnich lub dane wrażliwe;
- bezpłatne mechanizmy reklamacyjne, łatwe w użyciu, jeśli platforma internetowa usunie treści danego podmiotu czy osoby;
- uproszczone warunki.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Ra-

[147] https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers [dostęp 24.02. 2024 r.].
[148] Ibidem.
[149] Ibidem.

dy 2005/222/WSiSW[150]. Celami dyrektywy są: zbliżenie prawa karnego państw członkowskich w zakresie ataków na systemy informatyczne, poprzez ustanowienie minimalnych zasad dotyczących definicji przestępstw oraz odpowiednich kar, a także poprawa współpracy między organami, w tym policją oraz innymi wyspecjalizowanymi organami ścigania, a także właściwymi wyspecjalizowanymi agencjami i organami UE takimi jak Eurojust, Europol i należące do niego Europejskie Centrum ds. Walki z Cyberprzestępczością, a także Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*ENISA*).

3.3. Podmioty i instytucje właściwe w obszarze budowania świadomości i kompetencji cyfrowych

Przedostatni podrozdział trzeciego rozdziału obejmuje analizę dotyczącą poszczególnych komórek odpowiedzialnych za kształtowanie kompetencji cyfrowych i cyberbezpieczeństwa. Opisane zostaną instytucje państwowe oraz międzynarodowe.

Coraz szersza dostępność oferowanych usług przez cyberprzestrzeń, a także powszechność i codzienność korzystania z nich przez obywateli, powoduje konieczność stałego podnoszenia świadomości użytkowników w kwestii bezpiecznego korzystania z sieci.

Zgodnie z powstałymi i wdrożonymi regulacjami prawnymi, powstały również dedykowane komórki w podmiotach i instytucjach odpowiedzialnych za ww. działania[151]. Jednostki te mają szczegółowe zadania i obowiązki wynikające z potrzeb zapewnienia cyberbezpieczeństwa swoim członkom.

Na początku stycznia 2022 roku odbyło się w Ministerstwie Edukacji i Nauki (od 1 stycznia 2024 MEiN uległo ponownie podziałowi na Ministerstwo Edukacji Narodowej oraz Ministerstwo Nauki i Szkolnictwa Wyższego), spotkanie robocze dotyczące utworzenia Narodowego Centrum Sztucznej Inteligencji i Cyberbezpieczeństwa. Wśród korzyści płynących ze stworzenia Centrum zaprezentowano: zbudowanie infrastruktury sztucznej inteligencji, w ramach której Polska mogłaby zostać liderem Europy Środkowo-Wschodniej. Ponadto, szczególną uwagę poświęcono kwestiom bezpieczeństwa danych (przetwarzania, przechowywania, transmisji), bezpieczeństwa

[150] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32013L0040 [dostęp 03.05.2024 r.].
[151] Zob. S. Gwoździewicz, K. Tomaszycki, 2017, *Prawne i społeczne aspekty cyberbezpieczeństwa*, Wydawnictwo Międzynarodowy Instytut Innowacji Nauka – Edukacja – Rozwój, Warszawa.

e-tożsamości i aplikacji służących całemu społeczeństwu[152]. Utworzenie takiego centrum to również okazja na wzrost konkurencyjności i rozwój polskiej nauki na arenie międzynarodowej i popularyzacja sztucznej inteligencji w obszarze zagadnień takich jak: bezpieczeństwo, medycyna, przemysł, usługi, handel czy inżynieria.

Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów – poradnik MEN[153]. To tytuł przygotowanego we wrześniu 2020 roku z inicjatywy ówczesnego MEiN poradnika dla dyrektorów szkół, nauczycieli, uczniów oraz rodziców. Kompendium zostało opracowane we współpracy z instytucjami odpowiedzialnymi za bezpieczeństwo, organizacjami pozarządowymi, Ministerstwem Cyfryzacji, Ministerstwem Spraw Wewnętrznych i Administracji, Ośrodkiem Rozwoju Edukacji oraz Naukową i Akademicką Siecią Komputerową.

Publikacja odpowiada na aktualne potrzeby szkół. Podzielona została na trzy części tj. bezpieczeństwo fizyczne, bezpieczeństwo cyfrowe oraz bezpieczeństwo techniczne sieci i sprzętu *IT*. Przydatny element stanowi słowniczek podstawowych pojęć. Co jest najbardziej interesujące, rozdział dotyczący bezpieczeństwa cyfrowego zawiera opis możliwych zagrożeń występujących w sieci, rekomendacje profilaktyczne jak i strategiczne oraz najważniejsze – działania interwencyjne szkoły. Autorzy nie zapomnieli również o przybliżeniu kwestii reagowania w przypadku występowania incydentu zagrożenia cyberbezpieczeństwa.

Innym projektem Ministerstwa Cyfryzacji oraz Ministerstwa Edukacji Narodowej jest oparty na mocy ustawy o Ogólnopolskiej Sieci Edukacyjnej[154] program - Ogólnopolska Sieć Edukacyjna. OSE to program publicznej sieci telekomunikacyjnej, który umożliwia szkołom dostęp do bezpłatnego, bezpiecznego i szybkiego Internetu. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy świadczy usługi operatora OSE. Bezpieczeństwo cyfrowe uczniów, nauczycieli oraz pracowników to stan nabyty, nie dany z góry. Aby go zapewnić, niezbędnych jest wiele powiązanych ze sobą działań organizacyjnych, wychowawczych, edukacyjnych i co niezwykle istotne – technicznych. OSE zapewnia niezbędne narzędzia cyfrowe i treści eduka-

152 https://www.gov.pl/web/edukacja-i-nauka/robocze-spotkanie-dotyczace-utworzenia-narodowego-centrum-sztucznej-inteligencji-i-cyberbezpieczenstwa-z-udzialem-ministra-edukacji-i-nauki [dostęp 06.03.2022 r.].

153 https://www.gov.pl/web/edukacja-i-nauka/bezpieczenstwo-fizyczne-i-cyfrowe-uczniow--poradnik-men [dostęp 06.03.2022 r.].

154 Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz.U. 2017, poz. 2184; 2019, poz. 1815; 2020, poz. 695 z późn. zm.).

cyjne. NASK natomiast, zajmuje się zapewnieniem usług bezpieczeństwa, mających na celu ochronę szerokopasmowego dostępu do Internetu przed złośliwym oprogramowaniem, monitoring zagrożeń i bezpieczeństwo sieciowe, a także przeciwdziałanie dostępowi do treści, mogących stanowić bezpośrednie zagrożenie dla rozwoju uczniów[155]. Co jest warte podkreślenia, nie ma złotego środka w przypadku wystąpienia incydentu bezpieczeństwa cyfrowego. Każdy przypadek powinien być rozpatrywany indywidualnie, przy uwzględnieniu szeregu czynników, takich jak np. zachowanie ucznia, jego aktywność naukowa, tło incydentu oraz możliwy wpływ na pozostałe dzieci czy całą społeczność szkolną.

Zgodnie z *zarządzeniem nr 69/MON Ministra Obrony Narodowej z dnia 20 września 2021 r. zmieniającym zarządzenie w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej*, utworzony został Departament Cyberbezpieczeństwa MON. Departament odpowiada za koordynację wykonywania ustawowych zadań Ministra ON w obszarze cyberbezpieczeństwa[156]. Dyrektor tej nowoutworzonej komórki organizacyjnej resortu pełni także funkcję Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni[157].

Do zadań Departamentu, w szczególności należą zagadnienia:

- tworzenia propozycji celów w obszarze cyberbezpieczeństwa w zakresie planowania rozwoju systemu bezpieczeństwa narodowego;
- projektowania przedmiotowych rozwiązań systemowych i opracowywanie aktów prawnych na szczeblu rządowym;
- koordynowania realizacji implementacji polityki międzynarodowej oraz krajowej, w tym rozwoju zdolności resortu do działań w cyberprzestrzeni i przedsięwzięć szkoleniowych obszaru cyberbezpieczeństwa;
- wykonywania innych zadań zleconych przez Ministra w obszarze cyberprzestrzeni;
- obsługi Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni i wsparcie Pełnomocnika Ministra Obrony Narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni[158].

Należy podkreślić rolę Naukowej i Akademickiej Sieci Komputerowej w kształtowaniu bezpieczeństwa cyberprzestrzeni i ochrony użytkowników. NASK jest pań-

[155] https://ose.gov.pl/ [dostęp 20.05.2022 r.].
[156] https://www.gov.pl/web/obrona-narodowa/departament-cyberbezpieczenstwa [dostęp 06.03.2022 r.].
[157] Decyzja Nr 151/MON z dnia 14 października 2021 r. zmieniająca decyzję w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.
[158] Zarządzenie Nr 69/MON z dnia 20 września 2021 r. zmieniające zarządzenie w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej.

stwowym instytutem badawczym, a jego pracę nadzoruje Kancelaria Prezesa Rady Ministrów. Kluczowe pole aktywności instytutu stanowią działania związane z zapewnieniem bezpieczeństwa sieci. Pion Centrum Cyberbezpieczeństwa zajmuje się reagowaniem na zdarzenia naruszające bezpieczeństwo Internetu, w jego skład wchodzi m.in. zespół *CERT Polska*[159], do którego obowiązków wpisano:

- obsługę i rejestrowanie zdarzeń naruszających bezpieczeństwo sieci;
- reagowanie w przypadku wystąpienia zagrożeń dla użytkowników;
- udział w krajowych oraz międzynarodowych projektach dotyczących bezpieczeństwa teleinformatycznego;
- współpracę z pozostałymi zespołami *CERT/CSIRT* w kraju i na świecie;
- rozwijanie swoich narzędzi do wykrywania, analizy i korelacji cyberzagrożeń;
- publikowanie Raportu *CERT Polska* w zakresie bezpieczeństwa Internetu;
- działania edukacyjno-informacyjne, których celem jest wzrost świadomości użytkowników, w tym publikowanie informacji w serwisach społecznościowych;
- organizowanie rokrocznie konferencji *SECURE* – bezpieczeństwo sieci;
- analizowanie i wykonywanie testów w dziedzinie bezpieczeństwa teleinformatycznego.

Jednym z zespołów NASK jest Dyżurnet.pl, czyli punkt kontaktowy do zgłaszania treści nielegalnych w sieci, w szczególności tych związanych z seksualnym wykorzystywaniem dzieci[160]. Eksperci wspierani doświadczeniem i wiedzą innych zespołów NASK i przejrzyste procedury działań, są gwarancją skutecznych interwencji i pełnego bezpieczeństwa użytkowników, zgłaszających naruszenia. Ponadto, przynależność do Stowarzyszenia *INHOPE* (*The Association of Internet Hotline Providers*) przyczynia się do przeciwdziałania dystrybucji treści o znaczeniu seksualnego wykorzystywania dzieci w skali globalnej. Misją tej komórki jest podejmowanie i realizacja działań na poczet kształtowania bezpiecznego Internetu. Dyżurnet.pl promuje również i popularyzuje wiedzę na temat bezpiecznego poruszania się w sieci; przygotowuje publikacje w sferze cyber; prowadzi kampanie i programy społeczne, które promują dobre praktyki; uczestniczy w projektach Safer Internet, Kursor, Plik, Folder oraz inne. Wraz z pozostałymi ekspertami NASK prowadzi konferencje, seminaria, szkolenia, zajęcia dla uczniów, nauczycieli, policji, a także przedstawicieli wymiaru sprawiedliwości[161]. Poprzez

[159] https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html [dostęp 06.03.2022 r.].
[160] https://dyzurnet.pl/ [dostęp 06.03.2022 r.].
[161] https://dyzurnet.pl/o-nas [dostęp 06.03.2022 r.].

wszystkie te działania NASK stanowi właściwy przykład instytutu badawczego, który w sposób rzetelny wypełnia swoje zadania, kształtując świadomość użytkowników i rozwijając ich kompetencje cyfrowe.

Elementem budowania świadomości użytkowników sieci są także przeprowadzane i umieszczane na stronie Dyżurnet.pl badania naukowe. Aby posłużyć się przykładem, jedno dotyczyło prezentacji treści seksualnych przez młodzież poprzez wideoczaty. Badanie dotyczyło pojawiania się w Internecie materiałów o charakterze erotycznym, z udziałem nieletnich, przede wszystkim w kontekście wideo-rozmów. Badanie przeprowadzono w dniach od 20 sierpnia do 16 września 2013 roku metodą *CAWI* (*Computer Assisted Web Interview*). Objęto nim grupę blisko tysiąca osób w wieku 13-16 lat, doważanej do reprezentatywnej grupy internautów w tym wieku. Połowa badanych nastolatków słyszała o zjawisku wykorzystania rozmów do prezentacji treści o zabarwieniu seksualnym, zaś prawie 20 % zetknęło się z tym zjawiskiem bezpośrednio. 8 % badanych zadeklarowało, że zetknęło się na wideoczacie z prezentowaniem przez osobę nieletnią treści seksualnych. Podobna część twierdzi, iż zna osobę, która zajmuje się takim procederem. Zaledwie 2 % badanych przyznaje, że namawiały inne osoby do rozbierania się – w zdecydowanej większości byli to mężczyźni. Aż 12 % badanych kobiet było nakłanianych do rozbierania się. 3 % respondentów potwierdziło, że otrzymali pewne wynagrodzenie za udział w wideoczacie (pytanie nie wiązało się z czynnościami seksualnymi). W związku z tematyką i formą badania (badanie deklaratywne), nie powinno się generalizować jego wyników, temat mógł być rzeczywiście trudny dla wielu nastolatków, tak więc pozostaje pytanie o wiarygodność odpowiedzi. Rekomendowane są dalsze badania, stosując inne metodologie, nadal jednak mające na względzie prywatność badanych osób[162]. Autor jest zdania, iż zważając na błyskawiczny rozwój Internetu i odstęp czasowy od badania (blisko dekadę), wyniki badania mogłyby być zgoła inne, bardziej zatrważające, niepokojące. Powszechnie wiadomo, że coraz więcej młodych osób korzysta z sieci, włączając w to laptopy, tablety czy smartfony. Coraz więcej jest również przemocy online oraz tzw. groomingu, czyli uwodzenia dziecka przez Internet.

Na potwierdzenie powyższych tez, przedstawione zostaną rezultaty badania *EU Kids Online* z roku 2018. Na pytanie „*Czy w ciągu ostatniego roku choć raz otrzymałeś/aś przez Internet jakiekolwiek wiadomości związane z seksem? Chodzi*

[162] https://dyzurnet.pl/badania [dostęp 06.03.2022 r.].

o zdjęcia, słowa, obrazki bądź filmy", procent twierdzących odpowiedzi kształtuje się następująco: grupa 11-12 lat – 5,4 % chłopców i 1,1 % dziewczynek; 13-14 lat – 12 % chłopców i 9 % dziewczynek; 15-17 lat – 24 % chłopców i 23 % dziewczynek[163]. Ponadto, z badań Instytutu Profilaktyki Zintegrowanej (IPZIN) wynika, że ponad 72% chłopców opowiada się za korzystaniem z pornografii przy pomocy sieci. W sieci, w której brak jest ograniczeń[164]. Interesującym jest fakt, iż z wiekiem różnica w tym badaniu między chłopcami, a dziewczynkami zaciera się znacząco. Wpływ na to zjawisko mogą mieć względy natury psychologicznej lub rozwojowej.

Jak nieoceniony jest wkład NASK w rozwój kompetencji cyfrowych pokazuje jakość i ilość organizowanych szkoleń online. Np. w 2021 roku, w listopadzie instytut działania swe ukierunkował na pracowników administracji publicznej. W ramach kampanii #CyberbezpiecznySamorząd poruszono kwestie podstaw cyberbezpieczeństwa, podstaw prawnych krajowego systemu cyberbezpieczeństwa, analizy rodzajów cyberataków i reagowania na nie, zgłaszania incydentów i innych[165]. Poprzez udział pracowników w tego rodzaju warsztatach, stale podnoszona jest ich świadomość cyberzagrożeń i zarazem kompetencje cyfrowe. To niezwykle ważne obecnie, gdy wiele urzędów oraz instytucji w dobie COVID-19, prowadzi pracę zdalną. Bez wątpienia, wiedza i umiejętności nabyte podczas szkoleń wpływają pozytywnie na indywidualnego użytkownika, ale również na cały system teleinformatyczny, którego jest on częścią. Bowiem nawet jedno niewłaściwe działanie pojedynczego użytkownika, może mieć olbrzymi skutek na system i innych współużytkowników.

Nie należy zapominać również o konferencjach organizowanych w ramach instytutu. Podczas *Cyber24Day* skupiono się na budowaniu świadomości znaczenia zarządzania strategicznego i tworzenia sprawnego ekosystemu cyberbezpieczeństwa narodu, państwa i biznesu. Współczesny świat biegnie, pędzi, zmienia się wręcz w każdej sekundzie ludzkiego życia. Podobnie jest z cyberbezpieczeństwem. Nowinki technologiczne pojawiają się co kilka lat bądź nawet częściej, co powoduje powstawanie nowych wyzwań ale i szans. Zamiast zarządzać kryzysami, należy starać się przewidywać nowe zagrożenia i właściwie się na nie przygotowywać. Celem panelu „*Wyprzedzić*

[163] J. Pyżalski, A. Zdrodowska, Ł. Tomczyk., T. Abramczuk, 2019, *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, Wydawnictwo Naukowe UAM, Poznań.

[164] https://www.czasopismobiologia.pl/artykul/internet-a-edukacja-seksualna-mlodziezy-czyli-o-wyimaginowanym-wizerunku-seksu-oraz-tworzeniu-nieistniejacych-standardow-i-norm-seksualnych-w-sieci [dostęp 06.03.2022 r.].

[165] https://www.nask.pl/pl/aktualnosci/3977,cyberbezpiecznysamorzad-ruszamy-ze-szkoleniami.html [dostęp 06.03.2022 r.].

zagrożenie – jak skutecznie informować obywateli o nowych cyberzazgrożeniach" było przede wszystkim skupienie się na sferze udziału użytkowników w sieci i ich edukacji[166].

Ponadto NASK planuje i realizuje wiele innych projektów, m.in. *„Przygody Plika i Foldera w Sieci"*, *„Bądźmy bezpieczni w Internecie"*, *„Tworzymy bezpieczny Internet"* czy *„Senior dla Seniora".* Zainaugurowano również program *„Kursor"*, który dotyczy bezpiecznego korzystania z nowych technologii, stosowania *edutainment* zarówno w życiu codziennym, jak i praktyce szkolnej. Oferta edukacyjna stworzona przez NASK obejmuje swoim zasięgiem dzieci, młodzież, dorosłych, wykładowców akademickich oraz pracowników instytucji publicznych i przedstawicieli wymiaru sprawiedliwości. Wszystkie te działania popularyzatorskie i edukacyjne mają na celu zwiększanie świadomości bezpieczeństwa cyfrowego dzieci i młodzieży. Instytut obecny jest także w wydarzeniach typu Festiwal Nauki czy Piknik Naukowy organizowany przez Centrum Nauki Kopernik i Polskie Radio S.A. Ponadto, NASK PIB koordynuje zainicjowany przez *ENISA* Europejski Miesiąc Cyberbezpieczeństwa, odbywający się cyklicznie corocznie w październiku.

Warto przyjrzeć się nieco bliżej inicjatywie *European Cyber Security Month.* W 2021 roku miała miejsce jej ósma już edycja. *ECSM* to 31 dni warsztatów, kampanii, inicjatyw oraz konferencji, mających podnieść świadomość użytkowników w kwestii bezpieczeństwa w Internecie. Oprócz udziału w wydarzeniach, każdy obywatel może dołożyć swoją cegiełkę do wspólnego dzieła, jakim jest cyberbezpieczeństwo. Można zorganizować własną inicjatywę i po przesłaniu zgłoszenia do NASK oraz oczywiście po otrzymaniu akceptacji – upublicznić ją (np. przeprowadzenie wykładu o sztucznej inteligencji czy lekcji dla uczniów o bezpieczeństwie w portalach społecznościowych)[167].

Powstałe w 2020 roku Centrum Rozwoju Kompetencji Cyfrowych ma na celu rozwijanie i kształtowanie kompetencji cyfrowych nie tylko najmłodszych Polaków, ale także wspiera m.in. seniorów, osoby z niepełnosprawnością i innych mających problemy z dostępem do cyfrowych narzędzi. Prowadzi szeroko rozumianą współpracę

[166] https://www.nask.pl/pl/aktualnosci/4301,NASK-podczas-Cyber24Day.html [dostęp 06.03.2022 r.].
[167]https://www.nask.pl/pl/aktualnosci/2274,Dolacz-do-Europejskiego-Miesiaca-Cyberbezpieczenstwa.html [dostęp 22.05.2022 r.].

z podmiotami komercyjnymi, urzędami oraz organizacjami pozarządowymi. Do zadań departamentu w szczególności należą[168]:

- realizowanie działań mających na celu zwiększenie kompetencji sektora publicznego;
- zapobieganie zjawiskom negatywnym w sieci, przede wszystkim dezinformacji;
- prowadzenie analiz i badań w obszarze społeczeństwa informacyjnego, określanie wyzwań i koordynacja polityk publicznych;
- wypełnianie obowiązków określonych w ustawie o Zintegrowanym Systemie Kwalifikacji i organizowanie działań na rzecz cyfrowej dostępności;
- zapoczątkowywanie, koordynacja i realizacja działań w obszarze rozwoju społeczeństwa informacyjnego, w szczególności podnoszenia cyfrowych kompetencji.

Podstawę prawną Centrum stanowi Zarządzenie nr 2 Ministra Cyfryzacji z dnia 27 stycznia 2020 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Cyfryzacji[169]. Szereg zadań opartych jest na współpracy z podmiotami w obszarze cyberbezpieczeństwa, obejmując swoim zakresem system nauki i oświaty, przedsiębiorców czy sektor pozarządowy. Centrum w sposób holistyczny zbiera informacje dotyczące poziomu kompetencji cyfrowych, monitoruje trendy i potrzeby na rynku pracy, a także rekomenduje kierunku rozwoju transformacji cyfrowej kraju. W związku z powyższym, podmiot ten jest wiodący w zakresie niniejszego opracowania.

Niemniej istotnym elementem budującym nie tylko świadomość użytkowników i ich bezpieczeństwo w cyberprzestrzeni jest – Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni im. Jerzego Witolda Różyckiego. Do roku 2019 nosiło nazwę Narodowego Centrum Kryptologii (NCK). Jest to jednostka podległa Ministrowi ON, która zajmuje się badaniami oraz wdrażaniem rozwiązań kryptograficznych w obszarze potrzeb administracji publicznej oraz wojska. NCK utworzono decyzją Ministra ON w roku 2013.

Obecnie NCBC przy udziale innych podporządkowanych jednostek, przekształcone zostało w Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni. NCBC stanowiło zaczątek Wojsk Obrony Cyberprzestrzeni – jak stanowi ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny[170] – jest to specjalistyczny komponent sił zbrojnych. Zadaniem tego komponentu

[168] https://www.gov.pl/web/cyfryzacja/centrum-rozwoju-kompetencji-cyfrowych [dostęp 17.12.2023 r.].
[169] https://www.gov.pl/web/cyfryzacja/dumc-2020-poz3 [dostęp 17.12.2023 r.].
[170] Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655 z późn. zm.).

ma być prowadzenie pełnego spektrum działań w cyberprzestrzeni, ponadto proaktywnej ochrony i aktywnej obrony kluczowych zasobów cyberprzestrzeni RP.

W katalogu zadań nowoutworzonej jednostki ujęto[171]:

- zapewnienie bezpieczeństwa teleinformatycznego;
- prowadzenie badań naukowych;
- budowa i użytkowanie narodowych technologii kryptologicznych;
- wytwarzanie nowych produktów dla kraju dzięki zespoleniu potencjału naukowego z przemysłowym;
- prowadzenie działalności naukowo-edukacyjnej, wdrożeniowej, opiniodawczej;
- opracowywanie nowoczesnych metod wykrywania incydentów w cyberprzestrzeni, projektowanie rozwiązań do ochrony informacji, rozwijanie własnych urządzeń kryptograficznych;
- zapewnienie właściwego funkcjonowania zespołu *CSIRT MON* monitorującego sieć resortu ON w trybie 24/7.

Jednym z przykładów realizacji zadań ochrony użytkowników przed zagrożeniami czyhającymi w cyberprzestrzeni było spotkanie edukacyjne w dniu 10 lutego 2022 roku z kadrą kierowniczą 9 Brygady Wsparcia Dowodzenia Dowództwa Generalnego Rodzajów Sił Zbrojnych. W szkoleniu uczestniczyli ponadto przedstawiciele Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego, czyli *CSIRT KNF*. Biorąc pod uwagę charakter służby i pracy, personel ten podlega często dużo większym niebezpieczeństwom rodzącym się w sieci. Podczas panelu omówione zostały kwestie bezpiecznego korzystania z systemów wojskowych, identyfikacji zagrożeń w systemach bankowości elektronicznej i metod stosowanych przez cyberprzestępców. Podano przykłady nowych trendów w systemach e-commerce i szanse jak i ryzyka, jakie mogą powstawać przy rozwoju tego rodzaju ulepszeń. Szkoleni podzielili się swoimi spostrzeżeniami oraz doświadczeniami, tak z użytkowania wojskowego obszaru cyberprzestrzeni, jak i cywilnej jego części. Dzięki łączonej inicjatywie NCBC-DKWOC oraz *CSIRT-KNF* obawy przed swobodnym i bezpiecznym użytkowaniem sieci zostały zminimalizowane. W ocenie ekspertów oraz szkolonych, spotkanie było okazją do wymiany doświadczeń i omówienia zagrożeń, przed którymi stoi każdy obywatel cyfrowego świata[172]. Bez

[171] https://www.wojsko-polskie.pl/woc/zadania/ [dostęp 15.05.2022 r.].
[172] https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/ncbc-dkwoc-dzieli-sie-wiedza/ [dostęp 15.05.2022 r.].

wątpienia takiego rodzaju szkolenia zwiększają poziom świadomości zagrożeń w cyberprzestrzeni i powinny być intensyfikowane oraz rozszerzane na inne grupy społeczne w miarę możliwości.

Wymieniona już wcześniej *ENISA* (*The European Network and Information Security Agency)*, czyli Europejska Agencja Bezpieczeństwa Sieci i Informacji powstała z inicjatywy Komisji Europejskiej, w 2003 r. jako ponadnarodowa agencja zajmująca się zapewnianiem bezpieczeństwa w Internecie. Dzięki badaniom przeprowadzonym w latach 2006-2007 w *ENISA*, w kwestii zbudowania systemu *EISAS* (*European Information Sharing and Alerting System)*, tj. europejskiego systemu wymiany informacji dotyczących bezpieczeństwa komputerowego, uruchomiono realizację projektu *FISHA* (*A Framework for Information Sharing and Alerting)*. System ten odpowiada na potrzeby edukacyjne UE. Skierowano go do użytkowników domowych i firm z sektora średnich i małych przedsiębiorstw. Bezsprzecznie, grupy te mają ogromne znaczenie na bezpieczeństwo w sieci, a jednocześnie na bezpieczeństwo infrastruktury teleinformatycznej państw Unii. Co więcej, wymienieni stanowią łatwy cel ataku z powodu niskiej świadomości i czasami zaniedbywania zabezpieczeń[173]. Jak już wspomniano w poprzednim podrozdziale, w związku z wejściem w życie w 2019 r. *Cybersecurity Act* zmieniono nazwę *ENISA* z Europejskiej Agencji Bezpieczeństwa Sieci i Informacji na Agencję UE ds. Cyberbezpieczeństwa.

W ramach swojej działalności, *ENISA*:

- wspiera państwa członkowskie, organy, instytucje i jednostki organizacyjne UE w zakresie wdrażania europejskiej polityki cyberbezpieczeństwa i polityk sektorowych;
- doradza Komisji oraz państwom członkowskim w obszarze bezpieczeństwa informacji i pomaga im w rozwiązywaniu problemów z zakresu bezpieczeństwa oprogramowania i sprzętu;
- gromadzi i analizuje dane dotyczące naruszenia na terytorium Europy cyberbezpieczeństwa i dokonuje oceny analizy ryzyka;
- promuje metody analizy oceny ryzyka i zarządzania ryzykiem celem sprawniejszego reagowania na zagrożenia;

[173] P. Sienkiewicz, H. Świeboda, 2010, *Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa*, Polskie stowarzyszenie zarządzania wiedzą, nr 33, s. 32-33.

- uczestniczy w wymianie najlepszych, aktualnych praktyk w zakresie podnoszenia świadomości i współpracy z wieloma podmiotami w dziedzinie bezpieczeństwa teleinformatycznego, głównie przez tworzenie partnerstw publiczno-prywatnych;
- monitoruje proces opracowywania norm dla usług i produktów z dziedziny bezpieczeństwa sieci i systemów teleinformatycznych;
- promuje certyfikację w krajach członkowskich oraz ustanawia i utrzymuje ramy certyfikacji, koordynuje przejrzystość całego procesu i wzmacnia zaufanie do jednolitego rynku cyfrowego;
- zwiększa świadomość publiczną i poziom kompetencji cyfrowych przez działania edukacyjne[174].

W obszarze *ENISA* działają następujące komórki: Zarząd, Dyrektor Wykonawczy, Rada Wykonawcza, Grupa Doradcza ENISA (*ENISA Advisory Group)* i Sieć Krajowych Urzędników Łącznikowych.

Poszerzenie zadań i obowiązków *ENISA* pozwoli zmniejszyć pewne różnice i możliwości w zasobach oraz wprowadza nowe minimalne wymogi w zakresie cyberbezpieczeństwa. Bez wątpienia to właściwy krok ku lepszej harmonizacji europejskiego środowiska cyberprzestrzeni, jednak nadal pozostawienie w niektórych obszarach możliwości (dobrowolnego wyboru) – a nie obowiązku, powodować może brak poczucia danej potrzeby w państwach członkowskich.

Wszystkie wyżej wymienione podmioty stanowią szczególnie istotne ogniwa w całym systemie cyberbezpieczeństwa. Są odpowiedzialne za tworzenie i rozwijanie bezpiecznej cyberprzestrzeni, w której użytkownicy powinni być świadomi efektów każdego wykonanego przez nich kroku i podjętego działania.

3.4. System cyberbezpieczeństwa RP

Pod pojęciem system kryje się pojęcie układ. Mianowicie, systemem określa się skoordynowany wewnętrznie układ elementów, które spełniają określone funkcje. System jest traktowany jako wyodrębniony z otoczenia. Jego składowe stanowią integralną całość o jasno określonych prawidłowościach funkcjonowania w wyznaczony sposób[175].

[174] Ibidem.
[175] E. Zabłocki, 2012, *System bezpieczeństwa narodowego*, Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych, Dęblin, s. 71.

Pojęcie *„Krajowego systemu cyberbezpieczeństwa”* zostało zdefiniowane w *Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*[176], bowiem jest to system składający się z krajowych podmiotów lub struktur organizacyjnych podmiotów z relacjami między tymi podmiotami bądź strukturami, który służy zapewnieniu wysokiego poziomu cyberbezpieczeństwa – bezpieczeństwa cyberprzestrzeni RP.

Obecnie polski system cyberbezpieczeństwa oparto o ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Jej celem jest określenie sposobu organizacji i funkcjonowania krajowego systemu cyberbezpieczeństwa, formy sprawowania kontroli i nadzoru w zakresie stosowania jej przepisów, a także zakresu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Zgodnie z dyrektywą NIS, ustawa ta nie ma odzwierciedlenia w stosunku do przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania, objętych krajowymi i europejskimi wymogami sektorowymi w obszarze cyberbezpieczeństwa. Dokument ten nie obejmuje również podmiotów, które wykonują działalność leczniczą i tych tworzonych przez Szefa Agencji Wywiadu oraz Szefa Agencji Bezpieczeństwa Wewnętrznego.

Ustawa zdefiniowała system określając jego cel jakim jest *„zapewnienie cyberbezpieczeństwa na poziomie krajowym i w tym niezakłóconego świadczenia usług cyfrowych i usług kluczowych, poprzez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych, które służą do świadczenia tych usług i zapewnienia obsługi incydentów”.* Jak już wspomniano wcześniej, cyberbezpieczeństwo wg ustawy oznacza odporność systemów informacyjnych na działania naruszające poufność, dostępność, integralność i autentyczność wszystkich przetwarzanych danych bądź związanych z nimi usług, które oferowane są przez te systemy informacyjne.

W skład systemu, zgodnie z ustawą wchodzą:

- operatorzy usług kluczowych;
- dostawcy usług cyfrowych;
- Zespoły *CSIRT (CSIRT MON, CSIRT NASK, CSIRT GOV*) i zespoły sektorowe cyberbezpieczeństwa;
- Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa;
- Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa;
- Kolegium do Spraw Cyberbezpieczeństwa;

[176] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017.

- podmioty publiczne wskazane w przepisie w art. 4 ustawy.

Koncepcja systemu reagowania na incydenty komputerowe zakłada jego kompletność, kompleksowość i transparentność. *CSRIRT GOV, CSIRT MON, CSIRT NASK* współpracują z organami właściwymi ds. cyber, sektorowymi zaspołami cyberbezpieczeństwa, ministrem właściwym ds. informatyzacji i Pełnomocnikiem, co powinno zapewnić kompletny i jednolity system zarządzania ryzykiem na szczeblu krajowym. Ma on pozwolić ponadto, na przeciwdziałanie zagrożeniom cyberbezpieczeństwa o podłożu międzynarodowym i pozasektorowym. W szczególnych okolicznościach *CSIRT* mogą – poprzez wniosek dostawców usług cyfrowych, operatorów usług kluczowych i sektorowych zespołów cyberbezpieczeństwa – zapewnić właściwe wsparcie w obsłudze incydentów.

Ustawa w klarowny sposób określa zadania poszczególnych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego. *CSIRT GOV* odpowiada za koordynację procesu reagowania na incydenty komputerowe, które występują w zakresie administracji rządowej i infrastruktury krytycznej. Do zadań zespołu należą: rozpoznawanie, zapobieganie oraz wykrywanie zagrożeń mogących mieć wpływ na bezpieczeństwo systemów teleinformatycznych organów administracji państwowej bądź systemów sieci teleinformatycznych objętych wykazem instalacji, obiektów, usług i urządzeń infrastruktury krytycznej. Listę zamykają systemy teleinformatyczne właścicieli i posiadaczy obiektów, urządzeń czy instalacji infrastruktury krytycznej, które określone są w ustawie o zarządzaniu kryzysowym[177].

CSIRT MON swoje działania koncentruje wokół obronności. Zapobieganie, wykrywanie, reagowanie na incydenty komputerowe w sieciach i systemach teleinformatycznych w resorcie ON należą do jego zasadniczych kierunków. Struktura *CSIRT MON* jest trzypoziomowa: Centrum Koordynacyjne, Centrum Wsparcia i administratorzy systemów teleinformatycznych jednostek oraz komórek organizacyjnych resortu ON. Ponadto, w resorcie ON usytuowany jest także Narodowy Punkt Kontaktowy – w zakresie współpracy z *NATO*[178].

Trzeci podmiot stanowi *CSIRT NASK* – w ramach Naukowej Akademickiej Sieci Komputerowej. *NASK* jest państwowym instytutem badawczym, nad którym nadzór sprawuje minister właściwy do spraw cyfryzacji. Priorytetem w działalności *CSIRT*

[177] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), s. 27.
[178] Ibidem, s. 25-26.

NASK jest reagowanie na incydenty w obszarze cyberbezpieczeństwa cywilnego, tj. reagowanie na incydenty i zagrożenia w sieciach ogólnodostępnych. W razie ewentualnego ataku – zespół ten podejmuje czynności we współpracy z innymi ośrodkami w kraju a także za granicą, celem dokonania analizy sposobu, natury, zasięgu danego incydentu i wymiany informacji z kluczowymi instytucjami i sektorami[179]. *CSIRT NASK* ma możliwość wydawania rekomendacji dotyczących sposobu postępowania w momencie zagrożenia i kierunków działań mających na celu minimalizację skutków cyberataku.

Kategorię podmiotową otwierają jednostki sektora finansów publicznych (określone ustawą z dnia 27.12.2009 r. o finansach publicznych[180]). W katalogu podmiotów publicznych zawarto również: instytuty badawcze; Narodowy Bank Polski; Bank Gospodarstwa Krajowego; Polska Agencja Żeglugi Powietrznej; Polskie Centrum Akredytacji; Urząd Dozoru Technicznego; Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej, a także wojewódzkie fundusze; spółki prawa handlowego o charakterze zadań użyteczności publicznej wg ustawy z dnia 20.12.1996 r. o gospodarce komunalnej[181], co oznacza bieżące zaspokajanie potrzeb ludności; podmioty realizujące usługi z zakresu cyberbezpieczeństwa.

W każdym podmiocie publicznym wyznaczona jest osoba odpowiedzialna za utrzymywanie kontaktów z poszczególnymi podmiotami KSC. Obowiązkiem podmiotu publicznego jest także zarządzanie incydentem i jego zgłoszenie – do 24 godzin od momentu wykrycia, do właściwego *CSIRT*.

Istnieją również sektorowe zespoły cyberbezpieczeństwa, które oznaczają zespół ustanowiony przez właściwy organ dla danego podsektora lub sektora usług kluczowych, wymienionego w ustawie, odpowiedzialnego za wsparcie bądź całkowitą obsługę incydentów w danym podsektorze lub sektorze.

Kolejny element prowadzony jest przez ministra właściwego ds. informatyzacji, jest to PPK – Pojedynczy Punkt Kontaktowy. Zasadniczą funkcją PPK jest przekazywanie informacji, odbieranie zgłoszeń incydentu poważnego lub istotnego dotyczącego dwóch lub większej ilości państw członkowskich UE z PPK w innych państwach Unii, ponadto przekazywanie tych zgłoszeń do *CSIRTów* krajowych. Analogicznie, przekazywanie tego rodzaju zgłoszeń (incydentów poważnych lub istotnych dotyczącego

[179] Ibidem, s. 26-27.
[180] Ustawa z dnia 27 grudnia 2019 r. o finansach publicznych (Dz.U. 2009 nr 157 poz. 1240 z późn. zm.).
[181] Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. 1997 nr 9 poz. 43 z późn. zm.).

dwóch lub większej ilości państw UE) na wniosek właściwych *CSIRTów* do PPK w innych krajach członkowskich. Pojedynczy Punkt Kontaktowy zapewnia również reprezentację Polski w Grupie Współpracy i koordynację między organami właściwymi oraz organami władzy publicznej w RP wraz z odpowiednimi organami w krajach członkowskich Unii. PPK jest przekaźnikiem w kwestii wymian informacji na potrzeby Grupy Współpracy i Sieci *CSIRT*. Punkt pozostaje w kontakcie z Komisją Europejską w kwestii informowania o wyznaczonych organach właściwych, zleconych zadaniach, wykazie kluczowych usług i ich operatorach[182].

Odpowiedzialną rolę ma także Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, podległy Radzie Ministrów. Koordynuje on realizowanie polityki rządu w zakresie cyberbezpieczeństwa. Katalog zadań Pełnomocnika obejmuje:

- analizę i ocenę funkcjonowania krajowego systemu cyberbezpieczeństwa;
- kontrolę i nadzór procesu zarządzania ryzykiem KSC;
- inicjowanie różnego rodzaju działań mających na celu zapewnianie cyberbezpieczeństwa na poziomie krajowym i upowszechnianie nowych rozwiązań;
- inicjowanie ćwiczeń cybernetycznych na poziomie krajowym;
- wydawanie zaleceń dotyczących oprogramowania bądź sprzętu na wniosek właściwego *CSIRT*;
- współpraca z innymi państwami, organizacjami oraz instytucjami międzynarodowymi w zakresie cyberbezpieczeństwa;
- inicjowanie działań mających na celu rozwój badań naukowych i technologii;
- podejmowanie aktywności mających na celu poszerzanie świadomości społecznej w zakresie bezpiecznego korzystania z Internetu[183].

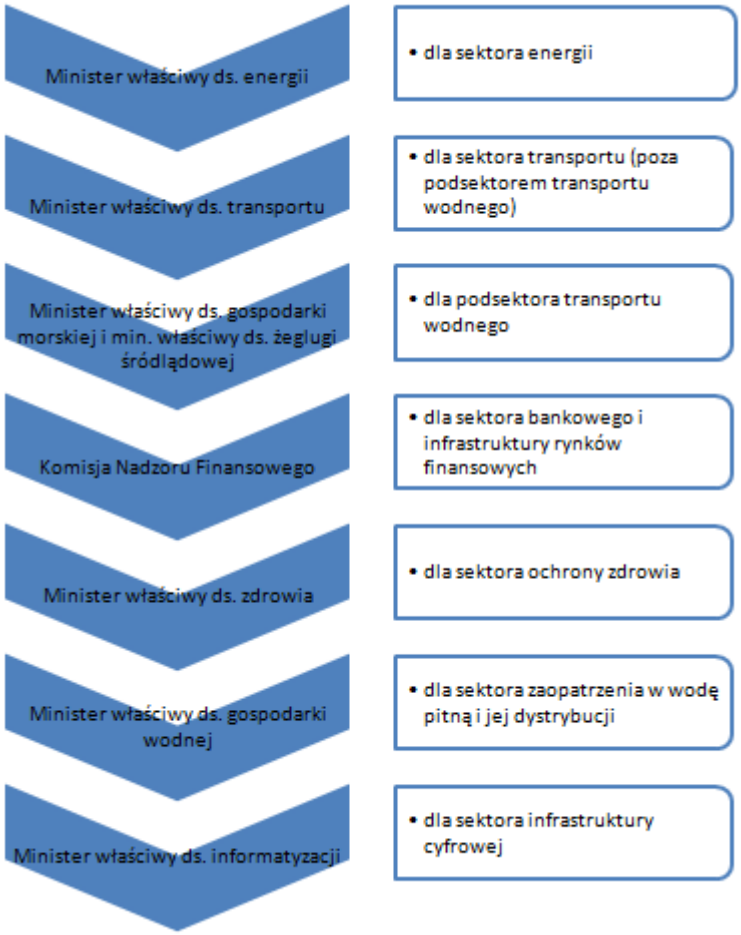
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa może przekazywać wnioski dotyczące podejmowania działań przez podmioty KSC. Ponadto, jego obowiązkiem jest koordynacja przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego dotyczącego zagrożeń cyberbezpieczeństwa, które mogłyby doprowadzić do sytuacji kryzysowej.

Przy Radzie Ministrów działa także Kolegium do Spraw Cyberbezpieczeństwa, które jest organem opiniodawczo-doradczym w obszarze cyberbezpieczeństwa i działań *CSIRT GOV, CSIRT MON i CSIRT NASK*, sektorowych zespołów cyberbezpieczeństwa

[182] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), s. 44-46.
[183] Ibidem.

i właściwych organów. Kolegium Przewodniczy Prezes Rady Ministrów albo z jego upoważnienia Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, członkami Kolegium są ministrowie wskazani w ustawie.

Ustawa o KSC powołuje organy właściwe do spraw cyberbezpieczeństwa, które odpowiadają za nadzór nad operatorami usług cyfrowych i kluczowych. Organy te stanowią element krajowego systemu cyberbezpieczeństwa, odpowiedzialny za opracowywanie we współpracy z *CSIRT* zasad bezpieczeństwa teleinformatycznego. Narzędziem organu właściwego jest wydawanie decyzji o uznaniu bądź cofnięciu uznania podmiotu za operatora usług kluczowej, ponadto bieżąca kontrola operatorów usług cyfrowych i kluczowych. Organ właściwy jest podmiotem kontrolującym i nadzorującym wykonywanie obowiązków przez dostawców usług cyfrowych i operatorów usług kluczowych, ma możliwość nakazania usunięcia ustalonych w drodze kontroli nieprawidłowości.



Rys. 3.4. Organ właściwy – kto jest kim? (źródło: opracowanie własne na podstawie: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa [dostęp 15.03.2022 r.])

Minister właściwy do spraw informatyzacji prowadzi PPK ds. cyberbezpieczeństwa, którego celem jest przekazywanie zgłoszeń incydentów poważnych i istotnych do krajów członkowskich UE oraz KE. Zadaniem ministra jest implementacja strategii cyberbezpieczeństwa, prowadzenie wykazu operatorów kluczowych usług, rozwijanie polityki informacyjnej w zakresie KSC. Odpowiada on także za rozwój systemu teleinformatycznego, który umożliwia zautomatyzowanie procesu obsługi incydentów, ostrzegania o zagrożeniach i szacowania ryzyka[184].

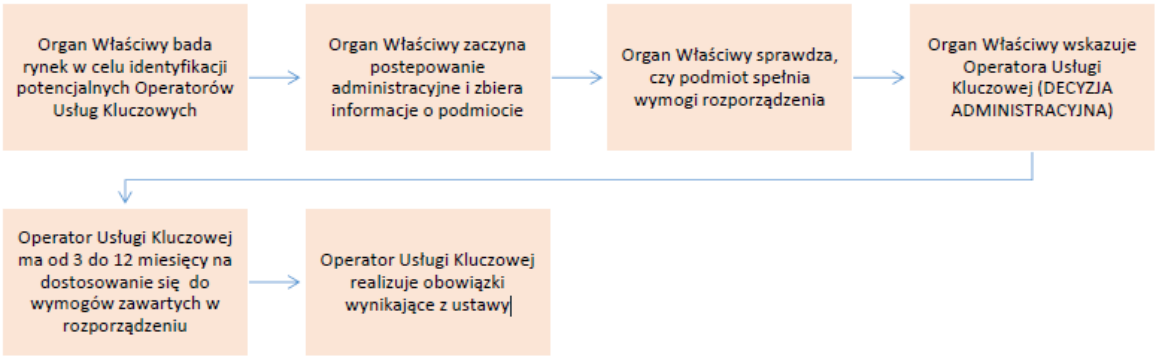
Kolejnym podmiotem w krajowym systemie cyberbezpieczeństwa jest Rządowe Centrum Bezpieczeństwa. RCB podlega Prezesowi Rady Ministrów i pełni funkcję Krajowego Centrum Zarządzania Kryzysowego. Utworzone zostało na mocy ustawy o zarządzaniu kryzysowym w 2007 r. Jednym z podstawowych zadań RCB jest analiza zagrożeń w oparciu o posiadane dane, uzyskiwane ze środków kryzysowych w ramach administracji publicznej, również partnerów międzynarodowych i innych źródeł. RCB opracowuje logiczne rozwiązania w sytuacjach kryzysowych i koordynuje przepływ informacji o zagrożeniach. W sferze cyberbezpieczeństwa – przyjmuje informacje o stanie bezpieczeństwa w cyberprzestrzeni oraz dokonuje stałej analizy w zakresie efektywności infrastruktury krytycznej[185]. Tak więc RCB nie jest bezpośrednio zaangażowane w realizację zadań w środowisku cyberprzestrzeni.

Szczególne znaczenie przypisuje się operatorom usług kluczowych. Bowiem zgodnie z *Dyrektywą NIS*, usługa kluczowa wymieniona musi być w wykazie usług kluczowych i jak sama nazwa wskazuje, ma znaczenie kluczowe dla krytycznej działalności gospodarczej bądź społecznej państwa. Podmiot prowadzący działalność w jednym z podsektorów lub sektorów wymienionych w załączniku ustawowym jest operatorem takiej usługi. Operator ten musi posiadać jednostkę organizacyjną na terytorium RP, zaś organ właściwy ds. cyberbezpieczeństwa wydaje decyzję o uznaniu danego go za operatora usługi kluczowej. Klasyfikacja sektorów i podsektorów odpowiada jednocześnie organom właściwym ds. cyberbezpieczeństwa i kształtuje się jak poniżej:

- sektor infrastruktury cyfrowej;
- sektor zaopatrzenia w wodę pitną i jej dystrybucję;
- sektor bankowości i infrastruktury rynków finansowych;
- sektor ochrony zdrowia;
- sektor transportu z podsektorami: lotniczym, kolejowym, wodnym oraz drogowym;

[184] C. Banasiński (red. nauk.): *Cyberbezpieczeństwo…,* op. cit., s. 164.
[185] C. Banasiński (red. nauk.): *Cyberbezpieczeństwo…,* op. cit., s. 165.

- sektor energii z podsektorami: energia elektryczna, ciepło, ropa naftowa, gaz, wydobywanie kopalin, dostawy i usługi dla sektora energii, a także jednostki nadzorowane przez ministra właściwego ds. energii.



Rys. 3.5. Wyznaczenie operatorów usług kluczowych (źródło: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- [dostęp 15.03.2022 r.])

Organ właściwy ds. cyberbezpieczeństwa wydając decyzję o uznaniu danego operatora za operatora usługi kluczowej bierze pod uwagę potencjalny incydent, który miałby istotny skutek zakłócający dla usługi kluczowej oraz operatora. Istotność skutku zakłócającego mierzona jest zgodnie z tzw. progami istotności określonymi w drodze rozporządzenia Rady Ministrów. Są to m.in. liczba użytkowników, zasięg geograficzny, wpływ incydentu. Szerzej opisano to powyżej podczas definiowana terminu incydent w podrozdziale „3.2 Wybrane regulacje prawne".

Nadrzędnym obowiązkiem operatora usługi kluczowej jest implementacja systemu zarządzania bezpieczeństwem (cyberbezpieczeństwem) w systemie informacyjnym, który wykorzystywany jest do świadczenia usługi kluczowej (do trzech miesięcy od otrzymania decyzji o ustanowieniu operatora). W zakresie systemu prowadzone jest szacowanie ryzyka wystąpienia incydentu; zarządzaniem tym ryzykiem i wprowadzenie właściwych środków technicznych i organizacyjnych (zapobiegawczych); gromadzenie informacji o cyberzagrożeniach i podatnościach systemu; zarządzanie incydentami; organizowanie w ramach systemu środków łączności zapewniających bezpieczną komunikację. Operator usługi kluczowej opracowuje przedmiotową dokumentację (do sześciu miesięcy od otrzymania decyzji administracyjnej), chyba, że jest on posiadaczem samoistnym, właścicielem lub posiadaczem zależnym urządzeń, usług, instalacji czy obiektów (będących w składzie infrastruktury krytycznej) wymienionych w ustawie o zarządzaniu kryzysowym z 2007 r., który posiada zaakceptowany plan ochrony infrastruktury krytycznej uwzględniający już kwestie cyberbezpieczeństwa – systemu informacyjnego niezbędnego do świadczeniu kluczowej usługi.

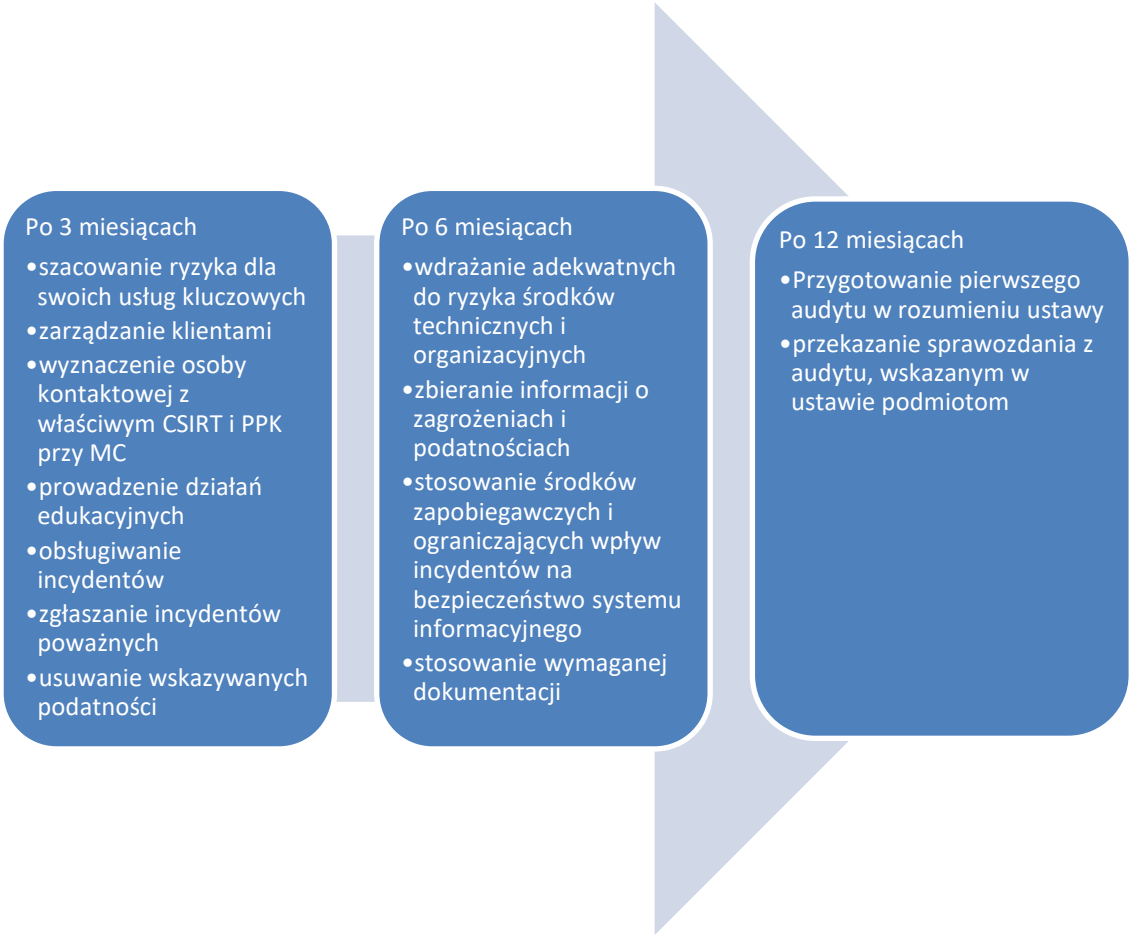
Ponadto, operator usługi kluczowej odpowiada za[186]:

- zapewnienie obsługi każdego występującego w ramach usługi incydentu;
- zapewnienie dostępu do archiwum rejestrowanych incydentów właściwym *CSIRT* w zakresie niezbędnym do realizacji zadań i sektorowemu zespołowi cyberbezpieczeństwa – o ile taki zostanie ustanowiony;
- klasyfikację incydentu jako poważnego według tzw. progów istotności;
- zgłoszenie incydentu poważnego nie później aniżeli 24 godzin od momentu wykrycia, do właściwego *CSIRT*;
- usunięcie podatności systemu informacyjnego, która może zostać wykorzystana przez zagrożenie bezpieczeństwa i poinformowaniu o tym fakcie organu właściwego ds. cyberbezpieczeństwa.

Na powyższym obowiązki operatora usługi kluczowej się nie kończą, bowiem musi zagwarantować on, co najmniej raz na dwa lata tzw. audyt bezpieczeństwa systemu informacyjnego, który wykorzystywany jest do świadczenia usługi. Audyt przeprowadzić mogą trzy wymienione w ustawie organy. Pierwszym jest jednostka oceniająca zgodność, akredytowana wg przepisów ustawy z 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku[187]. Drugi stanowi co najmniej dwóch audytorów, którzy posiadają certyfikaty zgodne z wytycznymi ministra właściwego ds. informatyzacji bądź co najmniej trzyletnią praktykę w obszarze audytu bezpieczeństwa systemów informacyjnych albo też co najmniej dwuletnią praktykę w obszarze audytu bezpieczeństwa systemów informacyjnych oraz posiadających dyplom ukończenia studiów podyplomowych (dot. audytu bezpieczeństwa systemów informacyjnych) – wydanym przez jednostkę organizacyjną uprawnioną (zgodnie z właściwymi przepisami), do nadawania stopnia naukowego doktora nauk prawnych, technicznych lub ekonomicznych. Ostatni organ to sektorowy zespół cyberbezpieczeństwa, jeśli oczywiście audytorzy są w stanie spełnić powyższe warunki. Operator usługi kluczowej przekazuje kopię sprawozdania z audytu, na uzasadniony wniosek do dyrektora RCB i organu właściwego ds. cyberbezpieczeństwa – gdy operator jest jednocześnie właści-

[186] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), s. 10-11.
[187] Zob. Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. 2016 poz. 542 z późn. zm.).

cielem, posiadaczem samoistnym lub posiadaczem zależnym urządzeń, instalacji, obiektów lub usług, które wchodzą w skład infrastruktury krytycznej i Szefa ABW[188].



Rys. 3.6. Obowiązki operatorów usług kluczowych (źródło: opracowanie własne na podstawie: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- [dostęp 15.03.2022 r.])

Dostawcą usług cyfrowych jest osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której siedziba, zarząd bądź przedstawiciel mieści się na terytorium RP, świadcząca usługę cyfrową (za wyjątkiem małych i mikroprzedsiębiorców- ustawa z 06.03.2018 r. prawo przedsiębiorców[189]). W sytuacji, gdy dostawca usługi cyfrowej oferuje usługę w Polsce, ale nie posiada jednostki organizacyjnej na terenie UE – wówczas wyznacza przedstawiciela, który posiada jednostkę organizacyjną w RP (o ile nie wskazał przedstawiciela w innym państwie członkowskim UE)[190]. Warto zaznaczyć, iż przedstawiciel to osoba fizyczna, prawna lub jednostka organiza-

[188] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), s. 14-16.
[189] Zob. Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2018 poz. 646 z późn. zm.).
[190] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), s. 16-20.

cyjna, nieposiadająca osobowości prawnej - ukonstytuowana w RP bądź innym państwie członkowskim Unii, która odpowiada za występowanie w imieniu dostawcy usługi cyfrowej (nieposiadającego jednostki organizacyjnej w Unii).

Sensem działania dostawców usług cyfrowych jest podejmowanie proporcjonalnych i właściwych środków organizacyjnych oraz technicznych do doprecyzowania elementów w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa systemów informacyjnych i sieci. Środki te powinny zapewnić sprawne zarządzanie ryzykiem, które dotyczy systemów informacyjnych wykorzystywanych do usługi cyfrowej. Środki uwzględniają takie czynniki jak: algorytm działania w przypadku obsługi incydentu; bezpieczeństwo systemów informacyjnych oraz obiektów; zarządzanie przepływem świadczenia usługi cyfrowej; monitoring, audyt i stałe testowanie i sprawdzanie; najnowszy stan wiedzy i zgodność z normami międzynarodowymi. Zadaniem dostawcy jest także stosowanie środków minimalizujących i zapobiegawczych w zakresie wpływu incydentów na świadczenie usługi cyfrowej; klasyfikowanie incydentów oraz zgłaszanie istotnego incydentu nie później niż do 24 godzin od czasu jego wykrycia.

W ustawie o KSC przewidziane są kary za niewykonywanie obowiązków spoczywających na operatorach usług kluczowych, dostawcach usług cyfrowych, przedsiębiorcach czy osobach fizycznych. Kary te są administracyjnymi karami finansowymi. Uzasadnienie kar, stanowi fakt, iż cyberprzestrzeń jest wspólnym dobrem, musi być więc chroniona i zabezpieczana w jednakowym stopniu przez każdego użytkownika. Brak synergii i wspólnego tonu w środowisku krajowym czy międzynarodowym może wpływać na skuteczność i efektywność działań na zdarzenia w cyberprzestrzeni. Kary te mają dwojaką funkcję, prewencyjną i odstraszającą od niedopełnienia ustawowych obowiązków. W zależności od naruszonego obowiązku kary mają charakter kwotowy bądź maksymalny w różnej wysokości - maksymalna kara to 200 tys. zł. Inna sytuacja występuje w momencie, gdy organ właściwy ds. cyberbezpieczeństwa uzna, że dostawca usługi cyfrowej lub dostawca usługi kluczowej rażąco narusza przepisy ustawy i powoduje: poważne i bezpośrednie zagrożenie cyberbezpieczeństwa państwa, w tym porządku publicznego albo życia i zdrowia ludzi; zagrożenie spowodowania utrudnień w świadczeniu usług lub poważnej szkody majątkowej – wówczas organ właściwy ma prawo nałożyć karę w kwocie do 1 000 000 zł[191].

[191] Ibidem.

W kwestii kar *ad personam* – mają one charakter fakultatywny. W sytuacji kiedy kierownik operator usługi kluczowej nie dochowuje należytej staranności, niewłaściwie wdraża system zarządzania bezpieczeństwem w systemie informacyjnym, nie prowadzi rzetelnie i systematycznie szacowania ryzyka, nie wyznacza osoby odpowiedzialnej, kontaktowej w ramach ksc bądź nie zapewnia audytu bezpieczeństwa (co najmniej raz na dwa lata), podlega karze w kwocie nie wyższej niż 200% miesięcznego wynagrodzenia. Kary proceduralne mogą być nałożone, jeśli operator utrudnia albo uniemożliwia przeprowadzenie kontroli[192].

Ogromną rolę w kształtowaniu i zapewnianiu bezpieczeństwa cyberprzestrzeni stanowią organy państwowe, sprawujące nadzór nad operatorami i dostawcami. Pouczające dla ww. może być ukaranie jednego podmiotu, co mogłoby spowodować włączenie funkcji odstraszania, czyli po prostu bardziej rzetelnego wypełnianie swoich obowiązków i zadań przez określone komórki.

3.5. Wnioski

Odnosząc się do regulacji prawnych poszczególnych państw, rozbieżności w zakresie definicji cyberbezpieczeństwa należy niwelować. Każde państwo członkowskie UE musi spełniać określone kryteria, jakie są przed nim stawiane. Ma to ułatwić współtworzenie systemu zintegrowanego, zapewniającego skuteczne bezpieczeństwo w cyberprzestrzeni. Działania te powinny być ukierunkowane na bezpieczeństwo obywateli jak i całego państw, tak aby każdy użytkownik mógł swobodnie i bez obaw w pełni korzystać z wynalazków jakie niesie za sobą cyfryzacja i rozwój technologii teleinformatycznych.

Ustawa o krajowym systemie cyberbezpieczeństwa stanowi wskazanie zadań i obowiązków, oraz uporządkowania kompetencji organów administracji publicznej, w taki sposób, aby obszary poszczególnych podmiotów nie dublowały się i aby uniknąć powstania luki kompetencyjnej pomiędzy nimi. Jednocześnie wprowadza wiele zadań i obowiązków poszczególnym elementom systemu cyberbezpieczeństwa. Bez wątpienia całkowite wdrożenie systemu i osiągnięcie przez niego właściwej sprawności może trwać nawet kilka lat, z uwagi na różny stopień zaawansowania firm w zakresie cyberbezpieczeństwa – odporności i reakcji.

[192] Ibidem, s. 58.

O uznaniu danego podmiotu jako operatora lub dostawcy decydują trzy przesłanki: czy podmiot świadczy usługę kluczową, czy właściwe realizowanie tej usługi zależy od działania systemów informacyjnych oraz czy prawdopodobny incydent w zakresie cyberbezpieczeństwa mógłby mieć poważny skutek dla świadczenia danej usługi.

W praktyce organy właściwe ds. cyberbezpieczeństwa wydają decyzję administracyjną, zgodnie z którą danego przedsiębiorcę lub dany podmiot mianują operatorem usługi kluczowej lub dostawcą usługi cyfrowej. Wiąże się to z realizacją określonych zadań i wypełnieniem wielu obowiązków.

Do obowiązków operatora usługi kluczowej w zakresie środków zapobiegających i ograniczających wpływ incydentów zaliczyć należy m.in. stworzenie mechanizmów zapewniających poufność, integralność, dostępność oraz autentyczność danych; ochronę przed nieuprawnioną modyfikacją lub dostępem do danych; aktualizację oprogramowania i co nie mniej ważne – podejmowanie działań bezpośrednio po zauważeniu podatności bądź zagrożenia.

Co jest istotne podkreślenia, realizacja ustawowych obowiązków wszystkich podmiotów systemu cyberbezpieczeństwa w obszarze przekazywania informacji o zdarzeniu do właściwych zespołów *CSIRT*, umożliwia sprawną ich obsługę i rozwój zdolności prewencyjnych. Oczywistym jest fakt, iż w sytuacji, gdy zespoły *CSIRT* nie mają odpowiednich danych i informacji – nie mogą skutecznie zareagować na zaistniały incydent.

Ustawa, sama w sobie nie wprowadza środków, które byłyby przełomem czy innowacją w cyberbezpieczeństwie, natomiast stanowi źródło podstaw prawnych do stosowania tychże środków. Środków (organizacyjnych i technicznych), które *de facto* powinny być realizowane przed określone podmioty już od lat.

Nie należy zapominać o innych karach, które wiązać można z obszarem cyberbezpieczeństwa. W momencie wycieku danych osobowych z np. przedsiębiorstwa, jego właściciel oprócz kary z ustawy o KSC odpowiadać również będzie w ramach RODO, gdzie należności te są znacznie surowsze.

Warto w tym miejscu wspomnieć ustawę o zarządzaniu kryzysowym, która zawiera ujęte przez RCB podmioty szczególnie istotne w obszarze infrastruktury krytycznej państwa. Ustawa o krajowym systemie cyberbezpieczeństwa stworzyła nową listę takich podmiotów, opracowaną przez Ministerstwo Cyfryzacji, ale w zakresie sfery cyber. Obszar ustawy o cyberbezpieczeństwie jest szerszy aniżeli o zarządzaniu kryzyso-

wym. Zastanawiającym jest fakt, iż RCB w systemie zarządzania kryzysowego jest informowane o zagrożeniach już przez operatora, natomiast w systemie cyberbezpieczeństwa – podmiot ten dostaje informacje od *CSIRT-ów*. Stąd, przepływ informacji w przypadku systemu cyberbezpieczeństwa jest wolniejszy.

Szereg zmian wprowadził również *Cybersecurity Act,* zgodnie z którym *ENISA* otrzymała permanentny mandat, a także została zmieniona jej nazwa na Agencję UE ds. Cyberbezpieczeństwa. Akt ten zwiększa znaczenie *ENISA* w obszarze współpracy z państwami członkowskimi, zespołami *CSIRT* i *CERT-EU* czy organami nadzorującymi ochronę prywatności. Zgodnie z powyższym, *ENISA* monitorując stan cyberbezpieczeństwa Unii przygotowuje raport uwzględniający zgłoszenia naruszeń bezpieczeństwa na obszarze wszystkich państw członkowskich. Ponadto, w dokumencie tym szerzej opisano zadania *ENISA* i tak np. nowym obszarem zainteresowania jest promowanie wdrożenia certyfikacji procesów, usług oraz produktów *ICT*[193]. Konkludując wyżej opisane treści, nie sposób się nie zgodzić, iż *ENISA* otrzymała miano pełnoprawnego gracza w obszarze cyber na arenie międzynarodowej.

Niedawno przyjęta *Dyrektywa NIS 2* ma na celu wzmocnienie bezpieczeństwa cybernetycznego w wybranych sektorach krytycznych na poziomie krajowym oraz unijnym. Przykładowo, zakres dyrektywy obejmuje szerzej podmioty z branży energetycznej jak i ochrony zdrowia oraz dostawców usług w obszarze infrastruktury cyfrowej. Rozszerzono również zakres samej dyrektywy, tak aby miała zastosowanie do nowych sektorów i podmiotów, tj. administracja publiczna, gospodarka odpadami i sektor spożywczy.

Dla rozwijania bezpieczeństwa cybernetycznego dyrektywa określa zarówno obowiązki w kwestii zgłaszania incydentów cybernetycznych w krytycznych sektorach społeczeństwa oraz w zakresie zarządzania ryzykiem. W dyrektywie wymieniono minimalne wymogi i środki, które wszystkie podmioty muszą podjąć celem zarządzania ryzykiem cyberbezpieczeństwa we własnej działalności. Zarządzanie ryzykiem cyberbezpieczeństwa oparte będzie na ryzyku i wynikach; w trakcie określania jego poziomu podmiot będzie musiał wziąć pod uwagę ekspozycję na ryzyko i swoją wielkość. Ponadto, jak dotychczas, podmioty muszą również informować organy a także, w stosownych przypadkach, odbiorców swoich usług o wszelkich istotnych incydentach.

[193] https://cyberpolicy.nask.pl/akt-o-cyberbezpieczenstwie-nowy-mandat-enisa/ [dostęp 22.05.2022 r.].

Opisywana *NIS 2* odpowiada na potrzeby wynikające z poprzedniej regulacji prawnej (*Dyrektywa NIS*). Brakowało bowiem pewnych interesariuszy, takich jak np. podmioty i organizacje administracji elektronicznej (nienależące do określonych kategorii), mimo, iż oferują one usługi ważne dla obywateli. Aktualizacja dyrektywy wskazała nowe sektory w oparciu o ich krytyczność dla społeczeństwa i gospodarki.

Bez wątpienia przykładem podnoszenia bezpieczeństwa w sieci jest unijny akt o usługach cyfrowych. *DSA* wprowadza szereg zmian, mających na celu poprawę ochrony użytkownika, zmniejszenie natężenia „niechcianych" reklam czy łatwiejsze sposoby zgłaszania nielegalnych treści czy zdarzeń.

Korzystanie z Internetu przez użytkowników motywowane jest różnymi czynnikami, tj. wiek, miejsce zamieszkania czy wykształcenie. Różna jest także intensywność działań, ich charakter oraz cel. Tak jak następuje rozwój technologiczny, tak również pojawiają się problemy będące wyzwaniem dla edukacji cyfrowej, która warunkuje rozwój społeczeństwa informacyjnego. W związku z powyższym niezwykle ważne są wszelkie działania podejmowane przez podmioty państwowe w obszarze budowania świadomości i kompetencji cyfrowych. Istotnym wydaje się być dbanie o osoby z regionów słabiej rozwiniętych, mniejszych miejscowości, w szczególności osoby starsze czy z niższymi dochodami.

4. Zagrożenia i wyzwania cyberbezpieczeństwa

4.1. Typologia cyberzagrożeń

W celu zrozumienia istoty cyberzagrożenia, należy uprzednio dokonać analizy terminu *zagrożenie*. Jest to sytuacja, w której obserwowane jest zwiększone prawdopodobieństwo powstania stanu niebezpiecznego, czyli stanu braku bezpieczeństwa[194]. Najprostsza definicja stanowi o tym, iż zagrożeniem określany jest stan bądź sytuacja, w której podmiot czuje się zagrożony, tak więc może nastąpić zdarzenie, które wywrze na niego negatywny wpływ[195]. Stąd, zagrożenie powoduje obniżenie poziomu bezpieczeństwa podmiotu.

Najczęściej zagrożenie jest konkretyzowane przez wartości, jakie mogą zostać utracone[196]. Człowiek obawia się straty wartości takich, jak: życie, zdrowie czy wolność. Charakterystyczna dla zagrożeń jest wysoka dynamika i zmienność, co ma przełożenie na poziom dyskomfortu poszczególnych osób czy całych społeczeństw[197].

W ustawie o KSC *zagrożenie cyberbezpieczeństwa* oznacza potencjalną przyczynę wystąpienia incydentu. *Incydent* zaś, jak już wspomniano stanowi zdarzenie, mogące mieć niekorzystny wpływ na całe cyberbezpieczeństwo[198]. Tak więc określenia te są ze sobą powiązane.

Jedną z najbardziej aktualnych definicji cyberzagrożenia ujęto w Akcie o cyberbezpieczeństwie: *"oznacza wszelkie potencjalne okoliczności lub zdarzenia, które mogą niekorzystnie wpływać na sieci i systemy informatyczne, ich użytkowników oraz osoby, których zagrożenie to dotyczy"*[199]. Opis ten został de facto powtórzony w *Dyrektywie NIS 2* z 2022 r.

[194] A. Wawrzusiszyn, 2015, *Bezpieczeństwo. Strategia. System. Teoria i praktyka w zakresie*. Wydawnictwo Difin SA, Warszawa, s. 34.
[195] J. Bralczyk, 2005, *Słownik 100 tysięcy potrzebnych słów,* Wydawnictwo PWN, Warszawa.
[196] B. Kaczmarczyk, 2014, *Bezpieczeństwo i zagrożenia w teorii oraz praktyce,* Wydawnictwo SAPSP, Kraków, s. 69.
[197] Ibidem, s. 67.
[198] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560 z późn. zm.)., art. 1.
[199] 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), art. 2.

Wyzwaniem cyberbezpieczeństwa będzie sytuacja problemowa w dziedzinie cyberbezpieczeństwa, stwarzana przez szanse i/lub ryzyka oraz dylematy decyzyjne, przed jakimi jest podmiot w uzgadnianiu spraw cyberbezpieczeństwa[200].

Cyberzagrożenia najczęściej przybierają postać cyberprzestępstw, cyberterroryzmu czy incydentów o różnym poziomie istotności zgodnie z KSC.

Jeden z podziałów zagrożeń - tendencji w cyberprzestępczości ujęto w Komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów KOM(2007) 267 dotyczącym ogólnej strategii zwalczania cyberprzestępczości[201]. Pierwszą kategorię zagrożeń stanowią przestępstwa tradycyjne w sieciach. Łączność elektroniczna „pozwala" na popełnianie większości przestępstw takich, jak: kradzież tożsamości, *phishing*, złośliwe kody czy spam. Kolejną stanowi także nielegalny międzynarodowy handel internetowy (broń, narkotyki, zagrożone gatunki zwierząt) oraz nielegalne treści. W sieci dostępnych jest stale coraz więcej portali zawierających nielegalne treści (np. materiały z wykorzystywaniem seksualnym dzieci, zachęcaniem do aktów terrorystycznych, propagowanie przemocy, terroryzmu czy rasizmu). Reagowanie na tego typu sytuacje jest niezwykle trudne, z uwagi na fakt administrowania i sterowania portalami często poza UE. Strony internetowe mają nieograniczone prawie możliwości sprawnego przemieszczania się pomiędzy państwami, zaś definicje tego, co jest nielegalne, w różnych państwach bywają różne. Ostatnią kategorię stanowią przestępstwa typowe dla sieci łączności elektronicznej. Ataki na masową skalę kierowane są często za pośrednictwem tzw. botnetów (grupa komputerów zainfekowana złośliwym oprogramowaniem i pozostająca pod jednolitą zdalną kontrolą) przeciwko osobom prywatnym, organizacjom i bezpośrednio systemom informatycznym. Coraz powszechniej notowane są także ataki na infrastrukturę krytyczną państwa. Celem takich ataków jest przede wszystkim wymuszanie. Zdarza się, iż liczba zgłaszanych ataków jest zaniżona, ponieważ upublicznienie takich informacji (luki, problemy z bezpieczeństwem) mogłoby przynieść przedsiębiorstwom straty[202].

Statystyki podmiotów zajmujących się szeroko rozumianym cyberbezpieczeństwem wskazują, że stale wzrasta liczba przestępstw informatycznych, zaś działania przestępcze są coraz bardziej złożone i wykraczające poza granice państw. Istnieją wy-

[200] Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, s.8.
[201] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM (2007) 267, Bruksela 2007.
[202] Ibidem.

raźne przesłanki, iż obserwuje się udział w cyberprzestępczości zorganizowanych grup przestępczych.

M. Szyłkowska wskazuje podstawowe grupy zagrożeń[203]:

a) wynikające z działalności człowieka:

- celowe (cyberprzestępcy, cyberterroryści, ale i „pozawirtualni" przestępcy, np. kradzież lub uszkodzenie urządzeń);
- niecelowe (nieprzeszkoleni/niefrasobliwi pracownicy);

b) wynikające z niezamierzonych zdarzeń:

- zagrożenia naturalne (katastrofa naturalna, powódź, silny wiatr, susza, epidemia);
- zagrożenia techniczne, wynikające z cywilizacyjnego rozwoju społeczeństwa (awarie chemiczne, pożary, katastrofy komunikacyjne).

Natomiast P. Sienkiewicz wyróżnia zjawiska (zasadnicze rodzaje cyberzagrożeń) mogące zakłócić ład społeczny i prowadzić do powstawania sytuacji konfliktowych, co obrazuje poniższa tabela.

Tab. 4.1

Zasadnicze rodzaje cyberzagrożeń

L.p.	**Zjawisko**	**Opis**
1.	Cyberwojna	Cyberprzestrzeń wykorzystywana do działań politycznych, które realizowane mogą być przez siły zbrojne (skierowane na przeciwnika).
2.	Cyberdemokracja	Cyberprzestrzeń wykorzystywana w polityce zgodnie z zasadami demokracji liberalnej.
3.	Cyberterroryzm	Cyberprzestrzeń wykorzystywana do działań terrorystycznych (tak państwowych, jak i niepaństwowych).
4.	Cyberinwigilacja	Cyberprzestrzeń wykorzystywana do pozyskania informacji (bądź kontroli) nad działaniami obywateli (tzw. efekt *„Big Brother"*).
5.	Cyberprzestępstwo	Cyberprzestrzeń wykorzystywana do dokonania aktów kryminalnych, zorganizowanych na zasoby organizacji bądź osób.

[203] M. Szyłkowska, 2023, *Ochrona cyberprzestrzeni*- materiał w zbiorach autora: Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania WAT, Warszawa.

6.	Cyberprzemoc	Cyberprzestrzeń wykorzystywana do wymuszania odbioru niepożądanych komunikatów, które zawierają informacje (treści, obrazy, dane) sprzeczne z wartościami adresata.

Źródło: opracowanie własne na podstawie: P. Sienkiewicz, 2012, *Bezpieczeństwo cyberprzestrzeni państwa,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Seria Ekonomiczne problemy usług", nr 88, s. 808

Jednym z najbardziej klasycznych podziałów są zagrożenia techniczne oraz zagrożenia nietechniczne (społeczne). Listę zagrożeń technicznych otwierają wirusy[204]:

- wirusy – programy uszkadzające (narażające) inne programy przez dodanie do nich specjalnego kodu celem uzyskania dostępu do zawartości komputera podczas uruchamiania zainfekowanego pliku;
- robaki – rodzaj szkodliwego oprogramowania, które rozprzestrzeniając się wykorzystuje zasoby sieci. Nazwa związana jest z „pełzaniem" oprogramowania z jednego komputera na drugi przy użyciu sieci, poczty elektronicznej czy innych rodzajów komunikacji, stąd tempo rozprzestrzeniania należy do najszybszych;
- *kruegerapps / kruegerware* – złośliwe oprogramowanie, którego nazwa pochodzi od Kruegera Freddy'ego, postaci filmu „Koszmar z ulicy Wiązów" i tym samym nawiązuje do zdolności i możliwości powracania do istnienia. Tego typu wirusy odradzają się nawet po czasie usunięcia z komputera (np. po skorzystaniu z opcji odzyskiwania systemu). Często to określenie dotyczy wirusów komputerowych, *spyware i malware*;
- *spyware* – oprogramowanie szpiegowskie, którego działania opiera się na gromadzeniu danych nt. konkretnej organizacji lub konkretnego użytkownika. Ofiara nie jest świadoma obecności spyware na swoim urządzeniu;
- *browser hijacker* / porywacz przeglądarek – rodzaj złośliwego oprogramowania, które bez wiedzy użytkownika zmienia ustawienia jego przeglądarki internetowej. Może to skutkować przekierowywaniem do niepożądanych stron www, dodawaniem nieproszonych zakładek np. pornograficznych bądź generowaniem niechcianych okienek tzw. *pop-up*. Zadaniem programów antywirusowych jest usuwanie hijackerów;
- *jokes* – oprogramowanie, którego celem jest wystraszenie użytkownika. Komputer wyświetla informacje o uszkodzeniu bądź zainfekowaniu urządzenia, choć w rzeczywistości taka sytuacja nie ma miejsca;

[204] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne [dostęp 15.08.2022 r.].

- *riskware* – oprogramowanie zawierające potencjalne zagrożenie, w niektórych przypadkach oznacza zagrożenie dla zapisanych danych;
- *poachware* – z j. angielskiego *„to poach”* – nielegalnie polować, kłusować. To oprogramowanie szpiegowskie mające na celu zdobycie wrażliwych danych np. hasła czy nazwy użytkownika;
- *malware – „malicious software”* – złośliwe oprogramowanie, które uszkadza komputer lub zapisane na nim informacje. Pod pojęciem malware mieszczą się robaki, wirusy, spyware, konie trojańskie, nieuczciwe oprogramowanie zwane adware i inne;
- konie trojańskie tzw. trojany – programy wykonujące niekontrolowane przez użytkownika działania np. mogą usuwać dane z dysku, wykradać prywatne dane czy powodować przerwy w działaniu systemu;
- *trojan dropper* – rodzaj trojana, który instaluje złośliwy kod na komputerze ofiary, często jest to aktualizacja już istniejącego złośliwego kodu;
- *trojan clicker* – rodzaj trojana, którego zadaniem jest informowanie autora działania o tym, iż kod został zainstalowany na komputerze ofiary. Ponadto, trojan clicker przekazuje informacje dotyczące aktywności użytkownika w zakresie np. odwiedzanych portali, używanych adresach mailowych itp.;
- *trojan downloader* – działa na podobnych zasad jak *trojan dropper*, jednak jest znacznie mniejszy niż on oraz można go wykorzystywać do pobierania niezliczonych ilości nowych wersji szkodliwego kodu;
- *trojan proxy* – trojan, który monitoruje i śledzi aktywność użytkownika, po czym wysyła zapisane na dysku dane do autora działania. Gromadzone są informacje dotyczące sekwencji wciskanych klawiszy, odwiedzanych stron czy zapisywanych haseł, co wykorzystywane jest do kradzieży bankowych czy oszustw internetowych;
- *trojan backdoor* – trojan instalowany i działający w ukryciu, bez wiedzy i zgody użytkownika. Pomaga osobie kontrolującej na zarządzanie komputerem ofiary;
- *crimeware* – program szpiegujący, którego celem jest gromadzenie poufnych danych użytkownika, co umożliwia uzyskanie dostępu do usług finansowych czy danych bankowych;
- *bundleware* – jest to sposób dystrybuowania oprogramowania, które dołączone jest do innego popularnego programu. Tym samym rozpowszechniane są programy szpiegujące, zaś nieświadomi zagrożenia użytkownicy sami przeprowadzają ich instalację;

- atak typu *DoS* – jeden z rodzajów ataków sieciowych, który zakłóca prawidłowe działanie systemu. Zakłócenie może dotyczyć defektu wybranej usługi internetowej (np. korzystania z poczty e-mail) bądź całego serwera. Przy tego rodzaju atakach wykorzystywane są błędy i luki, które występują w systemie. Atak nie wiąże się z kradzieżą czy utratą danych, ale poprzez blokowanie usług przynosi straty firmom, które nie działają w tym czasie optymalnie;
- atak typu *DDoS* – rodzaj zaawansowanego (zmasowanego) ataku hakerskiego, którego celem jest paraliż sieci i podłączonych do niego systemów komputerowych. Działanie opiera się na obciążeniu zasobów sztucznie generowanymi zapytaniami;
- *rootkit* – narzędzia, które wykorzystuje się do ukrywania złośliwego działania. To złośliwe oprogramowanie działa w taki sposób, aby aplikacje antywirusowe nie mogły ich wykryć;
- *spam* – niepożądana, anonimowa korespondencja pocztowa. Spam bywa wiadomością propagandową bądź polityczną, która zawiera prośby o pomoc. Może być także wiadomością oferującą wygranie ogromnej sumy pieniędzy, zaś maile służą kradzieży numerów kart kredytowych i haseł;
- *tabnapping* – z j. angielskiego *„tabnapping”* – jest to porywanie zakładek. *Tabnapping* to rodzaj ataku typu phishing, wykorzystujący fakt otwierania dużej ilości stron w wielu zakładkach przeglądarki. Atak skupia się na tym, iż witryna atakująca zmienia zawartość (podmienia) innej strony, która znajduje się w innej zakładce przeglądarki. W sytuacji, gdy podmienianą w tle stroną jest strona banku, użytkownik może nieumyślnie zalogować się na podszywającą się witrynę (spreparowaną stronę), która przechwyci hasło do konta bankowego;
- *vishing* – oszuści wykorzystują telefonię internetową i podszywają się pod instytucje finansowe. Jedną z metod jest np. rozsyłanie spamu z zawartym numerem 0-800, pod którym to odbiorca e-maila powinien dokonać aktualizacji swoich danych bankowych. W momencie wykręcania numeru włączany jest automat, który prowadząc ofiarę krok po kroku w formach próśb - wyłudza konkretne dane;
- *IP spoofing* – jest to przekłamywanie wyjściowego adresu IP, który rozsyłany jest przez pakiet sieciowy. Terminem tym można określić korzystanie z IP innego użytkownika, którego celem jest ukrycie tożsamości atakującego, ingerowanie w aktywność ofiary i stwarzanie pozorów innego użytkownika;

- *hacking* – działania polegające na przełamaniu, omijaniu informatycznego, elektronicznego, magnetycznego zabezpieczenia. Istotą hackingu jest przełamanie zabezpieczeń, które uniemożliwiają dostęp do informacji zawartych w systemie[205].
- *BotNet* – tzw. komputer – zombie, komputer, który pozostaje pod stałą kontrolą hakerów wykorzystujących wirusy, konie trojańskie itp. Statystyki dowodzą, iż 1/3 komputerów w sieci to sprzęt, nad którym kontrolę sprawują hakerzy. Użytkownik komputera-ofiary najczęściej nie jest tego świadomy. Komputery *BotNet'u* wykorzystuje się do przeprowadzania ataków DoS bądź do rozsyłania spamu. Pierwszym krokiem do przeciwdziałania takich sytuacjom jest regularna aktualizacja systemu, programu antywirusowego oraz zapory ogniowej (tzw. *firewall*).

W obszarze zagrożeń nietechnicznych (społecznych) obecny katalog nie jest tak znacznie rozbudowany jak w przypadku zagrożeń technicznych[206]:

- *cyberstalking* – zjawisko złośliwego i natrętnego dręczenia osoby, grupy osób bądź organizacji poprzez wykorzystywanie technologii informacyjnej – szczególnie Internetu. Takiego prześladowcę nazywa się stalkerem;
- *trollowanie* – nieprzyjazne zachowania w stosunku do innych użytkowników sieci, mające na celu rozproszenie prowadzonej dyskusji. Zjawisko to jest częstym w miejscach wymiany myśli, czyli na forach dyskusyjnych, czatach itp.;
- *flaming* – zaognianie wymiany zdań pomiędzy użytkownikami w różnych miejscach w sieci np. na forach, co prowadzić ma do narastania agresji wyrażeń i wypowiedzi;
- cyberprostytucja – uzyskiwanie korzyści materialnych za udostępnianie przy użyciu sieci materiałów pornograficznych lub erotycznych wytworzonych świadomie – samodzielnie – z własnym udziałem. Wymienia się filmy, zdjęcia bądź organizuje się pokazy na żywo przy pomocy kamerek internetowych;
- *seksting* – przesyłanie w sieci swoich filmów, zdjęć bądź wiadomości mających charakter seksualny. Zjawisko to dotyka całej grupy korzystających z Internetu, dzieci, młodzieży oraz dorosłych;
- *grooming* – przestępstwo, które wprowadza w błąd nieletnie dziecko w wieku do lat 15 celem produkcji materiałów pornograficznych bądź składania mu seksualnych propozycji przez sieć.

[205] P. Kozłowska-Kalisz, 2022, *Hacking*, [w:] Kodeks karny. Komentarz aktualizowany, M. Mozgawa (red.), LEX/el., art. 267.
[206] https://www.gov.pl/web/baza-wiedzy/zagroz-nietechniczne-spoleczne [dostęp 15.08.2022 r.].

Inny podział stanowią zagrożenia mieszane. Charakterystycznym dla tego rozróżnienia jest fakt, iż sprawcy ataku wykorzystują jednocześnie zarówno technikę, jak i korzystają z niewiedzy bądź nieświadomości użytkownika. Zagrożenia mieszane w cyberprzestrzeni odnoszą się do sytuacji, w których różne rodzaje ataków cybernetycznych są wykorzystywane jednocześnie lub w zorganizowany sposób, tak aby zwiększyć skuteczność ataku. Te zagrożenia mogą obejmować kombinację różnych technik, takich jak ataki hakerskie, socjotechnika, malware, fałszywe strony internetowe i inne, aby osiągnąć konkretne cele.

Przykładem są ataki przez *IoT (Internet of Things)*, Internet Rzeczy. Dzięki *IoT* można łączyć ze sobą różne urządzenia, tzn. przy użyciu smartfona kontrolować urządzenia domowe niezależnie od miejsca pobytu (kamera w mieszkaniu czy *GPS* w samochodzie). Cyberprzestępca hakując jedno urządzenia, uzyskuje dostęp do pozostałych. Ogromne znaczenie w ostatnich latach nabiera także sztuczna inteligencja *AI (Artificial Intelligence)* i uczenie maszynowe *ML (Machine Learning)*. Oprogramowanie to jest w stanie kodować pewne wzorce, zapisywać je i prognozować na podstawie zdarzeń z przeszłości. Tym samym następuje proces nauczania. Narzędzia te mogą być wykorzystywane zarówno do wysyłania spamu, przeprowadzania ataków hakerskich czy prób phishingu. Skuteczność i efektywność zagrożeń mieszanych może być większa ze względu na oddziaływanie na dwóch kierunkach jednocześnie. Inny przykład to ataki z wykorzystaniem botnetów czy ransomware. Cyberprzestępcy mogą wykorzystywać botnety (sieci zainfekowanych urządzeń) celem przeprowadzenia ataków *DDoS*, podczas gdy w tym samym czasie uruchamiają ataki ransomware na różnych systemach, a prowadzi to do równoczesnego zablokowania dostępu do danych i usług. *Phishing* – metoda oszustwa komputerowego ukierunkowana na podszywanie się pod inną osobę bądź instytucję celem pozyskania korzyści lub wyłudzenia danych (np. szczegółów karty kredytowej lub danych do logowania). Atak ten opiera się na tzw. inżynierii społecznej. Wyróżnia się ponadto tzw. *likejacking* – forma *phishingu*, której założeniem jest gromadzenie fanów przez „polajkowanie" danej strony lub profilu na Facebooku. Dzieje się tak np. gdy użytkownik „kuszony" jest treścią na profilu swojego znajomego (np. o treści erotycznej). Po kliknięciu w link nie ma jednak obiecywanej zawartości, zaś przeniesienie do strony, która powoduje automatycznie „polubienie" jej przez użytkownika bez jego zgody i wiedzy. Co więcej, ta sama atrakcyjna treść pojawia się na profilu właśnie „złapanego" użytkownika. Dzięki temu spam rozprzestrzenia się w nie-

bywałym tempie. Częstokroć docelowa strona zawiera także szkodliwe oprogramowanie typu wirusy, trojany itp.

Zagrożenia mieszane stanowią zdecydowane wyzwanie dla organizacji i wymagają holistycznego podejścia do bezpieczeństwa cybernetycznego, obejmującego tak techniczne środki obronne, jak i edukację pracowników oraz świadomość ryzyka.

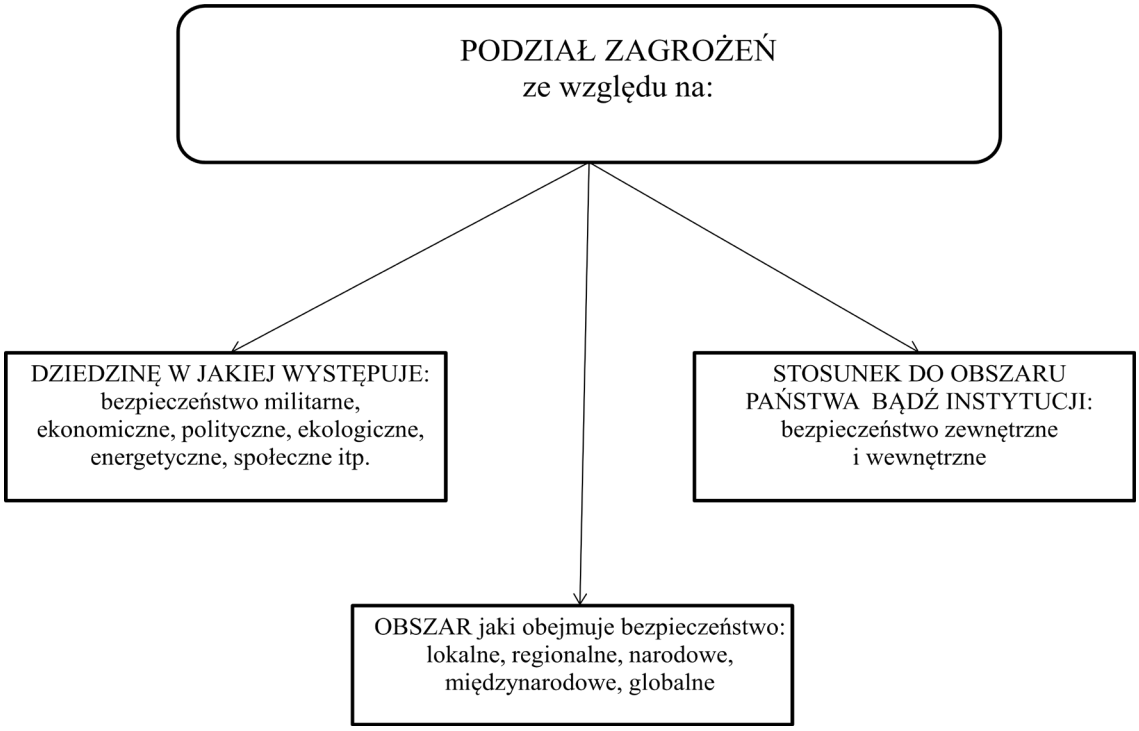
Według statystyk *CSIRT NASK*, *phishing* stanowi najczęściej stosowaną metodę – próbę zyskania tzw. pierwszego dostępu do atakowanego urządzenia (systemu). Specjaliści wykorzystują coraz bardziej nowoczesne i zaawansowane metody ataku, zaś ich ukierunkowane bezpośrednio działania oddziałują skutecznie na zmęczonego użytkownika. Obecnie obserwuje się wzrost aktywności w zakresie tzw. phishingu zgody. Polega to na wykorzystywaniu przez hakerów przyzwyczajenia użytkowników do klikania w linki, które prowadzą do dalszej części określonej informacji. Podczas dokonania wyboru poprzez zaznaczenie i kliknięcie/wciśnięcie opcji: „zgadzam się" bądź po prostu: „dalej", użytkownik nieświadomie staje się ofiarą przejęcia kontroli nad jego systemem czy zasobami.

Podstawowa grupa zagrożeń nietechnicznych (społecznych) to wykorzystywanie ludzkich błędów i zachowań za pomocą technik i narzędzi socjotechnicznych.

Zbliżoną koncepcję podziału zagrożeń podaje prof. Ryszard Tadeusiewicz, którego zdaniem istnieją dwa zasadnicze rodzaje zagrożeń, a mianowicie zagrożenia techniczne oraz zagrożenia związane z działalnością człowieka. Tak więc źródłem zagrożeń w cyberprzestrzeni mogą być: technika albo ludzie. Zagrożenia techniczne są rzeczywiście poważne, ale czy najpoważniejsze? Awaria komputera jest w stanie unieruchomić działalność instytucji, pozbawiając tym samym spodziewanych zysków i rosnącego prestiżu. Jednak we właściwie zbudowanej organizacji pewne systemy powinny być zdublowane. Awaria komputera roboczego jest przyczynkiem do przejęcia zadań przez komputer zapasowy, co ewentualnie może skutkować obniżeniem wydajności (zapasowy ma częstokroć mniejszą moc obliczeniową). Inne zagadnienie stanowi bezpieczeństwo danych. Dane zgromadzone w pamięci komputera stanowią większą wartość aniżeli komputer jako taki. Na skutek awarii technicznej (np. fizyczne uszkodzenie dysku) dane te mogą zostać utracone – poprzez wadliwe oprogramowanie bądź błędne działanie ludzi obsługujących system. Przed takim rodzajem uszkodzenia danych chronić się można stosując macierz dyskową *RAID*. Dla zabezpieczenia danych należy wykorzy-

stywać kopie bezpieczeństwa tzw. *backup-y*. Wyróżnia się następujące rodzaje kopii zapasowych: kopie pełne, kopie przyrostowe, kopie różnicowe[207].

Bez wątpienia kopie pełne dają możliwość najszybszego odzyskania sprawności systemu po awarii, jednak są najbardziej kłopotliwe w sporządzaniu. W pozostałych przypadkach odzyskanie danych jest coraz bardziej problematyczne. Co więcej, w sferze zagrożeń technicznych istnieją także zagrożenia związane z utratą zasilania. Kluczowe systemy informatyczne powinny być, a wręcz muszą być niezależne od wszelkich awarii sieci energetycznej i muszą posiadać awaryjne zasilanie. Awaryjne zasilanie w rozumieniu układów UPS bądź generatorów spalinowych napędzających prądnicę, co pozwoliłoby na dłuższy czas autonomicznej pracy[208].



Rys. 4.1. Podział zagrożeń wg wybranych kryteriów (źródło: opracowanie własne na podstawie: R. Tadeusiewicz, *Zagrożenia*…, op. cit., s. 39)

Europejska Agencja ds. Cyberbezpieczeństwa (*ENISA*) corocznie publikuje raport dotyczący zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych: *ENISA Threat Landscape.* Poniżej wyszczególniono osiem najpoważniejszych zagrożeń wskazanych przez *ENISA*[209]:

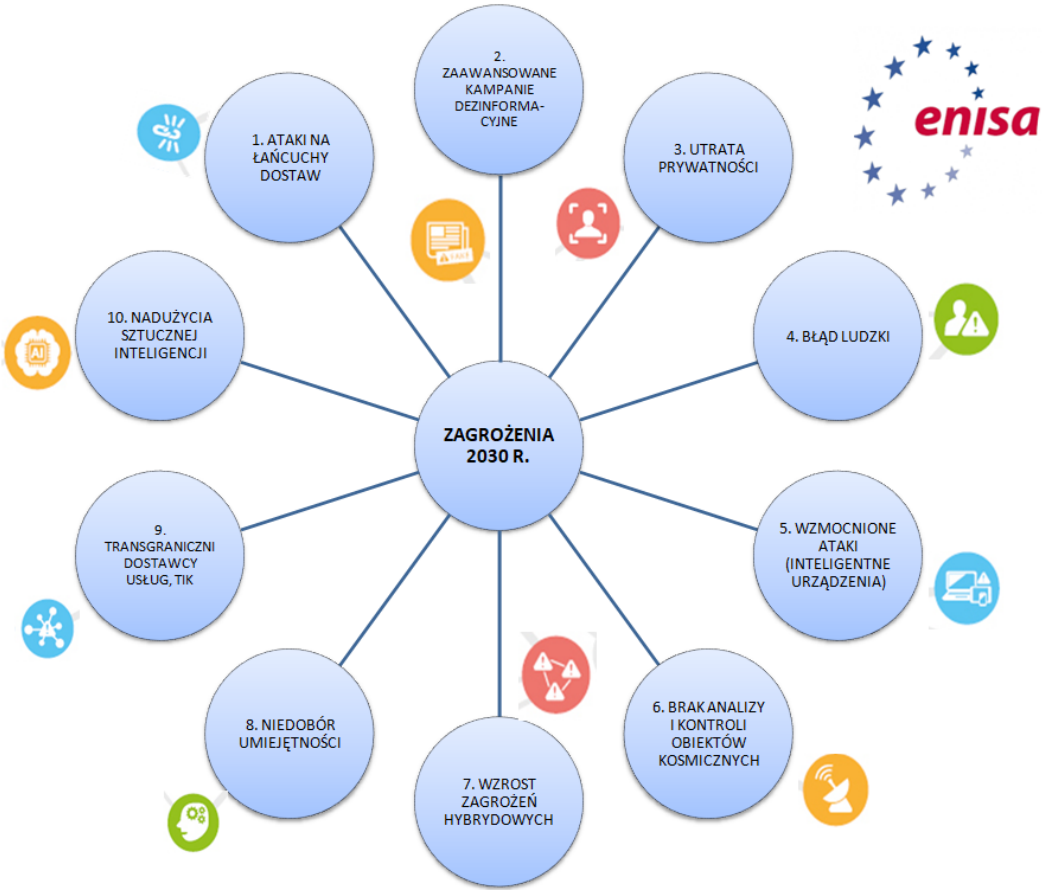
1. *Ransomware* (ataki przy pomocy złośliwego oprogramowania na sieci i blokowanie danych w celu żądania okupu);

[207] R. Tadeusiewicz, *Zagrożenia…,* op. cit., s. 36-37.
[208] Ibidem, s. 38.
[209] https://www.traple.pl/raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa-dotyczacy-zagrozen-dla-bezpieczenstwa-informacji-z-2022-r/ [dostęp 21.08.2023 r.].

2. *Malware* (złośliwe oprogramowanie);
3. Socjotechnika (inżyniera społeczna, wykorzystanie ludzkiego błędu, manipulacji);
4. Ataki na bazy danych bądź same dane (naruszenie danych, wyciek danych);
5. Zagrożenia dla integralności i dostępności danych (np. ataki DDoS - blokowanie dostępu do usług przez sztuczne generowanie dużej ilości zapytań - wzmożonego ruchu w sieci);
6. Zagrożenia dostępności Internetu, związane z e-mailami - pocztą elektroniczną;
7. Dezinformacja – dystrybuowanie fałszywych wiadomości;
8. Ataki na łańcuchy dostaw (ataki na relację między dostawcą a organizacją).

Ponadto, *ENISA* zidentyfikowała 10 najważniejszych zagrożeń dla cyberbezpieczeństwa, które najprawdopodobniej pojawią się do 2030 r. Identyfikacja jest wynikiem 8-miesięcznego badania prognostycznego. Przy wsparciu grupy ekspertów, sieci *CSIRT* oraz ekspertów *EU CyCLONe*, agencja przeprowadziła *burzę mózgów* podczas warsztatów kształtujących identyfikację zagrożeń, tak aby znaleźć rozwiązania dla pojawiających się wyzwań w perspektywie roku 2030. Ćwiczenie wskazuje, że uszeregowane i zidentyfikowane zagrożenia są bardzo zróżnicowane i obejmują te, które mają ważne znaczenie dzisiaj. Dzisiejsze zagrożenia będą stale wymagały reakcji, ponieważ zmieniły już swój charakter. Zauważono również, że istotny czynnik zmian stanowi wzrost zależności i popularyzacja rozwijających się nowych technologii. Wymienione czynniki zwiększają trudność zadania, a tym samym sprawiają, że zrozumienie cyberzagrożeń staje się coraz większym wyzwaniem. Zastosowana analiza prognostyczna jest podstawową techniką, która pozwala ocenić, w jaki sposób zagrożenia najprawdopodobniej będą ewoluować. Wnioski z ćwiczenia mają służyć jako podstawa i zachęta do podjęcia pewnych działań[210].

[210] https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [dostęp 02.05.2023 r.].



Rys. 4.2. 10 najważniejszych cyberzagrożeń do 2030 roku (źródło: opracowanie własne na podstawie: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030- [dostęp 02.05.2023 r.])

Analizując poszczególne zagrożenia, można wskazać ich faktory[211]:

1. Ataki na łańcuchy dostaw w zakresie zależności oprogramowania. Bardziej złożone komponenty i usługi pochodzące od dostawców oraz partnerów zewnętrznych doprowadzić mogą do powstania nieprzewidzianych i nowych luk w zabezpieczeniach, powodujących konflikt po stronie dostawcy i klienta.
2. Zaawansowane kampanie dezinformacyjne. Ataki typu deepfake manipulować mogą społecznościami z przyczyn (geo)politycznych i finansowych.
3. Wzrost autorytaryzmu nadzoru cyfrowego / utrata prywatności. Nadzór cyfrowy na platformach internetowych, rozpoznawanie twarzy, magazyny danych o tożsamości cyfrowej stać się mogą celem dla cyberprzestępców.
4. Błąd ludzki i wyeksploatowane systemy komputerowe w ramach ekosystemów cyberfizycznych. Szybkie przyjęcie Internetu Rzeczy, konieczność modernizacji starszych systemów i stały niedobór umiejętności prowadzić mogą do braku wiedzy, szkoleń, a także zrozumienia ekosystemu cyberfizycznego, co natomiast może prowadzić do problemów z bezpieczeństwem.

[211] https://www.enisa.europa.eu/news/foresight_2030_infographic.png- [dostęp 03.05.2023 r.].

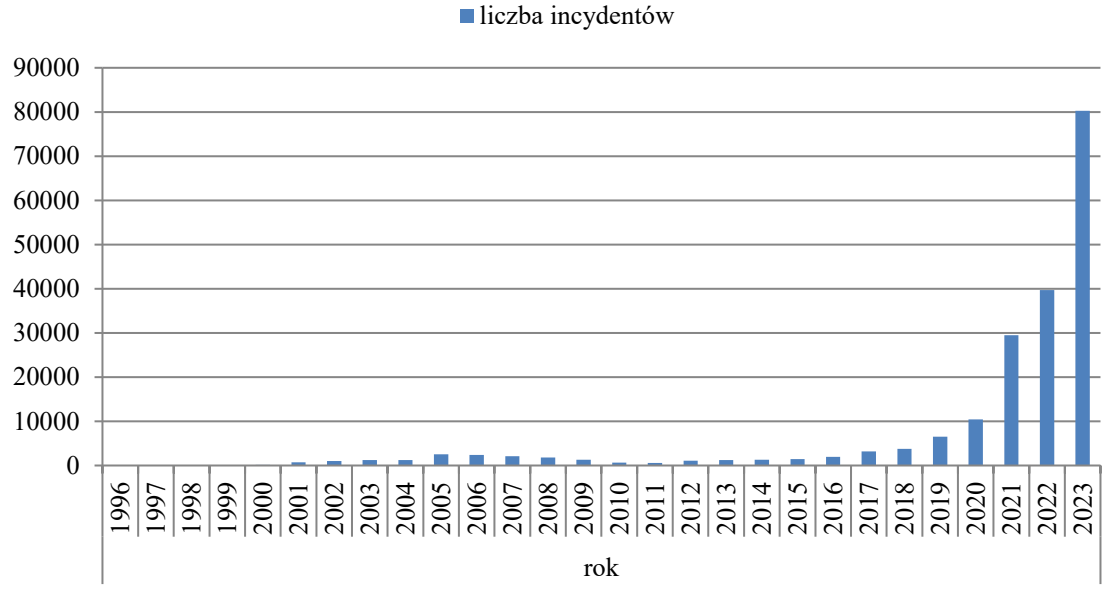
5. Wzmocnione ataki, ukierunkowane przez dane pochodzące z inteligentnych urządzeń. Dzięki tym danym, uzyskanym z podłączonych do Internetu urządzeń, osoby atakujące uzyskać mogą dostęp do informacji, celem przeprowadzenia dostosowanych i bardziej złożonych ataków.
6. Brak wystarczającej analizy i kontroli infrastruktury oraz obiektów kosmicznych. Ze względu na krzyżowanie się publicznej i prywatnej infrastruktury w przestrzeni kosmicznej zbadać należy bezpieczeństwo nowych technologii i infrastruktur, ponieważ brak zrozumienia infrastruktury kosmicznej narazić ją może na większe podatności ataków i przestojów.
7. Wzrost zaawansowanych zagrożeń hybrydowych. Ataki fizyczne lub offline stale ewoluują i są często łączone z cyberatakami biorąc pod uwagę wzrost liczby inteligentnych urządzeń, stosowanie chmurę, tożsamości online oraz platform społecznościowych.
8. Niedobór umiejętności. Brak zdolności oraz kompetencji spowodować może, że grupy cyberprzestępcze wezmą za cel organizacje o największych lukach w umiejętnościach i najsłabszej dojrzałości.
9. Transgraniczni dostawcy usług technologii informacyjnych i komunikacyjnych jako pojedynczy punkt awarii. Sektor *ICT* łączący usługi krytyczne, takie, jak: sieci elektryczne, transport i przemysł, świadczący usługi w skali transgranicznej, stać się może celem następujących technik: backdoory, odmowa świadczenia usług, manipulacja fizyczna, a także zostać wykorzystany jako środek bojowy w czasie potencjalnego konfliktu.
10. Nadużycia sztucznej inteligencji. Negatywne działania takie, jak: tworzenie fałszywych treści, dezinformacji, wykorzystywanie stronniczości czy zbieranie wrażliwych danych mogą być wzmacniane przez manipulację algorytmami *AI*.

Rozważając powyższe przykłady zagrożeń wraz z ich czynnikami można założyć, iż metody pozostaną zbliżone do tych obecnie stosowanych. Zmienione mogą być ewentualnie formy, jednak stale bazujące przede wszystkim na roli człowieka w sieci. W związku z powyższym, ponownie szczególnie istotna okazuje się być odporność na ataki socjotechniczne i świadomość, którą stale należy budować i rozwijać. Niezwykle trudne u użytkowników będzie najprawdopodobniej połączenie korzystania z nowych technologii i możliwości z jednoczesnym bezpiecznym i umiejętnym podejściem do tych obszarów.

4.2. Analiza wybranych statystyk zagrożeń dla instytucji, podmiotów i organizacji w kontekście rodzajów cyberzagrożeń i skali ich występowania

W niniejszym podrozdziale autor skupił się na statystykach prowadzonych przez: *CERT Polska* (czyli *CERT NASK*), *CERT Orange Polska, ENISA* oraz *International Business Machines (IBM)*. Autor zebrał raporty na przestrzeni lat i stworzył wizualizacje przedstawiające rozwój zagrożeń na ich przestrzeni. Nawiązując do poprzedniej części pracy, ogólnie rzecz przyjmując, można stwierdzić, że zagrożenie to okoliczności, w których podmiot spotyka się z pewną niebezpieczną sytuacją, czynnikiem lub stanem, które obniżają poziom stabilności lub jakości jego dalszego rozwoju i bytu[212].

Jednym z najpopularniejszych incydentów w ostatnich latach jest *phishing*, czyli wyłudzenie danych. Wykorzystuje błąd, naiwność lub właśnie brak świadomości użytkownika. Jakie skutki mogą wywołać takie zagrożenia? Autor postarał się je zidentyfikować i opisać.

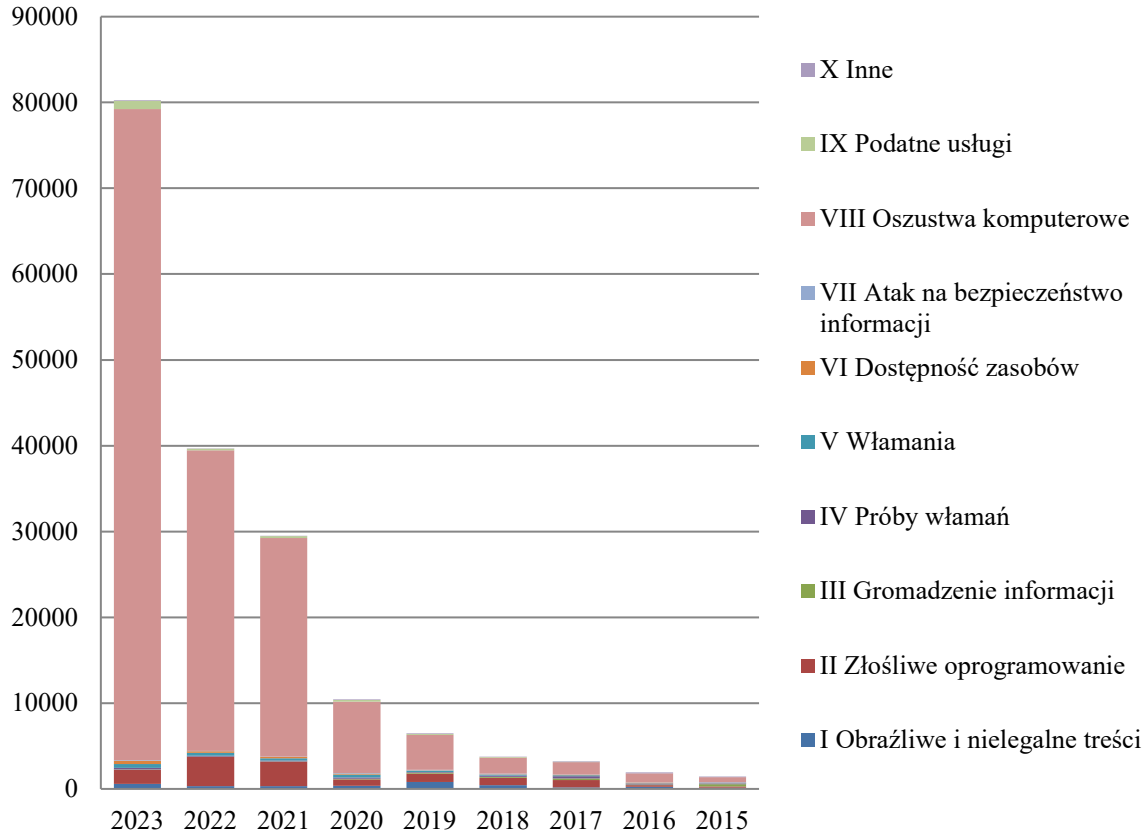


Wykres 4.1. Liczba incydentów obsłużonych przez *CERT Polska* na przestrzeni lat (źródło: opracowanie własne na podstawie Raport roczny z działalności *CERT Polska* [1996-2023])

Sukcesywnie rokrocznie *CERT Polska* rejestruje coraz więcej zgłoszeń oraz incydentów cyberbezpieczeństwa. W roku 2021 *CERT Polska* zarejestrował ponad 115 tys. zgłoszeń. Spośród wszystkich zgłoszeń specjaliści wytypowali ok. 65 tys., na podstawie których zarejestrowano łącznie 30 tys. unikalnych incydentów cyberbezpieczeń-

[212] M. Bańko (red.), 2000, *Inny słownik języka polskiego*, Wydawnictwo Naukowe PWN, Warszawa, s. 12-13.

stwa. Ogromny wzrost w ostatnich latach związany jest z pandemią *COVID-19* i transferem wielu usług a także aktywności do sieci. W roku 2022 odnotowano ogromny wzrost zgłoszeń, ponieważ ponad 322 tys.! Wytypowano 115 tys. zgłoszeń, spośród których łącznie blisko 40 tys. uznano za unikalne incydenty cyberbezpieczeństwa. Dane z roku 2023 wskazują na blisko 375 tys. zgłoszeń, z czego 80 tys. stanowią unikalne incydenty. Obserwowany jest stały wzrost, którego nie należy łączyć jedynie z negatywnymi zdarzeniami. Wzrost spowodowany jest również tym, iż wzrasta świadomość istnienia zespołu *CERT Polska*, czego przykładem są kampanie społeczne w telewizji i radiu informujące m.in. o zagrożeniach oraz sposobach zgłaszania takich sytuacji do zespołu.



Wykres 4.2. Liczba incydentów we wszystkich kategoriach obsłużonych przez *CERT Polska* na przestrzeni lat (źródło: opracowanie własne na podstawie Raport roczny z działalności *CERT Polska* [2015-2023])

CERT Polska odnotował znaczący wzrost obsłużonych incydentów, jest to poziom 182 % w porównaniu do roku poprzedniego. Należy przypomnieć, że w 2020 roku *CERT Polska* obsłużył ponad 10 tys. unikalnych incydentów cyberbezpieczeństwa (w roku 2023: 80 tys.).

Najpopularniejszym typem incydentów w 2023 roku był *phishing* – stanowiący aż blisko 52 % wszystkich incydentów. Liczba incydentów zaklasyfikowanych jako *phishing* (w kategorii oszustwa komputerowe) w porównaniu do 2020 roku wzrosła o 196 % i osiągnęła wartość około 41 tys. incydentów. Tak samo, jak poprzednio, fundamentalne znaczenie na zwiększenie liczby zarejestrowanych incydentów (*phishingowych*) miała wprowadzona w marcu roku 2020 Lista Ostrzeżeń przed niebezpiecznymi stronami. Najpopularniejszym *phishingiem* w roku 2023 było podszywanie się pod użytkowników serwisu aukcyjnego Allegro (11 tys. incydentów), *social media*, tj. pod serwis społecznościowy Facebook – blisko 5 tys. incydentów.

Drugie miejsce przypadło kategorii oszustwa komputerowe. Zgromadzono informacje nt. 34 tys. incydentów stanowiących ponad 42 % wszystkich zarejestrowanych incydentów. W roku 2022 miejsce to stanowiło szkodliwe oprogramowanie. Tego typu zdarzeń w 2022 roku odnotowano blisko 3,5 tys. W 2021 roku zarejestrowano prawie 3 tys., co stanowi 9,66 % wszystkich obsłużonych incydentów. Wartość ta w porównaniu do 2020 roku wzrosła o 281 %!

Trzeci typ incydentów pod względem liczby zidentyfikowanych zdarzeń wg *CERT Polska* przypada szkodliwemu oprogramowaniu. Rok 2023 to 1650 przypadków, tak więć o połowa mniej niż w roku poprzednim. Tego typu zdarzeń w 2022 roku odnotowano blisko 3,5 tys. W 2021 roku zarejestrowano prawie 3 tys., co stanowi 9,66 % wszystkich obsłużonych incydentów. Wartość ta w porównaniu do 2020 roku wzrosła o 281 %!

Ostatnie miejsce na podium w rankingu liczby zarejestrowanych incydentów (w roku 2022) wskazano włamaniom m.in. do systemów informatycznych i kont pocztowych – 354 incydenty stanowiące 0,89 % wszystkich incydentów. Natomiast w 2021 roku ostatnie miejsce na podium to kategoria obraźliwych i nielegalnych treści, w tym spamu. Odsetek tego rodzaju incydentów wyniósł 1,05 %. Niewielki procent wynika z tego, iż do jednego incydentu *CERT Polska* często przypisuje nie jedno, a wiele zgłoszeń. Jest to mocno zauważalne dla tej kategorii incydentów, w której za 311 incydentów odpowiadało blisko 25 tys. (aż) zgłoszeń. Ponadto, incydenty z kategorii nielegalnych i obraźliwych treści są obsługiwane przez przeznaczony do tego zespół Dyżurnet.pl, działający w strukturach NASK. Jednym z bardziej popularnych obsługiwanych tego typu incydentów były ataki tzw. *sextortion scam* (masowe rozsyłanie wiadomości mailowych zawierających informację o rzekomym przejęciu kontroli urządzeń ofiary, a także posiadaniu przez sprawcę (nadawcę) materiałów upokarzających, prezentują-

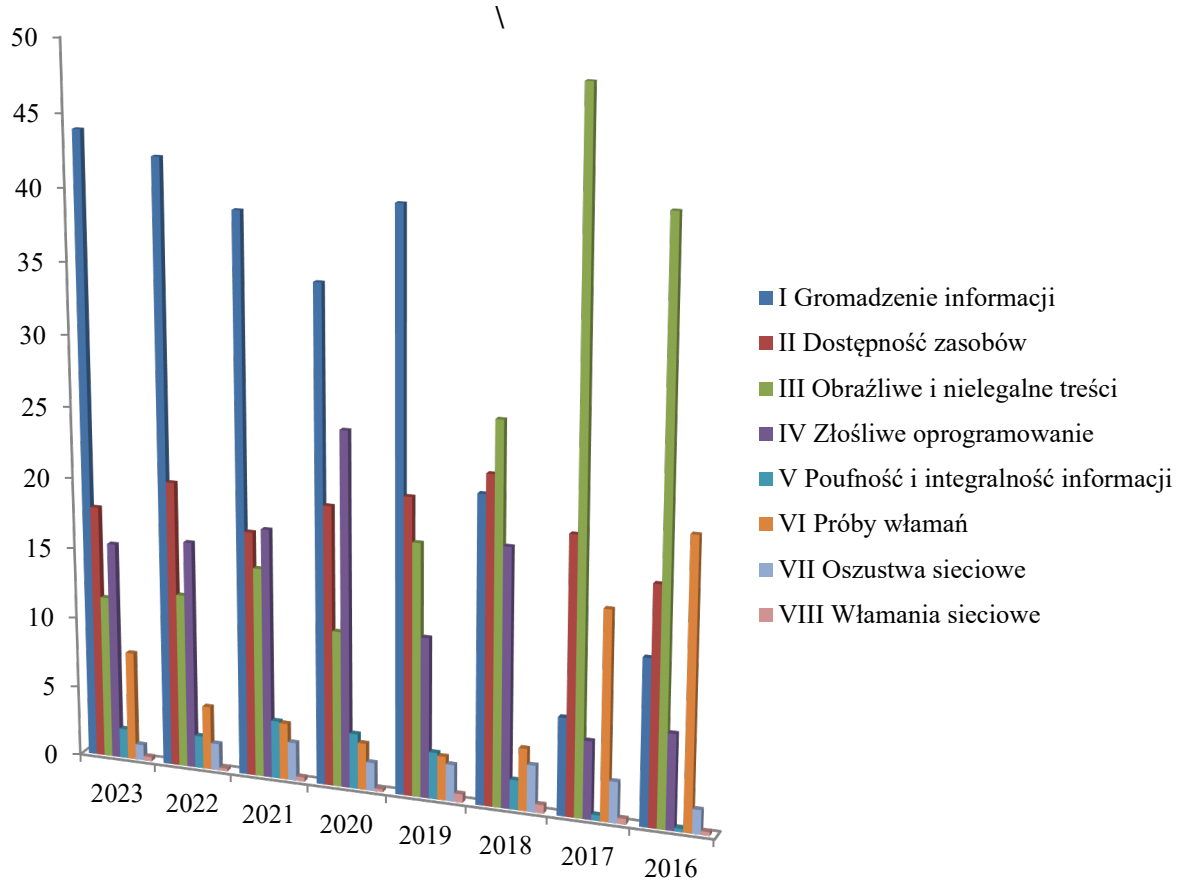
cych ofiarę w kontekście erotycznym). To rodzaj szantażu, ponieważ za zapłacenie żądanego okupu, przestępca oferuje skasowanie kompromitujących materiałów.

CERT Polska rejestruje incydenty i przypisuje je do odpowiednich sektorów, których dotykają. Pierwszy, pod względem ilości zarejestrowanych incydentów stanowi sektor handlu hurtowego oraz detalicznego. W tym sektorze w roku 2021 zarejestrowano 17,38 % wszystkich incydentów, co stanowi liczbę 5 tys. incydentów (rok później ok. 5,5 tys., zaś rok 2023 to już blisko 20 tys. incydentów). Dział ten obejmuje m.in. incydenty w sklepach internetowych oraz serwisach aukcyjnych. Podobnie, jak w mediach, w tym przypadku również incydenty typu *phishing* stanowią miażdżącą przewagę wszystkich incydentów, jest to bowiem 89,17 %.

Tuż za nim sklasyfikowano infrastrukturę rynków finansowych, blisko 19 tys. zdarzeń. Specjaliści zespołu w 2023 roku zarejestrowali łącznie ponad 10 tys. incydentów, które wystąpiły w sektorze o nazwie: *media* (w roku 2022 to ponad 7 tys. incydentów), trzecia lokata w opisywanym podziale. Ta liczba daje około 12 % wszystkich zarejestrowanych incydentów. Co więcej, gałąź ta obejmuje m.in. incydenty występujące w prasie, telewizji czy tzw. social mediach. Wśród wszystkich incydentów przydzielonych do sektora media, przeważająca ich część, czyli 91,73 % to incydenty typu *phishing*.

W porównaniu do poprzednich lat, media zajmowały pierwszą lokatę, zaś rok 2023 jest przełomowy, ponieważ zmiana prowadzenia przypadła sektorowi handel hurtowy, detaliczny oraz infrastruktura rynków finansowych.

Co łatwo zauważyć, na przestrzeni lat *phishing* pozostaje niezwykle częstym i poważnym zagrożeniem. Faktem jest, iż jego zastosowanie przybiera coraz to nowe formy. Ponadto, złośliwe oprogramowanie ciągle jest wysoko w hierarchii cyberzagrożeń, co oznacza, że użytkownik sieci stale powinien korzystać z programów antywirusowych, zapór i innych rodzajów zabezpieczeń.



Wykres 4.3. Procentowy rozkład liczby incydentów we wszystkich kategoriach obsłużonych przez *CERT Orange Polska* na przestrzeni lat (źródło: opracowanie własne na podstawie Raport roczny z działalności *CERT Orange Polska* [2016-2023])

Nieco inne ujęcie zagrożeń sieciowych znaleźć można w klasyfikacji incydentów wg *CERT Orange Polska*. Incydenty z kategorii „gromadzenie informacji" w roku 2021 i 2022 stanowiły najliczniejszą grupą obsłużonych incydentów (39,2 oraz 42,4 % wszystkich). Rok 2023 to ponownie wzrost, choć nieznaczny, ponieważ o 1,5 pp. (43,9 %). Składają się na nią przede wszystkim przypadki *phishingu* i skanowania portów. Tego typu zagrożenie to najczęściej istotny element bardziej zaawansowanych ataków, mających na celu oszustwa finansowe czy kradzież informacji.

Incydenty klasy „dostępność zasobów" (drugie miejsce) to przede wszystkim przypadki ataków *DDoS - Distributed Denial of Service*. Incydentów o takiej charakterystyce odnotowano w roku 2021 na poziomie 17,3, rok później 20,2 %, zaś w 2023 roku: 17,9 %.

Na grupę incydentów „złośliwe oprogramowanie" składają się głównie przypadki infekcji (m.in. infekcji oprogramowaniem złośliwym typu *trojan*, *ransomware*), *ho-*

stowanie złośliwych stron i *hostowania* serwerów kontrolujących w sposób zdalny sieć zainfekowanych komputerów.

„Obraźliwe i nielegalne treści" znajdujące się poza „podium", to w znacznej mierze przypadki dotyczące rozsyłania spamu. Pozostałe typy incydentów stanowią m. in. sytuacje dotyczące naruszeń praw autorskich (np. piractwo), a także rozpowszechniania informacji zabronionych prawem (np. pornografia dziecięca, treści rasistowskie, czy zawierające przemoc). W 2021 roku odnotowano 14,8 %, natomiast w 2022: 12,3 % tego typu przypadków. Rok 2023: 11,5 %.

W obszarze „poufność i integralność informacji" znajdują się przypadki nieautoryzowanego (nielegalnego) dostępu do informacji oraz zmiany bądź usunięcia zbiorów informacji. W roku 2021 zanotowano 4,1 % (2022: 2,3 %) tego typu przypadków. Rok później 1,9 %, a w 2023 roku: 1,1%. Niewielki procent nie oznacza niewielkiego zagrożenia, bowiem w praktyce zdarzenia te dotyczą poważnych problemów związanych z wyciekiem danych czy informacji.

Kategoria „próby włamań" zawiera przypadki usiłowania przełamania zabezpieczeń poprzez wykorzystanie podatności systemowych, jego komponentów albo całych sieci i prób logowania do systemów dostępowych lub usług (zgadywanie haseł), które ma na celu stworzenie dostępu do systemów bądź przejęcia nad nim pełnej kontroli. Incydentów o takim zabarwieniu było 4,0 % w 2021 roku, w następnym: 4,5% i w 2023 roku: 7,7 %, co stanowi wzrost o 3,2 pp. w stosunku do roku 2022.

W kategorii „oszustwa sieciowe" sklasyfikowane zostały głównie przypadki nielegalnego (nieuprawnionego) używania nazwy innego podmiotu, nieautoryzowanego użycia zasobów. Zdarzenia te stanowiły w roku 2021: 2,7 % oraz w 2022: 1,9 %, zaś w 2023 roku: 2,1 % wszystkich incydentów. Oszustwa sieciowe dotyczyły głównie ataków o charakterystyce podszywania się pod najbardziej znane i cenione marki, ale także instytucje w kampaniach *phishingowych* czy złośliwego oprogramowania.

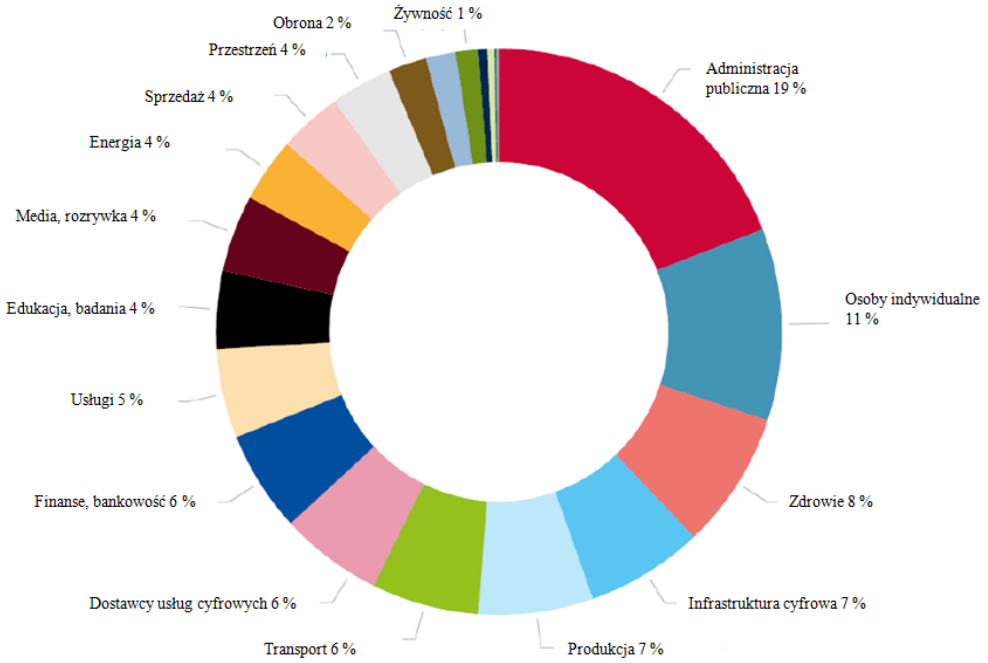
W obszarze włamań sieciowych, są one tożsame z klasą „próby włamań" jednakże zakończone „sukcesem" z punktu widzenia osoby atakującej. Takich incydentów w 2021 roku było zaledwie 0,3 %, zaś rok później 0,2 % i w 2023 roku: 0,3 %.

Incydenty niesklasyfikowane w opisanych wyżej kategoriach stanowiły nieznaczną część wszystkich przypadków. Nie jest możliwe określić żadnego dominującego typu wśród tych incydentów.

Podobnie, jak w przypadku klasyfikacji opracowanej przez *CERT Polska (CERT NASK)* incydenty *phishingowe* stanowią trzon zagrożeń. Implikacje nie mają tak naprawdę ograniczeń, albowiem zarówno prywatne osoby, jak i instytucje czy podmioty publiczne mogą stać się ofiarami. Idąc dalej, skutki takich zachowań często są trudne do zatrzymania. Mając na myśli ataki na infrastrukturę krytyczną – będzie to dotyczyło całego państwa, wszystkich jego systemów współdziałących ze sobą, o czym w następnej części niniejszej pracy.

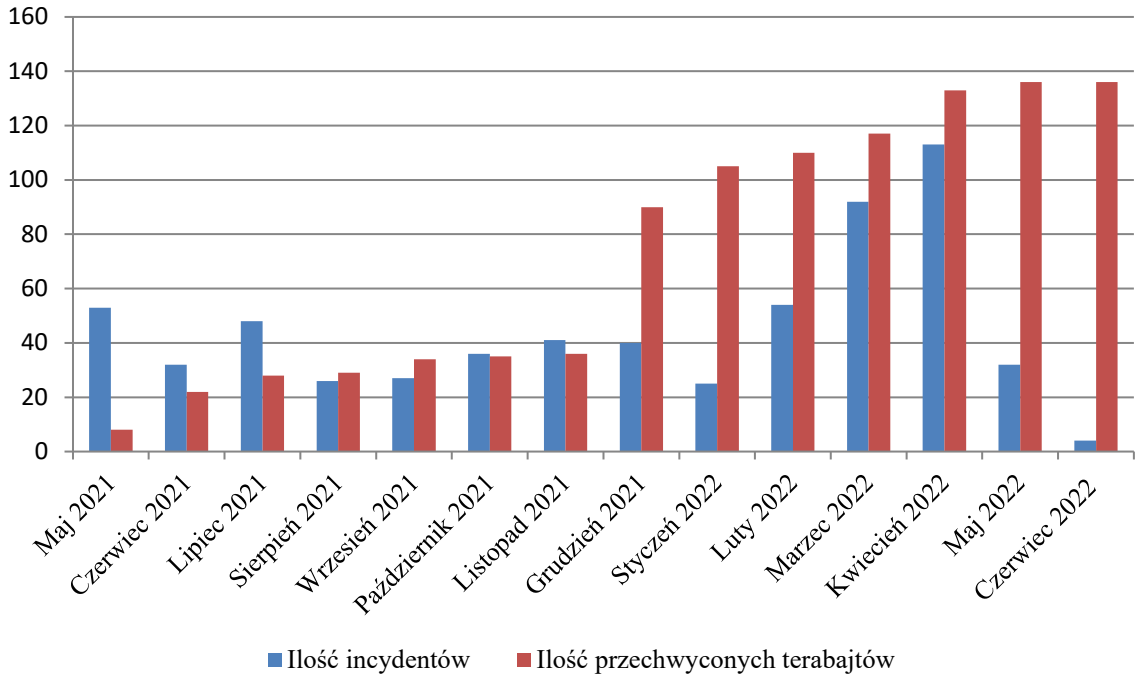
Europejska Agencja ds. Cyberbezpieczeństwa każdego roku publikuje raport przedstawiający *krajobraz cyberzagrożeń*, dzięki któremu decydenci i specjaliści ds. bezpieczeństwa mogą tworzyć lepsze strategie obrony przed zagrożeniami. Źródło raportu stanowią zarówno tzw. otwarte źródła, opinie ekspertów, artykuły medialne, raporty z badań bezpieczeństwa, analizy incydentów oraz wywiady z członkami grupy roboczej *ENISA*.

Wyniki raportu zostały zobrazowane w dalszej części w postaci wykresów. Pierwszy skupiony jest wokół ilości incydentów w danych sektorze państwa. Zaobserwowano znaczącą liczbę zdarzeń wymierzonych w administrację publiczną i dostawców usług cyfrowych. Tego ostatniego należy się spodziewać coraz częściej, biorąc pod uwagę horyzontalne świadczenie usług dla tego sektora, a tym samym jego wpływ na wiele innych sektorów. Zwrócono uwagę również na znaczną liczbę incydentów skierowanych przeciwko użytkownikom końcowym, ale niekoniecznie w konkretny sektor. Co interesujące, sektor finansowy miał do czynienia ze stałą liczbą incydentów, a tuż za nim uplasował się sektor opieki zdrowotnej.



Wykres 4.4. Sektory państwa będące celem ataków wg liczby incydentów (2021-2023) (źródło: opracowanie własne na podstawie Krajobrazu Cyberzagrożeń 2023- Raport *ENISA* (2021-2023), s.12-14)

Raport uwzględnia również jedno z zagrożeń będącym już dzisiaj znaną formą podatności – *ransomware* (zdefiniowane jako atak, w którym podmioty stanowiące zagrożenie mają na celu przejąć kontrolę i żądać okupu w zamian za przywrócenie pełnej dostępności zasobów). Zadanie sprawców oparte jest najczęściej na trzech filarach tj. na aktywności, działaniu i szantażu. Poniższy wykres zawiera dane dotyczące liczby incydentów oraz wykradzionych ilości danych.



Wykres 4.5. Stosunek liczby incydentów do ilości skradzionych danych [2021-2022] (źródło: opracowanie własne na podstawie Krajobrazu Cyberzagrożeń 2022- Raport *ENISA* [2021-2022)], s. 43-44)

Można zauważyć, iż obecnie nie jest potrzebna znacząca ilość incydentów – ataków, aby wykraść dużą ilość danych. Cyberprzestępcy stają się coraz bardziej wyrafinowani i wyspecjalizowani tak, aby jak najmniejszym wysiłkiem pracy - wyrządzić największe szkody, zyskać jak najwięcej. W porównaniu – w styczniu 2022 roku 25 incydentów spowodowało kradzież 105 TB danych, natomiast w czerwcu tego samego roku zaledwie cztery incydenty odpowiadały za 136 TB danych. Wartości i dane stanowią poważną przesłankę do bardziej wnikliwej analizy tego obszaru. Krajobraz *ransomware* staje się zmienny, zaś korzyści finansowe nie stanowią głównego faktora – zdaniem specjalistów *ENISA*. Wyróżnić można cztery wysokopoziomowe działania (blokowanie, usuwanie, szyfrowanie, kradzież), które wykorzystywane są przez oprogramowanie *ransomware* w celu wpłynięcia na: integralność, dostępność oraz poufność danych[213]. Wszystkie wyżej wymienione informacje świadczą o tym, że zagrożenie *ransomware* stale rośnie. Szczególnie istotne są działania zapobiegawcze, do których można zaliczyć m.in. regularną aktualizację oprogramowania, wykonywanie kopii roboczych, zabezpieczenie ewentualnych – potencjalnych źródeł infekcji czy monitoring sieci.

Ilość wykradzionych bądź zniszczonych danych rośnie z roku na rok. Rola danych, rola informacji we współczesnym świecie jest nieoceniona, czynniki te zyskują na

[213] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [dostęp 10.05.2023 r.].

znaczeniu, niestety zagrożenia w tym obszarze również stają się coraz bardziej obecne i trudniejsze do wyeliminowania.

Raport *ENISA* jest aktualnym i przydatnym źródłem danych oraz informacji przy ocenie przyszłych zagrożeń. Warto przyjrzeć się również zagadnieniu inżynierii społecznej, a zwłaszcza *phishingu*. Według raportu *Verizon Data Breach Investigations*[214] ponad 80% naruszeń związana jest z czynnikiem ludzkim, a nie mniej niż 60% naruszeń w Afryce, na Bliskim Wschodzie, ale i w Europie zawiera element inżynierii społecznej. Powód zainteresowania inżynierią społeczną jest dość oczywisty, ponieważ to poczta e-mail jest miejscem, w którym potencjalne ofiary można najłatwiej zlokalizować i osiągnąć zamierzony cel pomimo częstokroć uświadamiających kampanii. Hakerzy starają się wykraść uwierzytelniające dane, aby później posłużyć się nimi przy tworzeniu realistycznych pretekstów przeznaczonych do kolejnych przestępczych działań.

Niezwykle cenne źródło wiedzy stanowi także raport jednego z najstarszych przedsiębiorstw informatycznych *IBM Security (X-Force Threat Intelligence Index 2023)*[215]*,* którego podstawą są dane pochodzące ze stacji roboczych, urządzeń sieciowych oraz zgłoszeń incydentów.

Najczęściej występującym skutkiem cyberataków w roku 2022 był *ransomware* (wymuszenie). Najwięcej tego typu przypadków zanotowano w Europie (44%), gdzie starano się wykorzystywać napięcia geopolityczne. Do najczęściej atakowanej należała już po raz kolejny branża produkcyjna, z uwagi na m.in. jej atrakcyjność (mała tolerancja na przestoje). Jeden z najnowszych trendów skupia się na wykorzystywaniu skradzionych danych do prób ataku kolejnych ofiar, czego skutkiem jest zwiększona presja na zinfiltrowane organizacje[216].

IBM zaobserwował 100% wzrost liczby miesięcznych prób przejęcia konta e-mail (w porównaniu do roku 2021). Celem cyberprzestępców było zainfekowanie złośliwym oprogramowaniem urządzenie potencjalnej ofiary, co zaś prowadzić miało do infekcji *ransomware*. Innym trendem jest *porzucenie* działań związanych z danymi kart kredytowych. W ciągu roku liczba cyberprzestępstw z tego obszaru spadła o około połowę. Wskazuje to na fakt, iż priorytet stanowią dane osobowe, możliwe do wykorzystania w ramach kolejnych oszustw. Biorąc pod uwagę regiony świata, to

[214] https://www.verizon.com/business/resources/reports/dbir/ [dostęp 10.05.2023 r.].
[215] https://www.ibm.com/reports/threat-intelligence [dostęp 21.08.2023 r.].
[216] Ibidem.

Azja odnotowała najwięcej cyberataków (blisko 1/3 wszystkich ataków wg *IBM*). Połowę incydentów stanowiła branża produkcyjna[217].

4.3. Wpływ cyberzagrożeń na funkcjonowanie współczesnego państwa

„Możliwość pracy zdalnej, szybkiego komunikowania się, przesyłania danych to tylko niektóre z pozytywnych aspektów cyberprzestrzeni. Niezwykle ważne są umiejętności pozwalające reagować na zagrożenia pojawiające się w sieci. Zależy od tego bezpieczeństwo nas wszystkich, naszych granic, naszej gospodarki, naszych obywateli" - mówił Prezydent RP, Andrzej Duda na konferencji *CYBERSEC European Cybersecurity Forum 2021*[218].

Poniższa tabela przedstawia zagrożenia dla państwa w cyberprzestrzeni ze względu na podmiot, którego zagrożenie dotyczy. Nieco inne rozróżnienie występuje w nieobowiązującej już Doktrynie Cyberbezpieczeństwa z 2015 r., aczkolwiek zdaniem autora istotnej ze względu na standardowy charakter podziału. Zgodnie z doktryną, zagrożenia dzielą się na te występujące w wymiarze wewnętrznym oraz zewnętrznym. Wymiar wewnętrzny: cyberprzemoc, cyberprzestępczość, cyberprotesty, cyberdemonstracje, cyberzagrożenia w zakresie infrastruktury krytycznej, kradzież danych, naruszenie poufności, kradzieże tożsamości. Wymiar zewnętrzny natomiast stanowią: cyberkryzysy z udziałem podmiotów państwowych oraz niepaństwowych i mogące wynikać z tego ryzyko cyberwojny; cyberszpiegostwo związane z aktywnością służb obcych państw, w tym także organizacji terrorystycznych, wykorzystujących różnorodne narzędzia celem uzyskania dostępu do newralgicznych informacji państwa; organizacje terrorystyczne czy ekstremistyczne mogące mieć podłoże kryminalne, biznesowe, religijne, polityczne i ideologiczne. Poniżej zostały przedstawione i scharakteryzowane poszczególne zagrożenia. Mimo, że poszczególne zagrożenia sklasyfikowano do jednej z dwóch grup, to dyskusyjna pozostaje ich przynależność.

[217] Ibidem.
[218] https://www.youtube.com/watch?v=K2c0fCbUBKc [dostęp 03.09.2021 r.]. Zob.: https://cybersecforum.eu/ [dostęp 03.09.2021 r.].

Tab. 4.2

Zagrożenia dla państwa w cyberprzestrzeni

L.p.	Zagrożenie dla państwa polskiego	Zagrożenie dla obywateli państwa polskiego
1.	Cyberprzestępczość	
2.	Cyberdemonstracje	
3.	Cyberterroryzm	Cyberprzemoc
4.	Cyberszpiegostwo	Kradzież danych, kradzież tożsamości

Źródło: opracowanie własne na podstawie: A. Waloch, 2019, *Współczesne zagrożenia dla bezpieczeństwa państwa polskiego w cyberprzestrzeni*, Studia de Securitate, nr 9, s. 168

Obecnie wraz ze wzrostem znaczenia sfery *cyber*, tak dla państwa, jak i obywateli, coraz bardziej istotny staje się problem jej bezpieczeństwa[219].

Niestety wraz z rozwojem cyberprzestrzeni, rozwinęły się również w niej zagrożenia. Bowiem sieć, jak już wspomniano, to idealne miejsce dla przestępców takich, jak: wyłudzacze, pedofile i przede wszystkim hakerzy. Główną przyczynę stanowić może poczucie anonimowości. Internet jest również źródłem komunikacji terrorystów na praktycznie całym świecie. Oprócz terrorystów działają także służby wywiadowcze czy państwa kierujące agresję do innych państw, co prowadzić może do cyberwojny.

Jedno z podstawowych zagrożeń dla państwa stanowi cyberszpiegostwo definiowane jako: zdobywanie istotnych materiałów i informacji w cyberprzestrzeni poprzez służby wywiadowcze przy użyciu różnych metod oraz technik, ze szczególnym uwzględnieniem metod cybernetycznych. Skala aktów cyberszpiegostwa jest dość znacząca w innych państwach[220]. W Polsce – jasne ostrzeżenie wydał zespół *CERT Polska* oraz Służba Kontrwywiadu Wojskowego w kwietniu 2023 r. Współpraca tych podmiotów pozwoliła zaobserwować kampanię szpiegowską – połączoną z działaniami służb specjalnych Federacji Rosyjskiej, która miała na celu nielegalne pozyskiwanie informacji z placówek dyplomatycznych oraz ministerstw spraw zagranicznych, należących do NATO oraz UE. Nowa narzędzia wykorzystywane przez hakerów były stosowane niezależnie od siebie bądź też kolejno, tak aby zastąpić starsze rozwiązania, cechujące się spadającą skutecznością. Pozwoliło to sprawcom na zachowanie i utrzymanie ciągłości

[219] J. Świątkowska, 2014, *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny,* Wydawnictwo Instytut Kościuszki, Kraków, passim.
[220] R. Białoskórski, 2011, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa, s. 71.

swoich przestępczych działań[221]. Informacje i mechanizmy mające na celu podniesienie bezpieczeństwa wykorzystywanych systemów informatycznych zawarto na stronach rządowych typu gov.pl. Celem raportu było przerwanie trwającej kampanii szpiegowskiej i uniemożliwienie procedowania dalszych czynności cyberprzestępców.

Wszystkie zarejestrowane przypadki skupiały się na korzystaniu z techniki *spear phishingu*. Do konkretnych placówek rozsyłano wiadomości e-mail podszywające się pod wskazane ambasady krajów europejskich. W korespondencji zawierano zaproszenie do wspólnej pracy nad dokumentem bądź na spotkanie wraz z załączonym dokumentem *PDF* (kierującym rzekomo do kalendarza czy szczegółów spotkania). Odnośnik kierował bezpośrednio do przejętej strony, na której umieszczono skrypt – złośliwy plik umieszony na stronie jest *odkopywany* dzięki JavaScript w trakcie otwierania strony, po czym pobierany na urządzenie ofiary, co jeszcze bardziej utrudnia wykrycie po stronie serwera, na którym jest on przechowywany. Dodatkowo, skrypt skonstruowano w ten sposób, aby wyświetlał stroną internetową z treścią właściwą dla ofiary – tak by była ona utwierdzona w przekonaniu, iż pobrała prawidłowy załącznik[222].

Pomimo pewnych zmian w stosowanych narzędziach, część elementów kampanii szpiegowskiej pozostało taka sama. Złośliwy kod zawierano w linku bądź w dokumencie PDF podanym w wiadomości e-mail (czynnik ludzki pełnił w tym przypadku decydującą rolę). Pliki wykonywalne dodawano do nietypowych lokalizacji np. nośników zewnętrznych czy katalogów tymczasowych, co również powinno być zablokowane bądź wychwycone przez administratorów monitorujących ruch w sieci.

Innymi słowy, cyberszpiegostwem jest wykorzystywanie systemów komputerowych i technologii w celu nielegalnego uzyskiwania informacji od organów państwa i innych podmiotów.

W kręgu szczególnego zainteresowania wywiadu znajdują się dane dotyczące technologii, strategii rozwoju, negocjacji czy umów międzynarodowych. Rząd USA podaje, iż około stu organizacji obcego wywiadu próbuje rocznie włamywać się do systemów komputerowych rządu i amerykańskich firm. Określa się, iż zdecydowana część tych ataków kierowana jest ze strony Chin. Hakerzy decydują się atakować infrastrukturę państw zachodnich, m.in. przemysł, telekomunikację, energetykę, lotnictwo, obronę, elektronikę. Wykradzione dane trafiają do chińskich przedsiębiorstw państwowych,

[221] https://itwiz.pl/cert-polska-i-skw-ostrzegaja-przed-dzialaniami-rosyjskich-szpiegow/ [dostęp 10.06.2023 r.].

[222] https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi [dostęp 10.06.2023 r.].

dominujących w gospodarce chińskiej. Ponadto, intensywny rozwój systemów wywiadowczych ma miejsce w Rosji. Władze Kremla starają się wzmacniać defensywny, jak i ofensywny charakter swoich cyberdziałań[223].

Obserwuje się tendencję wzrostową w kwestii liczby personelu służb wywiadu, pomimo jednak tego faktu, nadal główny problem stanowi niewystarczająca ilość analityków[224]. Zadanie pozyskiwania informacji jest wypełniane na wysokim poziomie, jak ocenia literatura, natomiast równie ważny i trudny obowiązek stanowi analiza i interpretacja, weryfikacja i scalanie danych. Wyzwanie w tym obszarze stanowi zbyt duża ilość informacji pozyskiwanych, a zbyt małe możliwości przyswojenia i analizy[225]. W związku z powyższym, polityka kadrowa służb wywiadowczych powinna uwzględnić potrzeby nie tylko w kwestii fizycznego gromadzenia informacji, ale przede wszystkim wypełnić lukę analityczną w tym zakresie.

Cyberprzestępczość określa się jako *„motywowane finansowo bądź materialnie akcje w cyberprzestrzeni lub ich zamiar prowadzone przez pojedyncze osoby albo ugrupowania o charakterze przestępczym, które kierowane są przeciw różnym podmiotom państwowym / niepaństwowym i mogą prowadzić (bezpośrednio lub pośrednio) do określonych strat materialnych lub finansowych*"[226]. Istotne dla dalszych rozważań jest ustalenie różnic, granic pomiędzy pojęciami takimi, jak: cyberterroryzm i cyberprzestępczość, bowiem będzie to miało znaczenie dla wyboru środków, narzędzi oraz sposobów im przeciwdziałania. Literatura przedmiotu za najważniejszą różnicę wymienia kwestię intencji (motywacji sprawcy). Podczas dokonywania cyberataku, osoba odpowiedzialna za jego plan i realizację może być motywowana np. finansami. Natomiast, cyberterrorysta za najbardziej znaczący czynnik uznaje cele polityczne, społeczne bądź religijne. Stąd aktywność w cyberprzestrzeni może być rozumiana jako analogiczna, jednakże jej uzasadnienie stanowiące podstawę działania, prawdopodobnie będzie już zgoła inne[227]. Reasumując, różnicą jest: cel, intencja i motywacja danej osoby/ grupy.

Obecnie cyberprzestępstwa określane są jako najbardziej rozpowszechniona forma cyberzagrożeń. Są bardziej powszechne aniżeli zjawisko wojny cybernetycznej czy zjawisko cyberterroryzmu. Tworzone są specjalne, zorganizowane grupy do prowadzenia cyberprzestępczości. Rozwój specjalistycznych zestawów umiejętności

[223] A. Dean, 2012, *Cyber Threats in the 21st Century*, Security, vol. 49 (9), s. 71-77.
[224] M.M. Aid, 2012, *Intel wars: The secret history of the fight against terror,* New York, s. 214.
[225] Ibidem, s. 214.
[226] https://www.computerworld.com/article/2523545/the-fog-of--cyber--war.html *[*dostęp 01.08.2022 r.].
[227] M. Górka, 2017, *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa,* Cywilizacja i polityka, nr 15, s. 304-305.

technicznych pozwala cyberprzestępcom na sprawniejsze organizowanie działań występujących w różnych formach, tj.: fałszerstwa, oszustwa, ingerencja w system danych, kradzież własności intelektualnej, nielegalny dostęp do urządzeń elektronicznych[228]. Jedną z - wydawać by się mogło - niezwiązaną z aktami cyberterroryzmu, metodą cyberprzesępstwa są przestępstwa finansowe. Wiele organizacji terrorystycznych popełnia tego rodzaju przestępstwa, są to m.in. kradzież tożsamości, fałszowanie kart kredytowych, co pozwala na dostęp do kont bankowych i umożliwia regularne finansowanie działalności terrorystycznych. Dowodzi to, iż z pozoru zwykła kradzież tożsamości może być w rzeczywistości mniejszym trybem w całej machinie większego ataku terrorystycznego. Badacze wskazują, że świat cyberprzestępczości nazywany bywa swoistym *poligonem dla hakerów*, mogących rozwijać i doskonalić własne umiejętności[229]. Przykładem takiego cyberpoligonu jest bez wątpienia Ukraina i jej cyberprzestrzeń. Od 2015 roku mają miejsce cykliczne cyberataki rosyjskich hakerów, których celem jest destabilizacja sytuacji na Ukrainie, powodując m.in. paraliż metra czy lotnisk.

Wojna w Ukrainie stanowi potwierdzenie, iż to cyberprzestrzeń jest jak najbardziej integralnym miejscem wojen i konfliktów. To, co dzieje się za wschodnią granicą Polski, oddziałuje również na inne państwa, nie tylko sąsiedzkie. Choć to właśnie pociski i bomby spadają na tereny ukraińskie, to inne działania obserwowane są w różnych miejscach Europy. W przypadku SZ RP mówi się o wzroście wręcz pięciokrotnym w kontekście prób cyberataków przeciwnika. Celem Rosji jest zakłócenie strategicznych procesów (przede wszystkim dotyczących infrastruktury transportowej- utrudniając dostawy na Ukrainę)[230]. Tak więc opór Polski ma ogromne znaczenie i również zależy od współpracy z innymi państwami.

Innym zagrożeniem są *cyberdemonstracje*, czyli zbiorowe, *publiczne* zgromadzenia, których celem jest wyrażenie zdań protestujących osób przeciwko danej sprawie w Internecie. Jako przykład podać można pierwszą polską cyberdemonstrację w sprawie *ACTA* na tak ogromną skalę. W pierwszej fazie polegała ona na masowej blokadzie stron internetowych należących głównie do administracji państwowej. W późniejszym etapie doszło do serii ataków na serwery rządowe. W związku z tym, iż wydarzenie

[228] A. Dean, 2012, *Cyber…,* op. cit.
[229] J. Carr, 2011, *Inside Cyber Warfare, 2nd Edition Mapping the Cyber Underworld*, O'Reilly Media, s. 22–25.
[230] https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-ataki-rosji-na-nato-wywiad-oceniaryzyko [dostęp 23.10.2023 r.].

takie miało miejsce w państwie po raz pierwszy, Polska nie była właściwie przygotowana do przeciwdziałania takiej sytuacji[231].

Postępująca globalizacja i rozwój technologiczny doprowadził do bardzo dużego uzależnienia od technologii informatycznych, co z kolei wiąże się z powstaniem nowej formy terroryzmu jaką jest cyberterroryzm. Podobnie, jak z definicją zagrożenia, pojawia się niezgodność co do dokładnego określenia cyberterroryzmu, a jego postrzeganie zależy od tego, jak jest prezentowana w mediach, jak jest omawiana przez specjalistów oraz od tego jak została określona w dziedzinie informatyki.

Amerykańskie Narodowe Centrum Ochrony Infrastruktury określa cyberterroryzm jako: „akt kryminalny, do którego popełnienia użyto komputera i telekomunikacji, powodujący przerwanie i / lub zniszczenie świadczonych usług w celu wywołania strachu, poprzez wprowadzenie niepewności, zamieszania w danym społeczeństwie, tak aby wpływać na rządy i ludność w celu osiągnięcia własnych celów społecznych, politycznych czy ideologicznych"[232].

Amerykańskie Federalne Biuro Śledcze (*FBI*[233]) definiuje cyberterroryzm jako każdy umyślny i umotywowany politycznie atak na systemy komputerowe, informacje, programy i dane, którego skutkiem jest przemoc wobec ludności cywilnej[234].Jak się okazuje, aby sklasyfikować atak jako cyberterroryzm, musi być on przeprowadzony przy użyciu systemu informatycznego lub urządzenia elektronicznego[235].

Współcześnie terroryści działają nie tylko przy użyciu bomb czy karabinów maszynowych, nowoczesnym uzbrojeniem terrorysty okazuje się komputer, Internet, sieć WWW, a także płyty CD/DVD czy konta e-mailowe. Dzięki swoim nowoczesnym narzędziom, terroryści potrafią kontrolować przekaz w mediach, dodawać do niego odpowiedni kontekst oraz dostosowywać środki przekazu do docelowej grupy odbiorców[236].

Terroryści chętnie korzystają z Internetu, a w tym bazują na mediach społecznościowych ze względu na: łatwy dostęp; brak regulacji i cenzury państwowej lub w bar-

[231] A. Waloch, „*Współczesne zagrożenia…",* op. cit., s. 169.
[232] T. Szubrycht, 2005, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty naukowe Akademii Marynarki Wojennej, Gdynia, s. 174-175.
[233] Federal Bureau of Investigation.
[234]K. T. Hanna, K. Ferguson, L. Rosencrance, *cyberterrorism,* https://searchsecurity.techtarget.com/definition/cyberterrorism, [dostęp 28.07.2021 r.].
[235] T. Szubrycht, 2005, *Cyberterroryzm...,* s. 176.
[236] B. Hoffman, 2006, *Foreword*, [w:] G. Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington, s.9.

dzo ograniczonym stopniu; potencjalnie ogromną grupę odbiorców na całym świecie; możliwość anonimowej komunikacji; bardzo szybki przepływ informacji; niskie koszty działalności w sieci WWW; multimedialność; możliwość narzucania tematów oraz plików w odpowiednim kontekście mass mediom, które bardzo często stosują źródła internetowe jako odpowiednie źródło informacji[237].

W 2014 roku opublikowany przez firmę *Symantec* raport ujawnił działania grupy cyberprzestępców *Dragonfly*, którzy co najmniej od 2013 roku przeprowadzali działania szpiegowskie w cyberprzestrzeni nakierowane na polskie firmy z sektora energetycznego[238].

Kolejnym przykładem działania cyberterrorystów może być atak skierowany na polski resort obrony. Były szef Narodowego Centrum Kryptologii i ABW, generał Krzysztof Bondaryk ujawnił, że w wyniku działań cyberterrorystów skradziono kilkaset tysięcy maili ze skrzynek pracowników resortu obrony. Działania szpiegowskie prawdopodobnie udawało im się prowadzić w latach 2006-2014. Na skalę problemu bezpieczeństwa w cyberprzestrzeni uwagę zwraca fakt długości trwania działań szpiegowskich oraz ogrom przejętych informacji. Przeprowadzone badania wykazały, że średnio aktywność szpiegowska może trwać nawet 205 dni, zanim zostanie zauważona[239].

Z powyższymi definicjami związana jest zdaniem autora infrastruktura krytyczna. Bowiem regulacje określają ją jako systemy i wchodzące w ich skład powiązane obiekty, obiekty budowlane, instalacje, urządzenia a także usługi kluczowe dla obywateli i całego państwa, które służą zapewnieniu właściwego i skutecznego funkcjonowania administracji publicznej (w tym także instytucji i przedsiębiorców)[240]. Według ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. w skład infrastruktury krytycznej wchodzą następujące systemy:

- zaopatrzenia w energię, paliwa i surowce energetyczne;
- sieci teleinformatycznych;
- łączności;
- finansowe;
- zaopatrzenia w żywność i wodę;

[237] B. Hoffman, 2006, *Foreword,* op. cit., s. 9-11.
[238] Fireeye, APT28: A Window Into Russia's Cyber Espionage Operations?, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyberespionage-operations.html [dostęp 28.07.2021 r.].
[239] Fireeye, M-Trends 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf [dostęp 28.07.2021 r.].
[240] https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp 23.10.2022 r.].

- ochrony zdrowia;
- ratownicze;
- transportowe;
- produkcji składowania, magazynowania i stosowania substancji chemicznych, promieniotwórczych, w tym także rurociągi substancji niebezpiecznych;
- zapewniające właściwe działanie i ciągłość administracji publicznej[241].

Szczególny wymiar IK sprawia, że jest ona poddana specyficznej ochronie. Precyzyjne zdefiniowanie czym jest IK wymusiło na państwie wskazane podmiotów, które właściwe są do zarządzania IK i jej ochroną. Było to możliwe dzięki stworzeniu podstaw prawnych. Istotną rolę stale odgrywa również współpraca publiczno-prywatna, czego efektem jest poprawa warunków bezpieczeństwa i stworzenie przejrzystych zasad oraz procedur. Współpraca ta polega m.in. na: wymianie informacji; tworzeniu kanałów informacyjnych dla sygnałów alarmowych, nadawanych przez służby państwowe; zapewnieniu bezpieczeństwa danym, które stanowią tajemnicę handlową i pochodzą od operatorów[242].

W poniższej tabeli wskazane zostały przykłady cyberataków na infrastrukturę krytyczną ze szczególnym uwzględnieniem sektorów narażonych na zainfekowanie bądź na jakikolwiek wpływ danego zdarzenia.

Tab. 4.3

Przykładowe cyberataki na infrastrukturę krytyczną

Czas i miejsce	**Cyberatak**	**Sektor**	**Opis**
1997, Stany Zjednoczone	Worcester Air Traffic Communications Attack	Transport lotniczy	Doprowadzono do wyłączenia linii telefonicznych, które obsługiwały wieżę kontrolną, ochronę lotniska, straż pożarną i służbę pogodową. Unieruchomiono oświetlenie pasa startowego.

[241] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89, poz. 590, z późn. zm.).
[242] J. Trubalska, 2015, *Wybrane aspekty ochrony infrastruktury krytycznej w Polsce,* Zeszyty Naukowe WSEI. Seria Administracja, nr 1, s. 116.

1999, Australia	System dostawy wody pitnej	Dostawa wody	Były pracownik dezaktywował system alarmowy, który był obsługiwany drogą radiową, co doprowadziło do zakłóceń w dostawie wody pitnej oraz do jej zanieczyszczenia.
2003, Stany Zjednoczone	System sygnalizacji kolei *CSX*	Transport kolejowy	Zastosowano robaka internetowego o nazwie *SoBig*, który zainfekował system komputerowy do obsługi ruchu kolejowego korporacji *CSX* w 23 stanach amerykańskich. Skutkowało to odwołaniem części pociągów oraz opóźnieniami w ruchu kolejowym.
2003, Stany Zjednoczone, Kanada	Zanik dostawy prądu w pn.-wsch. części Ameryki Północnej	Dostawa energii elektrycznej	Pozbawiono prądu około 50 mln osób prawdopodobnie przy użyciu robaka internetowego Blaster, który był w stanie zakłócić działanie systemu alarmującego o awarii. Straty oszacowano na 4-10 mld dolarów amerykańskich.
2006, Stany Zjednoczone	System filtracji wody	Dostawa wody	Atak doprowadził do przejęcia kontroli nad systemem zarządzającym filtracją wody i wykorzystania go jako nośnika spamu i przechowania pirackiego oprogramowania. Atak przeprowa-

			dzono poprzez podłączony do Internetu komputer pracownika firmy, przy pomocy którego zdalnie zainstalowano wirusa i oprogramowanie szpiegujące na serwerze głównym.
2010, Iran	Wirus Stuxnet	Energia atomowa	Przeprowadzono atak na irańskie systemy informatyczne obsługujące elektrownie atomowe, który spowodowała zakłócenia w funkcjonowaniu elektrowni.
2014, Korea Południowa	Systemy komputerowe	Elektrownia jądrowa	Jeden z użytkowników portalu *Twitter* przyznał się do ataku na systemy komputerowe elektrowni, domagając się wyłączenia starszej generacji generatorów. Groził, że udostępni kolejne materiały dotyczące planów reaktorów jądrowych, kosztów czy też narażenia na promieniowanie.
2016, Korea Południowa	Sieci ministerstwa obrony	Systemy obrony	O ataku informację do mediów podano dopiero rok po nim. Hakerzy zdołali wykraść plany operacyjne dotyczące ewentualnej wojny Korei Płd. z USA i Koreą Płn. Z dostępnej wiedzy wynika, iż zdobyto ponad

			200 gigabajtów danych.
2016, Ukraina	Elektrownia w Zaporożu	Dostawa energii elektrycznej	Atak przeprowadzony najprawdopodobniej przez Rosję spowodował nagłe przerwanie dostaw energii elektrycznej do blisko miliona gospodarstw domowych.
2017, Polska	System bankowy. Grupa Lazarus (podejrzewana o szereg zmasowanych akcji na całym świecie)	System finansowy	Operację rozpoczęto zainfekowaniem strony internetowej Komisji Nadzoru Finansowego. Zastosowano tzw. taktykę wodopoju, zgodnie z którą atakowana jest dana organizacja, po czym hakerzy obserwują z jakich stron www korzysta ofiara, tak by zainfekować również te witryny. Wirusy przenoszą się na kolejne komputery. Wg KNF poszkodowanych zostało ok. 20 polskich banków. Zdaniem *„New York Times”* atak zorganizowała Korea Północna.
2017, Ukraina	System bankowy, telekomunikacyjny, lotniska, sieci komputerowe, elektrownie, ciepłownie i metro w Kijowie. Wirus	Energetyczny, transport, pozostałe sektory	Atak przeprowadzony najprawdopodobniej przez Rosję doprowadził do wstrzymania operacji finansowych jednego z największych banków Ukrainy. Zainfekowano również sieć

	Petya		komputerową na terenie nieczynnej elektrowni w Czarnobylu (przechowującej zużyte paliwo jądrowe).
2018, Francja	Systemy komputerowe	Elektrownia jądrowa	Atak, którego celem była francuska firma Ingerop skutkował kradzieżą tysięcy poufnych dokumentów dotyczących elektrowni jądrowych (plany pomieszczeń, dane osobowe pracowników).
2019, Indie	Systemy komputerowe	Elektrownia jądrowa	Przeprowadzono atak na sieć elektrowni, którego celem było pozyskanie informacji w zakresie projektu budowy elektrowni.
2020, Polska	Systemy (nieokreślone)	Sieć elektroenergetyczna	Znaczący polski operator padł ofiarą ataku, który skutkował częściowym wyłączeniem systemów.
2022, Ukraina	Systemy komputerowe	Elektrownia atomowa	Rosyjscy hakerzy przeprowadzili skoordynowany atak, w ramach którego doszło do kradzieży danych z zasobów *MAEA*.

Źródło: opracowanie własne na podstawie: Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej*, Warszawa 2013, s. 49-50 oraz K. Piękoś, 2017, *Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków,* Krakowskie Studia Małopolskie, nr 22, s. 107-113; https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf [dostęp 01.06.2023 r.].

Zmasowane ataki zagrażające stabilności państw i narodów sprawiają, że niezbędne są działania prewencyjne i zapobiegawcze. Stąd np. w roku 2017 na Litwie odbyły się ćwiczenia, w ramach których sprawdzano odporność systemu fi-

nansowego na ataki cybernetyczne. Sprawdzeniu podlegały zabezpieczenia dostępności usług elektronicznych, procedury zarządzania ryzykiem i inne. Specjalistka litewskiego banku centralnego określiła, iż ich systemy informatyczne poradziły sobie z pozorowanymi atakami i tym samym oceniono gotowość systemu na tego rodzaju zagrożenia sieciowe. W dobie ataków hakerskich kluczowym jest zabezpieczenie wrażliwych obszarów państwa, tj. systemu bankowego czy elementów infrastruktury krytycznej[243].

Zwalczanie cyberterroryzmu stało się bardzo poważnym zagadnieniem i problemem zarówno natury politycznej, jak i ekonomicznej. Po pamiętnych atakach we wrześniu 2001 roku władze amerykańskie wydały około 4,5 mld dolarów w celu zabezpieczenia swoich systemów informatycznych. W dzisiejszej rzeczywistości władze coraz lepiej radzą sobie z klasycznym terroryzmem i w wielu przypadkach potrafią zapobiegać aktom terroryzmu na świecie, co skłania potencjalnych terrorystów do przejścia na inne metody działania i korzystania z możliwości, jakie dają sieci informatyczne i telekomunikacyjne, co natomiast może doprowadzić do wzrostu cyberprzestępczości[244].

Cyberterroryzm może być nieprzewidywalny i może wpływać na stabilność i funkcjonowanie struktur państwowych. Zniszczenie lub uszkodzenie infrastruktury krytycznej może doprowadzić do osłabienia zdolności obronnych państwa oraz zagrozić jego bezpieczeństwu. Najbardziej zagrożonymi elementami infrastruktury są: systemy zaopatrzenia w wodę, system bankowy, telekomunikacja, energetyka, transport, wydobycie ropy i gazu ziemnego ora służby ratownicze i administracja publiczna[245].

4.4. Wyzwania cyberbezpieczeństwa

Termin: *wyzwanie cyberbezpieczeństwa* odnosi się do różnych trudności, problemów i zagrożeń związanych z obszarem cyfrowym (cyberbezpieczeństwem, cyberprzestrzenią). Jest to obszar działań podejmowanych w środowisku komputerowym, sieciowym i technologicznym. Wyzwania cyberbezpieczeństwa obejmują szeroką gamę kwestii, które mogą mieć wpływ na: bezpieczeństwo, prywatność, stabilność i integralność systemów informatycznych oraz danych przechowywanych w tych systemach.

Mając na uwadze dotychczasowe rozważania zawarte w niniejszym rozdziale można przyjąć, że cyberzagrożenia stanowią poważne wyzwanie dla funkcjonowania

[243] K. Piękoś, 2017, *Ataki…,* op. cit., s. 112-113.
[244] T. Szubrycht, 2005, *Cyberterroryzm....,* op. cit. s. 185.
[245] W. Smolski, 2015, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa,* Wydawnictwo Niepaństwowa Wyższa Szkoła Pedagogiczna, Białystok, s. 492

państwa i narodu. Sytuacja międzynarodowa oddziałuje na obszary cyberprzestrzeni, która rozwija się stale i dynamicznie. Stąd geopolityka ma znaczący wpływ na różnego rodzaju operacje cybernetyczne. Jak destrukcyjne mogą być ataki zauważyć można obserwując toczący się konflikt w Ukrainie. Analizując obecne faktory stwierdzić należy, iż do szczególnie podatnych i narażonych na ataki zalicza się: sektory przemysłu zbrojeniowego, elementy infrastruktury krytycznej państwa - w tym sektory usług finansowych oraz energetycznych.

Ataki hakerskie mogą mieć szereg różnorodnych skutków zarówno dla jednostek, jak i dla organizacji czy społeczeństwa jako całości. Poniżej wskazano kilka głównych skutków ataków hakerskich.

Kradzież danych osobowych: ataki hakerskie często mają na celu kradzież danych osobowych, takich, jak: numery kart kredytowych, dane logowania, dane identyfikacyjne czy informacje medyczne. Skutkiem może być naruszenie prywatności, oszustwa finansowe, utrata tożsamości i niewłaściwe wykorzystanie danych.

Utrata danych: ataki hakerskie mogą prowadzić do utraty lub uszkodzenia danych przechowywanych na serwerach, komputerach lub w chmurze. Skutkiem może być utrata ważnych informacji biznesowych, dokumentów, plików klientów czy innych cennych zasobów, co może prowadzić do znacznych strat finansowych i operacyjnych.

Przerwy w działaniu usług: ataki hakerskie powodują przerwy w działaniu usług online, takich jak strony internetowe, systemy bankowe, platformy handlowe czy usługi komunikacyjne. Skutkiem może być utrata dostępności, zakłócenia w działaniu biznesu, niezadowolenie klientów oraz straty finansowe.

Sabotaż infrastruktury: ataki hakerskie bywają ukierunkowywane na krytyczną infrastrukturę, taką jak systemy energetyczne, transportowe czy telekomunikacyjne. Skutkiem może być zakłócenie działania tych systemów, przerwy w dostawie energii, utrudnienia w komunikacji czy opóźnienia w transporcie, co może mieć poważne konsekwencje dla bezpieczeństwa publicznego i gospodarki.

Dystrybucja złośliwego oprogramowania: ataki hakerskie często wykorzystują złośliwe oprogramowanie takie, jak: wirusy, *trojany* czy *ransomware*, które może rozprzestrzeniać się w sieci lub infekować systemy. Skutkiem może być dalsze ataki, utrata kontroli nad systemem, szkody finansowe czy utrudnienia w działaniu. Błędy w oprogramowaniu, znane jako luki bezpieczeństwa, stanowią potencjalne wejścia dla atakujących. Konieczność ciągłego aktualizowania i zabezpieczania oprogramowania stwarza

wyzwanie, zwłaszcza gdy wiele systemów korzysta z przestarzałych lub niemodernizowanych wersji.

Zagrożenie bezpieczeństwa publicznego: ataki na infrastrukturę krytyczną mogą stanowić poważne zagrożenie dla bezpieczeństwa publicznego. Przykładowo, atak na systemy monitoringu lotniska, kontroli granicznej czy systemy alarmowe może prowadzić do utraty kontroli nad tymi obszarami, stwarzając ryzyko dla bezpieczeństwa pasażerów, obywateli czy interesów państwowych.

Szkody finansowe: ataki hakerskie mogą prowadzić do znacznych strat finansowych dla jednostek, organizacji czy instytucji. Skutkiem może być kradzież środków z kont bankowych, żądania okupu w przypadku ransomware, straty związane z przerwą w działaniu biznesu czy koszty związane z przywracaniem systemów i ochroną przed kolejnymi atakami.

Warto zauważyć, że skutki ataków hakerskich są różne w zależności od rodzaju ataku, celu i podmiotu, który jest atakowany. Dlatego ważne jest, aby podejmować odpowiednie środki ochronne i reagować szybko w przypadku podejrzenia ataku, aby zminimalizować skutki i chronić się przed przyszłymi zagrożeniami.

W przypadku ataków na infrastrukturę krytyczną państwa, skutki mogą być szeroko zakrojone i mieć poważne konsekwencje dla społeczeństwa, gospodarki i bezpieczeństwa publicznego. Dlatego ważne jest, aby państwa i organizacje odpowiedzialne za infrastrukturę krytyczną stosowały odpowiednie środki ochrony, monitorowały zagrożenia i reagowały skutecznie w przypadku ataków cybernetycznych.

Cyberzagrożenia mogą mieć poważny wpływ na funkcjonowanie państwa na wielu poziomach.

Bezpieczeństwo narodowe: ataki cybernetyczne mogą stanowić poważne zagrożenie dla bezpieczeństwa narodowego. Mogą obejmować próby infiltracji i szpiegostwa, sabotaż systemów wojskowych, krytycznej infrastruktury czy też naruszenia wrażliwych danych państwowych. Znaczące ataki na te obszary mogą poważnie osłabić zdolności obronne, destabilizować kraje lub narażać na utratę ważne informacje i sekrety.

Infrastruktura krytyczna: wiele sektorów infrastruktury krytycznej, takich jak systemy energetyczne, transportowe, telekomunikacyjne czy systemy finansowe, jest uzależnionych od technologii informatycznych. Ataki na te systemy mogą prowadzić do zakłóceń, przestojów i utraty usług o znaczeniu dla społeczeństwa. Może to mieć poważne skutki dla gospodarki, bezpieczeństwa publicznego i stabilności państwa.

Dane osobowe i prywatność: państwa przechowują ogromne ilości danych osobowych swoich obywateli. Ataki na te dane mogą prowadzić do kradzieży tożsamości, oszustw finansowych, naruszenia prywatności i niewłaściwego wykorzystania danych. To z kolei może poważnie wpłynąć na zaufanie obywateli do instytucji państwowych i systemów publicznych. Wprowadzenie surowych przepisów dotyczących prywatności, takich jak RODO (Rozporządzenie o Ochronie Danych Osobowych) w Europie, wymaga od organizacji skomplikowanych działań w zakresie ochrony danych i zapewniania zgodności z przepisami.

Działalność administracji publicznej: ataki na systemy informatyczne administracji publicznej mogą zakłócić działalność rządową i utrudnić świadczenie usług publicznych. Przestępcy mogą próbować przechwycić dane, naruszać stron internetowych, zakłócać komunikację i manipulować informacjami. To może osłabić zaufanie obywateli do państwa i wpływać na efektywność rządowych działań.

Wymiar sprawiedliwości i bezpieczeństwo publiczne: ataki na systemy wymiaru sprawiedliwości, organy ścigania i agencje bezpieczeństwa mogą prowadzić do utraty dowodów, wycieku informacji o świadkach lub działaniach policyjnych. To może mieć negatywny wpływ na prowadzenie śledztw, egzekwowanie prawa i utrzymanie porządku publicznego.

Biorąc pod uwagę raporty cyberbezpieczeństwa można wskazać na wiele innych wyzwań, z którymi mierzą się obecnie, bądź będą mierzyć w przyszłości narody i państwa. Dezinformacja dzięki użyciu sztucznej inteligencji jest w stanie zakłócić relacje społeczne i wprowadzać niepokoje np. na etapie tworzenia przepisów prawa. Ponadto, zagrożeniem mogą być sytuacje związane z *deepfakeami* czy zalewaniem różnego rodzaju stron rządowych fałszywymi czy podsycającymi negatywnie komentarzami. Co jest szczególnie istotne, dezinformacja stanowi ogromne narzędzie w wojnie. Wykorzystano ją np. w ramach działań przygotowawczych do rozpoczęcia inwazji Federacji Rosyjskiej na Ukrainie. Związane z cyberwojną są także podatności na sieci mobilne, przede wszystkim smartfony.

Skuteczne przeciwdziałanie tym wyzwaniom wymaga stałej uwagi, inwestycji w technologie bezpieczeństwa, edukacji uczniów, nauczycieli, pracowników oraz współpracy między sektorami publicznym a prywatnym.

Kluczowym wyzwaniem w obszarze publicznym jest odporność cyfrowa. W styczniu 2023 roku weszło w życie rozporządzenie UE- *DORA (Digital Operational Resiliance Act)*, które będzie obowiązywać od stycznia 2025 roku. Jego celem jest

wzmocnienie bezpieczeństwa informatycznego podmiotów finansowych, banków, towarzystw ubezpieczeniowych i firm inwestycyjnych. Sektor finansowy staje się coraz bardziej zależny od technologii cyfrowych, wynikiem jest większa podatność podmiotów finansowych na ataki czy incydenty cybernetyczne. Regulacja oprócz kwestii zarządzania ryzykiem *ICT* obejmować także będzie testowanie cyfrowej odporności operacyjnej, co pozwoli na bieżące i aktualne monitorowanie poziomu cyberbezpieczeństwa[246].

Niezwykle ważny filar *DORA* stanowić będzie zobligowanie podmiotów finansowych do wymiany między sobą informacji w zakresie metod ochrony przed cyberatakami. Z pewnością fakt powstania rozporządzenia umożliwi stworzenie jednolitego, finansowego rynku cyfrowego i jednocześnie zwiększy jego konkurencyjność na świecie. Niemniej jednak, implementacja założeń i spełnienie wymagań będzie wyzwaniem dla podmiotów finansowych i dostawców technologii.

W obszarze prywatnym ogromne wyzwanie stanowi rozwój i doskonalenie umiejętności użytkowników sieci. Szczególnie ważna jest w tym aspekcie świadomość społeczeństwa z jakimi cyberzagrożeniami może się mierzyć i jak im przeciwdziałać.

4.5. Wnioski

Wielość i różnorodność zagrożeń sprawia, iż niezbędne staje się tworzenie wyspecjalizowanych komórek odpowiedzialnych za kwestie cyberbezpieczeństwa. To bez wątpienia zadanie niezwykle trudne, którego realizacja przekładać się będzie na bezpieczeństwo i ochronę własnych interesów.

W poszczególnych obszarach bezpieczeństwa w cyberprzestrzeni koniecznym jest powołanie liderów i instytucji specjalizujących się w gromadzeniu wiedzy w określonym zakresie i koordynacji działań wszystkich elementów podsystemu ochrony i obrony. Dotyczy to przede wszystkim: zwalczania terroryzmu, w tym monitorowania międzynarodowego terroryzmu, prewencji na terytorium kraju, ochrony infrastruktury krytycznej, treningu i szkolenia jednostek przeznaczonych do aktywnego zwalczania aktów terrorystycznych, ponadto także metod i procedur przygotowania społeczeństwa (ludności) na wypadek aktu terroru. Te wszystkie przedsięwzięcia wymagają ustanowienia nowych regulacji prawnych o zwalczaniu terroryzmu, zwalczania przestępczości zorganizowanej, z precyzyjnym określeniem wiodącej roli Biura Bezpieczeństwa Naro-

[246] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [dostęp 17.02.2024 r.].

dowego. Obecnie istnieją obszary przestępczości, którymi zainteresowane są niemal wszystkie podmioty. Niezbędnym jest również utworzenie publiczno-prywatnej platformy współpracy na rzecz zwalczania cyberprzestępczości, a także dopracowanie (zmiana) regulacji prawnych określających uprawnienia i obowiązki jej członków, wskazanie pochodzenia finansowania, określenie relacji i zasad współpracy krajowej i międzynarodowej, w tym właściwa ocena ilości przetwarzanych danych oraz wskazanie rozwiązań technicznych dla tej platformy[247].

Dyrektor *ENISA*, Juhan Lepassaar oznajmił: *"Łagodzenie przyszłych cyberzagrożeń nie może być odkładane ani unikane. Stąd, każdy wgląd w przyszłość to nasz najlepszy plan ubezpieczeniowy. Przecież "lepiej zapobiegać aniżeli leczyć". Nasz obowiązek stanowi podjęcie wszelkich sił i środków z wyprzedzeniem, tak aby zapewnić, że w przeciągu kilku lat zwiększymy naszą odporność na wzmocniony krajobraz bezpieczeństwa cybernetycznego w roku 2030 i nawet później"*[248].

Różnice pomiędzy wymienianymi wyżej zjawiskami (cyberterroryzm, cyberprzestępczość etc.) stopniowo rozmywają się. Wielość sprawców tych zdarzeń, jak: organizacje, instytucje państwo czy pojedyncze osoby powodują trudności definicyjne, ale także sprawiają trudności w wyborze działań defensywnych przed cyberzagrożeniami. Każde z powyższych cyberzagrożeń charakteryzuje się indywidualną motywacja, celami, które jednak w działaniu praktycznym łączą się i nakładają na siebie.

Wskazanie realnych (potencjalnych) zagrożeń jest podstawą do zwiększania świadomości cyberbezpieczeństwa. Potrzebna jest wspólnotowa dyskusja i analiza obszarów szczególnie podatnych na zagrożenia. Żaden kraj nie będzie w stanie poradzić sobie w pojedynkę z działaniami w cyberprzestrzeni, a tylko silne partnerstwo i stała wymiana informacji może stanowić środek zaradczy[249]. W związku z powyższym, cyberzagrożenia stanowią realne i stałe wyzwanie dla państwa i wymagają skutecznej ochrony cyberbezpieczeństwa na wszystkich poziomach, włączając w to zarówno rozwijanie odpowiednich strategii i przepisów, jak i edukację społeczeństwa w zakresie bezpieczeństwa cybernetycznego.

[247] A. Pieczywok, 2019, *Cyber threats and challenges targeting Man versus his education*, *Cybersecurity and Law*, nr 1, s. 223-233.
[248] https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [dostęp 02.05.2023 r.].
[249] https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-cyberbezpieczenstwo-2030-co-bedzie-najwiekszym-zagrozeniem [dostęp 21.10.2023 r.].

5. Kompetencje cyfrowe użytkowników

5.1. Podział kompetencji cyfrowych

Kompetencje cyfrowe odnoszą się do umiejętności, wiedzy i zdolności niezbędnych do skutecznego, bezpiecznego i krytycznego korzystania z technologii cyfrowych. W dobie, gdzie technologia odgrywa kluczową rolę w różnych obszarach życia, posiadanie kompetencji cyfrowych staje się coraz ważniejsze.

Kompetencje cyfrowe mogą być rozumiane jako zespół kompetencji informacyjnych, które obejmują umiejętności wyszukiwania informacji, zrozumienia jej i oceny wiarygodności, a także kompetencji informatycznych – czyli umiejętności wykorzystywania komputera i innych elektronicznych urządzeń, umiejętności posługiwania się Internetem i korzystania z aplikacji oraz tworzenia treści cyfrowych[250].

Kluczowe w zakresie cyberbezpieczeństwa instytucje podają swoje definicje kompetencji cyfrowych, które jednak nieznacznie od siebie odbiegają. Poniżej autor prezentuje kilka wybranych rozumień tego terminu.

Unia Europejska: *"Kompetencje cyfrowe oznaczają korzystanie z technologii cyfrowych, komunikację za pomocą mediów cyfrowych, ocenianie, szukanie i przetwarzanie informacji rozwiązywanie problemów przy użyciu cyfrowych narzędzi, tworzenie treści cyfrowych i świadome, krytyczne a przede wszystkim bezpieczne korzystanie z technologii informacyjno-komunikacyjnych"*[251].

Organizacja Współpracy Gospodarczej i Rozwoju *(OECD): "Jako kompetencje cyfrowe określa się umiejętność korzystania z cyfrowych technologii, rozwiązywania problemów w środowisku informacyjnym i komunikowania się, a także umiejętność korzystania z narzędzi cyfrowych w celu efektywnego współdziałania w społeczeństwie"*[252].

European Digital Competence Framework (DigComp): "Kompetencje cyfrowe stanowią umiejętność korzystania z technologii cyfrowych, zrozumienie ich potencjału

[250] V. Szymanek, 2013, *Społeczeństwo Informacyjne w liczbach*, Ministerstwo Administracji i Cyfryzacji, Warszawa, s. 14.
[251] *Digital Competence Framework for the European Schools,* https://www.eursc.eu/BasicTexts/2020-09-D-51-en-2.pdf, Joint Teaching Committee, [dostęp 22.11.2023 r.].
[252] https://digital-skills-jobs.europa.eu/en/inspiration/research/oecd-skills-digital-transition-2022 [dostęp 22.11.2023 r.].

i funkcji, krytyczną ocenę informacji, efektywne poszukiwanie, analizowanie i przetwarzanie danych, a także bezpieczne i etyczne korzystanie z zasobów cyfrowych"[253].

Kompetencje cyfrowe w Polsce (projekt ePaństwo): *"Poprzez kompetencje cyfrowe rozumie się umiejętność efektywnego i swobodnego korzystania z technologii informacyjno-komunikacyjnych, w tym także zdolność do obsługi sprzętu (oprogramowania), rozumienie funkcjonowania Internetu, zdolność korzystania z elektronicznych źródeł informacji oraz świadomość zagrożeń wynikających z korzystania z technologii"*[254].

Wszystkie te definicje podkreślają, że kompetencje cyfrowe nie są ograniczone jedynie do technicznej obsługi urządzeń czy oprogramowania, ale obejmują przede wszystkim umiejętność korzystania z technologii w celu osiągnięcia jasnych, konkretnych celów, zrozumienie kontekstu kulturowego i społecznego, a także rozwój zdolności bezpiecznego korzystania z zasobów cyfrowych oraz krytycznego, zdroworozsądkowego myślenia.

Własna, autorska definicja kompetencji cyfrowych jest następująca: przez kompetencje cyfrowe rozumie się zbiór umiejętności i wiedzy pozwalających na sprawne i bezpieczne korzystanie z technik i technologii cyfrowych w tym komunikowanie się, a także dążenie do ciągłego rozwoju w tej dziedzinie.

Kompetencje cyfrowe obok pisania, czytania, umiejętności matematycznych oraz językowych, stanowią zespół podstawowych umiejętności współczesnego człowieka. Ministerstwo Cyfryzacji podaje, iż kompetencje cyfrowe to harmonijna kompozycja wiedzy, postaw i umiejętności umożliwiających uczenie się, życie i pracę w społeczeństwie cyfrowym, tj. w społeczeństwie, które wykorzystuje w życiu codziennym jak i w pracy - technologie cyfrowe[255].

Ministerstwo Cyfryzacji wskazuje, że na kompetencje cyfrowe składają się trzy zasadnicze elementy[256]:

- kompetencje informatyczne**,** które obejmują posługiwanie się komputerem i innymi urządzeniami cyfrowymi, bezpieczne korzystanie z sieci - internetu, aplikacji i oprogramowania, nowych technologii cyfrowych i zdolność stosowania metod po-

[253] https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#:~:text=In%20DigComp%2C%20digital%20competence%20involves,and%20for %20participation%20in%20society [dostęp 22.11.2023 r.].
[254] https://www.porp.pl/kompetencje-cyfrowe-czy-polska-efektywnie-wykorzystuje-potencjal-technologii-cyfrowych [dostęp 22.11.2023 r.].
[255] https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 19.11.2023 r.]. Szerzej o kompetencjach: zob.: J. Czarkowski *et al.*, 2023, *Zarządzanie Służbą Więzienną oparte na ochronie dynamicznej z wykorzystaniem luki kompetencyjnej*, *The Prison Systems Review*, nr 118, Warszawa.
[256] Ibidem.

chodzących z informatyki przy tworzeniu rozwiązań informatycznych dla problemów z różnych obszarów i dziedzin (tzw. myślenie komputacyjne);

- kompetencje informacyjno-komunikacyjne**,** mające u podstaw umiejętności wyszukiwania informacji, rozumienia, ponadto selekcji i krytycznej oceny, jak również zdalnego komunikowania się na odległość przy pomocy technologii cyfrowych;
- kompetencje funkcjonalne**,** które oznaczają realne wykorzystanie wyżej wymienionych kompetencji w różnych sferach życia, takich jak zdrowie, praca i rozwój zawodowy, finanse, utrzymywanie relacji, hobby, zaangażowanie obywatelskie, życie duchowe itd., zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych.

Kompetencje cyfrowe można podzielić na kilka obszarów lub kategorii. Oto kilka głównych kategorii kompetencji cyfrowych:

Tab. 5.1

Kategorie kompetencji cyfrowych

L.p.	**Umiejętność**	**Opis**
1.	Umiejętność obsługi technologii.	Obsługa urządzeń: umiejętność obsługi komputerów, laptopów, tabletów, smartfonów, a także urządzeń peryferyjnych, takich jak drukarki, skanery itp. Znajomość systemów operacyjnych: zdolność do efektywnej pracy na różnych systemach operacyjnych, takich jak Windows, macOS, Linux czy systemy mobilne (Android, iOS).
2.	Umiejętność korzystania z oprogramowania.	Znajomość pakietów biurowych: umiejętność korzystania z programów do edycji tekstu, arkuszy kalkulacyjnych, prezentacji i innych narzędzi biurowych. Specjalistyczne narzędzia: zdolność do obsługi specjalistycznych programów związanych z daną dziedziną pracy, np. programów graficznych, narzędzi programistycznych itp.
3.	Umiejętność korzystania z Internetu.	Wyszukiwanie informacji online: skuteczne korzystanie z wyszukiwarek internetowych, umiejętność filtrowania wyników i oceny ich wiarygodności. E-commerce: znajomość zasad bezpiecznych trans-

		akcji online, korzystanie z platform zakupowych, umiejętność oceny wiarygodności sklepów internetowych.
4.	Umiejętność komunikacji cyfrowej.	Komunikatory i poczta elektroniczna: zdolność do korzystania z różnych komunikatorów, e-maili, zarządzanie skrzynką pocztową. Media społecznościowe: skuteczne korzystanie z platform społecznościowych, zarządzanie kontem, umiejętność rozróżniania prywatności online.
5.	Umiejętność rozwiązywania problemów cyfrowych.	Diagnozowanie problemów technicznych: rozpoznawanie i rozwiązywanie problemów związanych z funkcjonowaniem urządzeń i oprogramowania. Bezpieczeństwo cyfrowe: umiejętność identyfikacji i reagowania na zagrożenia cybernetyczne, zabezpieczanie systemów przed atakami.
6.	Umiejętność tworzenia treści cyfrowych.	Edycja tekstu i grafiki: zdolność do tworzenia i edycji tekstu, grafiki, a także korzystania z programów do obróbki zdjęć. Tworzenie multimediów: umiejętność tworzenia i udostępniania treści wideo, dźwięku, prezentacji.
7.	Umiejętność zarządzania informacjami.	Zarządzanie danymi: skuteczne przechowywanie, organizowanie i przetwarzanie danych w różnych formatach. Praca w chmurze: korzystanie z usług chmurowych do przechowywania i współdzielenia danych.
8.	Umiejętność współpracy online.	Współpraca zdalna: zdolność do efektywnej współpracy wirtualnej, korzystanie z narzędzi do pracy grupowej online. Zarządzanie projektami: umiejętność planowania, monitorowania i zarządzania projektami online.
9.	Umiejętność krytycznego myślenia	Rozpoznawanie dezinformacji: umiejętność identyfikacji fałszywych informacji, rozumienie mechanizmów dezinformacji online.

	cyfrowego.	Krytyczna ocena treści: zdolność do krytycznej oceny treści cyfrowych, zrozumienie kontekstu i źródła informacji.
10.	Umiejętność dbania o bezpieczeństwo prywatności.	Zarządzanie danymi osobowymi: ochrona swoich danych osobowych, zrozumienie zasad prywatności online. Kontrola dostępu: skuteczne zarządzanie ustawieniami prywatności na różnych platformach i usługach online.

Źródło: opracowanie własne na podstawie R. Vuorikari, S. Kluzer, Y. Punie, 2022, *DigComp 2.2. The Digital Competence Framework for Citizens, Luxembourg Publications Office of the European Union.*

Podział kompetencji cyfrowych może być bardziej szczegółowy i uwzględniać dodatkowe aspekty w zależności od konkretnego kontekstu i ram odniesienia. Warto jednak pamiętać, że kompetencje cyfrowe nie są statycznymi umiejętnościami, ale rozwijają się wraz z rozwojem technologii i potrzeb społecznych.

5.2. Społeczna świadomość cyberzagrożeń i poziom kompetencji cyfrowych

Rozważania dotyczące świadomości cyberzagrożeń wśród uczniów szkół podstawowych oraz nauczycieli należy rozpocząć od aktu prawnego, który stanowi wykładnię kształcenia w szkołach, jakim jest Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. *w sprawie podstawy programowej* […][257].

Kształcenie w szkołach podstawowych jest fundamentem wykształcenia, a zadaniem szkoły łagodne wprowadzenie dziecka do świata wiedzy. Nauka w szkołach oparta jest o dwa etapy, pierwszy obejmuje klasy I-III – jest to tzw. edukacja wczesnoszkolna, zaś II etap – IV-VIII. Do najważniejszych umiejętności rozwijanych w ramach ogólnego kształcenia w szkole podstawowej zalicza się: rozwijanie problemów w sposób kreatywny świadomie wykorzystując narzędzia i metody wywodzące się z informatyki; programowanie; krytyczną analizę i wykorzystywanie informacji spośród różnych źródeł; posługiwanie się komputerem i urządzeniami cyfrowymi; stoso-

[257] Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz. U. 2017 r. poz. 356 z późn. zm.).

wanie nabytych umiejętności w pracy z tekstem, obliczeniami, przetwarzaniem informacji i prezentacji w różnych postaciach[258].

Wraz z wprowadzeniem nowej podstawy programowej do szkół podstawowych (2017 r.) i ponadpodstawowych (2018 r.) kształcenie informatyczne zostało unowocześnione w Polsce i objęto nim wszystkich uczniów. Jego zasadniczym założeniem jest kształtowanie tzw. komputacyjnego myślenia prowadzącego do bezpiecznego i efektywnego wykorzystania metod oraz technik wypływających z informatyki podczas rozwiązywania problemów z różnych dziedzin życia. Od pierwszej klasy szkoły podstawowej, przez wszystkie lata szkolnej edukacji w ramach przedmiotów informatycznych (edukacja informatyczna, informatyka) jest realizowanych w sposób spiralny pięć podstawowych celów[259]:

1. Rozumienie, analizowanie, rozwiązywanie problemów na bazie abstrakcyjnego i logicznego myślenia, myślenia algorytmicznego i sposobów reprezentowania informacji.
2. Programowanie oraz rozwiązywanie problemów z wykorzystaniem komputera i innych urządzeń cyfrowych: układanie wraz z programowaniem algorytmów, wyszukiwanie, organizowanie i udostępnianie informacji, posługiwanie się komputerowymi aplikacjami.
3. Posługiwanie się komputerem, cyfrowymi urządzeniami oraz sieciami komputerowymi, w tym także: znajomość zasad działania sieci komputerowych i urządzeń cyfrowych oraz wykonywanie obliczeń i programów.
4. Rozwijanie kompetencji społecznych, tj.: komunikacja oraz współpraca w grupie, w tym także w środowiskach wirtualnych, udział w projektach oraz organizacja i nimi zarządzanie.
5. Przestrzeganie prawa oraz zasad bezpieczeństwa. Respektowanie prywatności informacji wraz z ochroną danych, praw własności intelektualnej, ponadto znajomość etykiety w komunikacji i norm współżycia społecznego. Ocena zagrożeń związanych z technologią oraz uwzględnienie dla bezpieczeństwa swojego i innych.

Od wielu lat komputery i postępująca cyfryzacja wywierają coraz bardziej znaczący wpływ na zmiany zachodzące w funkcjonowaniu społeczeństwa: w gospodarce, bankowości, administracji, handlu, nauce i edukacji, komunikacji czy życiu osobistym obywateli.

[258] Ibidem, zał. nr 2, s. 11-31.
[259] Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.), s. 17.

Co warto podkreślić, cyfryzacja wymuszona została czwartą rewolucją przemysłową, zaś rozwój procesów *ICT*, usług oraz produktów to podstawy do określanej mianem Przemysł 5.0 – piątej rewolucji przemysłowej. Związana będzie z podniesieniem poziomu komunikacji maszyn z ludźmi dzięki optymalizacji wspomnianych działań przy użyciu *AI*, analityki *machine learningu* czy technologii *blockchain*[260].

Dziedzina wiedzy - informatyka wraz z technologiami, które wspiera, integruje się z niemal wszystkimi pozostałymi dziedzinami i staje się ich nierozerwalnym elementem. Wczesny kontakt w szkole z tym przedmiotem powinien przybliżyć uczniom możliwości jego zastosowań oraz wzbudzić zainteresowanie informatyką. Zakłada się, iż wkraczający w dorosłe życie uczniowie będą właściwie przygotowani do podjęcia wyzwań i obowiązków, jakie stawia przed nimi XXI wiek. Powinni oni zatem poznać podstawowe metody informatyki, tak aby w przyszłości móc stosować je w sytuacjach praktycznych w różnych dziedzinach. Dotychczas dużą uwagę w edukacji przywiązywano do kształcenia umiejętności korzystania z aplikacji i zasobów oraz komunikacji w sieci. Obecnie oczekiwane kompetencje obywateli wykraczają poza tradycyjnie rozumianą tzw. alfabetyzację komputerową i biegłość w obszarze korzystania z technologii. Umiejętności te są nadal potrzebne, jednak nie są już wystarczające dziś, gdy informatyka staje się językiem powszechnym niemal każdej dziedziny życia. Główne zadanie szkoły – alfabetyzacja w zakresie czytania, pisania oraz rachowania – wymaga rozszerzenia o alfabetyzację w obszarze umiejętności rozwiązywania problemów z różnych dziedzin biorąc pod uwagę świadome wykorzystanie metod i narzędzi wywodzących się z informatyki. Umiejętność programowania staje się elementem kształcenia powszechnego. Programowanie jest rozumiane szerzej niż jedynie samo napisanie programu w języku programowania. Jest to proces, obejmujący informatyczne podejście do rozwiązywania problemu: począwszy od specyfikacji problemu poprzez znalezienie i opracowanie rozwiązania, aż do zaprogramowania rozwiązania, testu jego poprawności i korekty przy użyciu właściwie dobranej aplikacji bądź języka programowania. Tak określone programowanie stanowi część zajęć z informatyki już od najmłodszych lat, ma wpływ na sposób nauczania innych przedmiotów, służy odpowiedniemu rozumieniu pojęć informatycznych oraz metod informatyki. Wspomaga kształcenie następujących umiejętności: precyzyjne prezentowanie myśli i pomysłów, logiczne myślenie, sprzyja

[260] Zob. S. Szybowska, 2024, *Środki zarządzania ryzykiem w cyberbezpieczeństwie w polityce bezpieczeństwa ICT i wyzwaniach prawnych,* [w:] *Wielowymiarowość cyberbezpieczeństwa,* J. Żylińska, K. Huczek, K. Borkowski (red.), Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej, Warszawa, s. 262-277.

dobrej organizacji pracy, buduje kompetencje przydatne w pracy zespołowej i efektywnej realizacji projektów. Nabyte podczas programowania umiejętności są przydatne na zajęciach z różnych przedmiotów, jak i później w życiu dorosłym, w różnych zawodach, niekoniecznie informatycznych. Ogólne cele kształcenia informatycznego są niezmienne, dla wszystkich etapów edukacyjnych. Opis szczegółowych wymagań ma charakter przyrostowy – każdy kolejny etap edukacyjny wymaga od uczniów umiejętności zdobytych podczas wcześniejszych etapów edukacyjnych i rozszerza się je o umiejętności nowe[261].

Od klasy IV zajęcia z informatyki zaczynają mieć bardziej formalny charakter. Uczniowie zajmują się sytuacjami problemowymi, przedstawianymi w sposób opisowy (również za pomocą ilustracji i historyjek), ale tworzą je samodzielnie i abstrahują z nich działania, z których tworzą własne realizacje jako programy lub czynności wykonywane w innych programach. W ten sposób rozwijają i poszerzają podejście algorytmiczne w rozwiązywaniu sytuacji problemowych z różnych dziedzin. Posługując się komputerem rozwijają również umiejętności wyrażania własnych myśli oraz ich prezentacji, które potrafią wykonywać indywidualnie, a także zespołowo. W sieci poszukują danych i informacji przydatnych w rozwiązywaniu stawianych zadań oraz problemów. Doceniając rolę współpracy w rozwoju swojej wiedzy i umiejętności są w stanie postępować odpowiedzialnie i etycznie w komputerowo-sieciowym środowisku.

Od klasy VII uczniowie realizujący informatykę w klasach IV-VI (dla 6-letniej szkoły), wprowadzani są do algorytmicznego myślenia poznając zasadnicze pojęcia informatyki. Zdobyte do tej pory umiejętności i wiedza są rozwijane, uczniowie rozpoczynają wizualne bądź tekstowe języki programowania. Wykorzystując dostępne oprogramowanie uczniowie przygotowują projekty i rozwijają kompetencje grupowego rozwiązywania problemów z różnych dziedzin. W czasie trwania zajęć każdy uczeń powinien mieć do dyspozycji osobny komputer z dostępem do sieci i odpowiednim oprogramowaniem. Ponadto, realizując projekt (zespołowy bądź indywidualny) uczeń powinien mieć zapewnioną możliwość korzystania z komputerów lub innych urządzeń cyfrowych, zależnie od swoich.

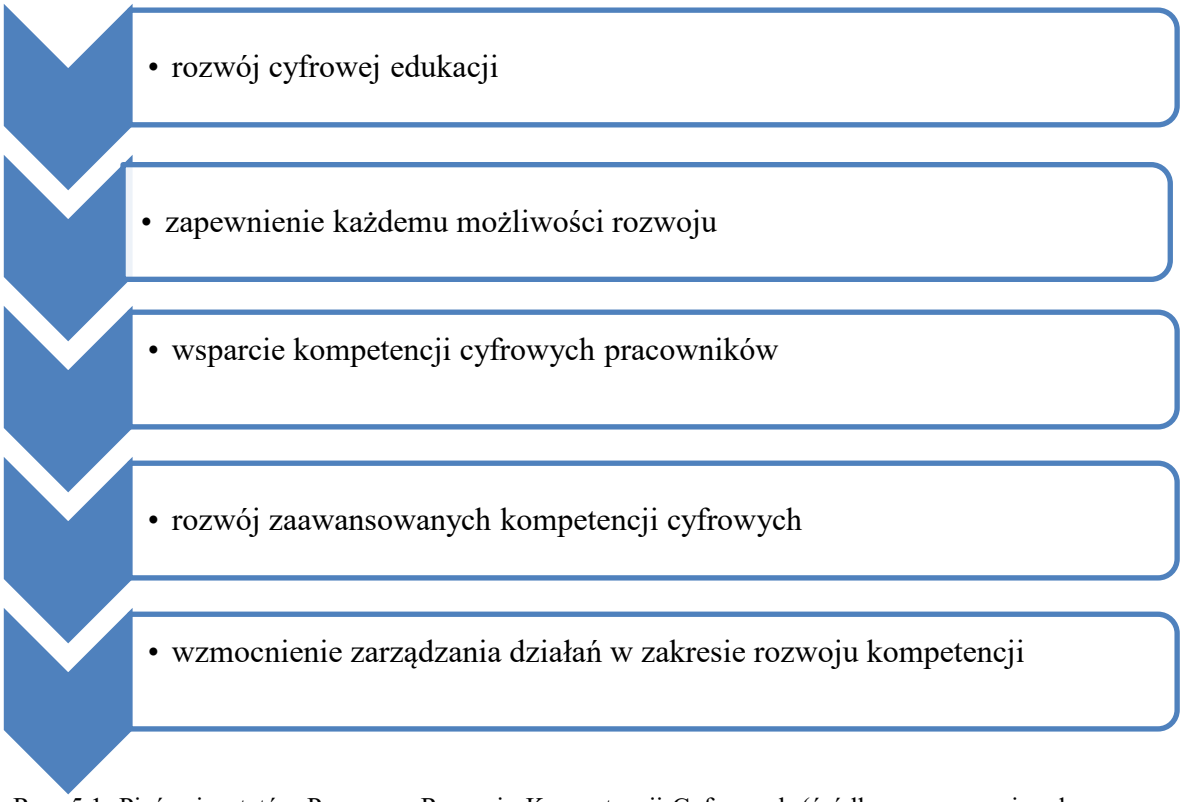
W odpowiedzi na wiele nowych wyzwań w obszarze rozwoju cyfrowego i nieustannie zmieniającym się świecie, w 2023 roku stworzono *Program Rozwoju*

[261] Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej, op. cit. zał. nr 2, s. 26-27.

Kompetencji Cyfrowych[262], który jako zasadniczy cel zakłada wzrost poziomu cyfrowych kompetencji poprzez zapewnienie ich każdemu obywatelowi Polski. W program wpisują się osoby edukacji przedszkolnej, wczesnoszkolnej, jak i osoby wieku senioralnego. Wsparcie programu kierowane jest do wszystkich, którzy chcą podnosić swoje umiejętności i kompetencje cyfrowe, w tym nauczyciele, pracownicy wszystkich sektorów gospodarki, urzędnicy, przedsiębiorcy i osoby utalentowane cyfrowo, mające w przyszłości zasilić szeregi specjalistów IT. Projekt zawiera inicjatywy, które pozwolą zwiększyć świadomość dotyczącą korzystania z technologii cyfrowych i propagowanie tzw. higieny cyfrowej[263].

Punkt wyjścia do sformułowania celów, działań i priorytetów w ramach Programu stanową krajowe i europejskie dokumenty strategiczne oraz analiza obecnego stanu kompetencji cyfrowych w Polsce. Program polityki *Droga ku cyfrowej dekadzie* do roku 2030 wyznaczył dwa cele dla Unii Europejskiej: co najmniej 80% społeczeństwa w przedziale wiekowym 16-74 lat wyposażona będzie w przynajmniej podstawowe umiejętności cyfrowe oraz minimum 20 milionów pracowników UE stanowić będą specjaliści *ICT*, zaś dysproporcje pomiędzy mężczyznami, a kobietami praktycznie nie wystąpią. Kolejnym dokumentem jest: *Plan działań w dziedzinie edukacji cyfrowej 2021-2027*, wskazujący na wykorzystanie potencjału sieci celem udostępnienia społeczeństwu możliwości e-edukacji; wsparcie i współpracę z krajami UE na rzecz dostosowywania własnych systemów kształcenia oraz zasadniczo zwiększenie umiejętności cyfrowych[264]. Przygotowanie samego programu rozpoczęło się od licznych spotkań i warsztatów z wieloma ekspertami działającymi w obszarze rozwoju kompetencji cyfrowych.

[262] Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.).
[263] https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.].
[264] https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.].



Rys. 5.1. Pięć priorytetów Programu Rozwoju Kompetencji Cyfrowych (źródło: opracowanie własne na podstawie: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.])

Rada Ministrów przyjęła uchwałę dotyczącą ustanowienia programu rozwoju kompetencji cyfrowych, którego koszt określono na ponad 2 mld 789 mln zł. Młode pokolenie - bez wątpienia, już w szkole podstawowej musi budować te kompetencje, aby później być w stanie konkurować na rynku pracy. *Pamiętajmy, że już dziś jesteśmy liderem w szkoleniu i zatrudnianiu kobiet w IT. Celem programu, który będziemy realizować do 2030 r. jest podniesienie poziomu kompetencji cyfrowych w społeczeństwie oraz rozwój edukacji cyfrowej* – zaznacza Paweł Lewandowski, Podsekretarz Stanu w Kancelarii Prezesa Rady Ministrów[265].

Zakładane efekty realizacji programu, stan planowany na rok 2030[266]:

- 80 % mieszkańców Polski będzie posiadać co najmniej podstawowe kompetencje cyfrowe;
- 40 % mieszkańców Polski dysponować będzie ponadpodstawowymi kompetencjami cyfrowymi,
- 6 % pracujących będą stanowić specjaliści IT;
- 29 % specjalistów IT to kobiety.

[265] https://www.gov.pl/web/cyfryzacja/ponad-25-mld-na-program-rozwoju-kompetencji-cyfrowych [dostęp 17.12.2023 r.].
[266] Ibidiem.

Poniżej prezentowane dane wskazują, jak niezwykle istotny program został zainicjowany, aby społeczeństwo mogło się rozwijać lepiej. W roku 2021 około 16 mln Polaków (57%) w wieku 16-74 lat nie dysponowało nawet podstawowymi kompetencjami cyfrowymi, zaś u seniorów (65-74) było to dziewięć na dziesięć osób. Co czwarty Europejczyk posiadał ponadpodstawowe umiejętności cyfrowe, natomiast w Polsce – była to co piąta osoba. Wykluczeni cyfrowo – blisko 80 % społeczeństwa – stanowili seniorzy, osoby powyżej 60 roku życia. Niepełnosprawni korzystający z pomocy społecznej – a niekorzystający z sieci, to blisko 45 % badanych[267].

W Polsce od kwietnia do października 2022 roku przeprowadzono certyfikowany *IT Fitness Test* - sprawdzian kompetencji cyfrowych, który po raz pierwszy objął swoim zasięgiem szkoły podstawowe oraz ponadpodstawowe. Za projektem stoi branża cyfrowa[268], przygotowująca rekomendacje dla szkół, mających wesprzeć w prawidłowym rozwijaniu i kształceniu kompetencji cyfrowych uczniów.

Sprawdzianowi poddano niemal 30 tys. uczniów szkół podstawowych oraz ponadpodstawowych i ich nauczycieli. Egzamin podzielono na pięć kategorii: Internet, bezpieczeństwo, rozwiązywanie problemów, narzędzia współpracy i sieci społecznościowe. W szkołach podstawowych uczniowie rozwiązali średnio 45% zadań poprawnie, zaś ponadpodstawowych – 40%. Największe problemy sprawiło wykorzystywanie programów komputerowych, głównie arkuszy kalkulacyjnych (szkoły podstawowe: 38%, ponadpodstawowe: 26% prawidłowych odpowiedzi). Tzw. myślenie algorytmiczne lepiej wypada, jeśli chodzi o szkoły podstawowe (45%), zaś licea i technika to zaledwie 34%. Co zastanawiające, wyniki w obszarze korzystania z sieci społecznościowych również dają wiele do myślenia (podstawówki: 39% i ponadpodstawówki: 39%). A przecież mogłoby się wydawać, że większość osób wie, w jaki sposób korzystać z tzw. *social mediów*. Nieco bardziej optymistycznie można spojrzeć na teorię, znajomość zasad bezpiecznego zachowania w sieci – odpowiednio 57% oraz 53%[269].

Na poziomie szkół podstawowych najwyżej ocenieni zostali uczniowie z Dolnego Śląska, zaś najsłabiej zaprezentowało się województwo lubuskie. Równocześnie *Fitness Test* był prowadzony w Grupie Wyszechradzkiej, Polacy zaprezentowali niemalże ten sam poziom co Słowacy i Czesi. Gorsze wyniki natomiast osiągnęli Wę-

[267] https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.].

[268] Związek Cyfrowa Polska jest branżową organizacją pracodawców o charakterze non-profit. Zrzesza największe firmy z branży RTV i IT w Polsce. Obejmuje zarówno producentów, importerów jak i dystrybutorów sprzętu elektrycznego i elektronicznego.

[269] https://cyfrowapolska.org/pl/umiejetnosci-cyfrowe-polskich-uczniow-do-poprawy-znamy-wyniki-pierwszego-w-polsce-cyfrowego-testu/ [dostęp 17.12.2023 r.].

grzy. *„Kompetencje cyfrowe są dzisiaj kluczowe i nie wyobrażamy sobie sprawnego życia i funkcjonowania bez nich. Dlatego tak ważne jest monitorowanie ich poziomu, który nie tylko buduje świadomość, ale również pozwala nam na bieżąco reagować na potrzeby uczniów jak i całego społeczeństwa w systemie edukacji”*– podsumowała Justyna Orłowska, Pełnomocnik Prezesa Rady Ministrów ds. *GovTech* – Szef Centrum *GovTech*, Pełnomocnik Ministra Edukacji i Nauki ds. Transformacji Cyfrowej[270].

Przykład *IT Fitness Testu* stanowi o tym, jakiego znaczenia nabierają kompetencje cyfrowe i jakie znaczenie mają na obecnym rynku pracy. Bardzo dobrze, że formuła ta objęła swoim zasięgiem również sąsiadów Polski, co pozwala na szersze ujęcie i możliwość porównania naszych uczniów z pozostałymi. Najbardziej istotne jednak są rekomendacje i wnioski z przeprowadzonych badań, które skłonić powinny do refleksji i m.in. realizacji samoedukacji w opisywanym obszarze.

Wyniki testu przeprowadzonego w 2023 roku nie napawają optymizmem. Alarmującym może być fakt, iż polscy uczniowie znaleźli się na końcu stawki, za rówieśnikami z Czech, Słowacji oraz Węgier. Szczegółowych informacji na ten temat jednak nie podano.

Sprawdzeniu poddano blisko 23 tys. uczniów, nauczycieli i rodziców. Wśród uczniów szkół podstawowych średnia odpowiedzi dla całej Polski wzrosła o 1 punkt procentowy w porównaniu do roku 2022. Wyniki poszczególnych kategorii obrazuje poniższe zestawienie. Warto zwrócić uwagę na spadek o aż 6 pkt. proc. w porównaniu do roku poprzedniego.

Rys. 5.2. *IT Fitness Test 2023* – szkoły podstawowe (źródło: https://cyberdefence24.pl/cyberbezpieczenstwo/znamy-wyniki-testu-umiejetnosci-cyfrowych-w-polskich-szkolach-nie-jest-najlepiej- [dostęp 17.02.2024 r.])

[270] Ibidem.

Jak podaje Związek Cyfrowa Polska - uczniowie szkół ponadpodstawowych dokonali wyboru 43 % właściwych odpowiedzi (co stanowi wzrost o 3 pkt proc. w porównaniu do roku poprzedniego)[271].

5.3. Analiza porównawcza kompetencji cyfrowych na tle wybranych państw

Źródeł niezbędnych do porównań danych dotyczących poziomu kompetencji cyfrowych jest wiele, aczkolwiek jedynie część z nich jest powszechnie dostępna. Wiele państw przeprowadza badania dotyczące umiejętności cyfrowych uczniów jako część ogólnokrajowych ocen edukacyjnych. Takie badania mogą obejmować różne aspekty kompetencji cyfrowych. Międzynarodowe instytucje edukacyjne, takie jak *Organizacja Współpracy Gospodarczej i Rozwoju (OECD)*, przeprowadzają międzynarodowe badania umiejętności uczniów, w tym kompetencji cyfrowych. Przykładem takiego badania jest program *PISA (Programme for International Student Assessment).* Jest to międzynarodowe badanie umiejętności uczniów na świecie, realizowane cyklicznie co trzy lata w krajach członkowskich *OECD*, a także w kilkudziesięciu innych państwach. Polska uczestniczy od samego początku, tj. od roku 2000. Natomiast od 2013 roku, zgodnie z decyzją ówczesnego Ministerstwa Edukacji Narodowej, badanie w naszym kraju prowadzone jest przez Instytut Badań Edukacyjnych.

W każdej edycji nacisk ukierunkowywany jest na jedną z następujących dziedzin: umiejętności matematyczne, rozumienie czytanego tekstu lub rozumowanie w naukach przyrodniczych. Do zasadniczego badania dołączane są dodatkowe komponenty, zarówno krajowe, jak i międzynarodowe, poszerzające zakres badania o inne dziedziny, np. umiejętności finansowe. Badanie kierowane jest zawsze do uczniów, którzy rok przed realizacją badania ukończyli 15 lat. Wskazanie badania *PISA* jest zasadne w kwestii możliwości rozwoju kompetencji cyfrowych ogółem.

W niektórych regionach szkoły i instytucje edukacyjne przeprowadzają własne oceny kompetencji cyfrowych uczniów. Mogą to być testy, projekty edukacyjne czy oceny wyników z codziennego korzystania z technologii w ramach procesu nauczania i uczenia się. Instytucje badawcze, uniwersytety i organizacje edukacyjne często przeprowadzają badania mające na celu ocenę poziomu kompetencji cyfrowych wśród uczniów. Wyniki takich badań mogą dostarczyć cennych informacji na temat skuteczności programów edukacyjnych.

[271] https://cyberdefence24.pl/cyberbezpieczenstwo/znamy-wyniki-testu-umiejetnosci-cyfrowych-w-polskich-szkolach-nie-jest-najlepiej [dostęp 17.02.2024 r.].

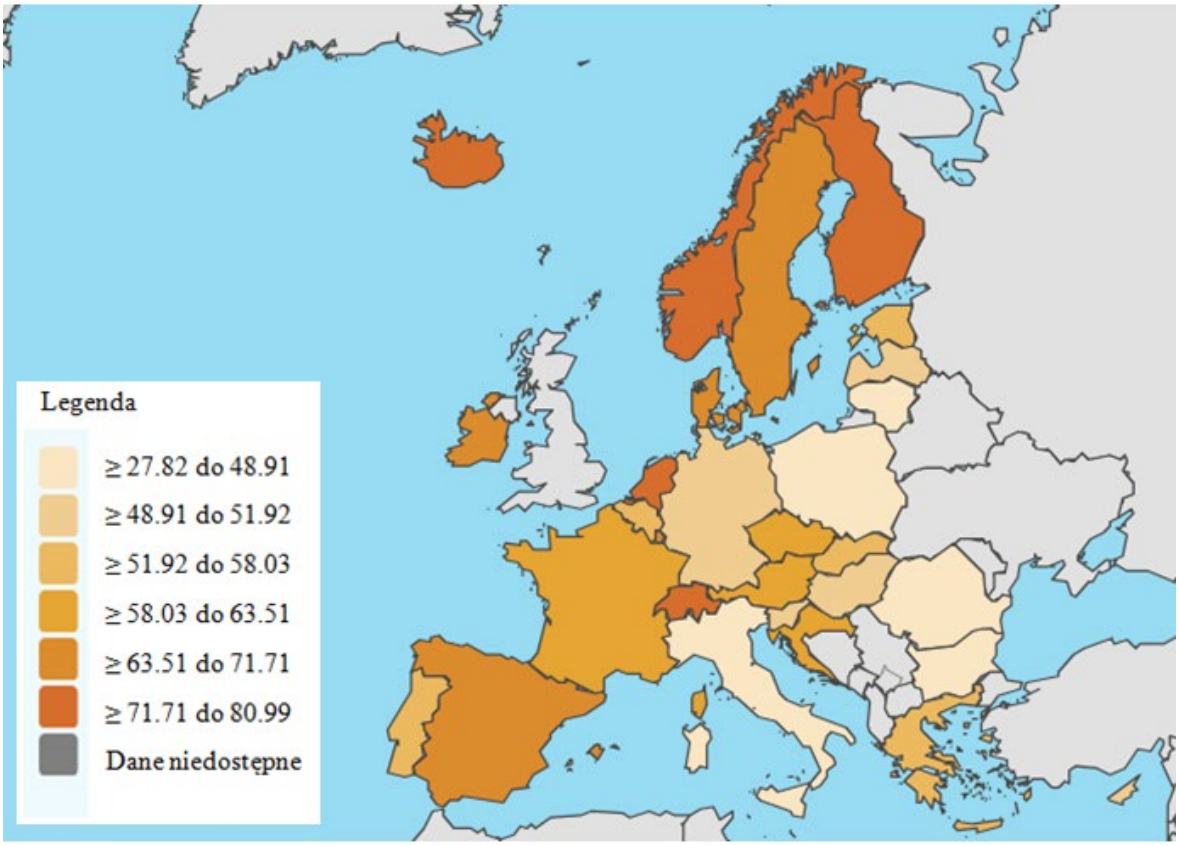
Ramy Kompetencji Cyfrowych dla Obywateli *(DigComp)* stanowią próbę zapewnienia wspólnego jednolitego języka i opisu kluczowych obszarów cyfrowych kompetencji. *DigComp* jest ogólno-unijnym narzędziem do podnoszenia cyfrowych kompetencji obywateli, planowania inicjatyw edukacyjnych i polityk wspierających. Od 2013 roku *DigComp* został wdrożony celem skonstruowania Wskaźnika Umiejętności Cyfrowych *(DSI)*, który natomiast wykorzystywany jest do celów politycznych oraz monitorowania społeczeństwa i gospodarki cyfrowej *(DESI)*[272]. Kompetencje cyfrowe w *DigComp* określone są przez pięć obszarów kompetencji: informacja i dane; komunikacja i współpraca; tworzenie treści cyfrowych; bezpieczeństwo oraz rozwiązywanie problemów. Trzy pierwsze obszary mieszczą się w określonych działaniach i zastosowaniach. Obszary czwarty oraz piąty są „przekrojowe", albowiem dotyczą każdego rodzaju prowadzonej działalności przy pomocy środków cyfrowych.

Warto zauważyć, że podział na obszary i kompetencje ramowe wydaje się nieco sztuczny i w rzeczywistości różne obszary i kompetencje często nakładają się i nawiązują do siebie. Również charakter obszarów nie zawsze jest jednoznaczny. Prawdopodobnie obszar „Rozwiązywanie problemów" jest najbardziej przekrojowy ze wszystkich i dlatego kompetencje, które obejmuje można znaleźć we wszystkich innych obszarach.

Wskaźnik poziomu rozwoju cyfrowego państw członkowskich Unii Europejskiej - *Indeks Cyfrowej Gospodarki i Społeczeństwa Cyfrowego (The Digital Economy and Society Index - DESI)* wskazuje na niezbędną konieczność intensyfikacji działań w zakresie cyfrowej transformacji Polski. Bowiem jak wspomniano, indeks *DESI* syntetyzuje osiągnięcia poszczególnych krajów w czterech wymiarach: łączność (dostęp do Internetu), kapitał ludzki, integracja technologii cyfrowych w przedsiębiorstwach, cyfrowe usługi publiczne. Do każdego komponentu przyporządkowuje się wskaźniki cząstkowe z przypisaną wagą. Według indeksu *DESI*, w 2022 roku Polska zajęła odległe 24. miejsce (na 27 uczestników - państw członkowskich).

Poniższa mapa (rysunek) obrazuje poziom umiejętności użytkowników w zakresie kompetencji cyfrowych. Nietrudno zauważyć, iż prym wiodą państwa skandynawskie oraz część państw Europy Zachodniej. Podział z uwzględnieniem poszczególnych wartości ujęto na kolejnym wykresie.

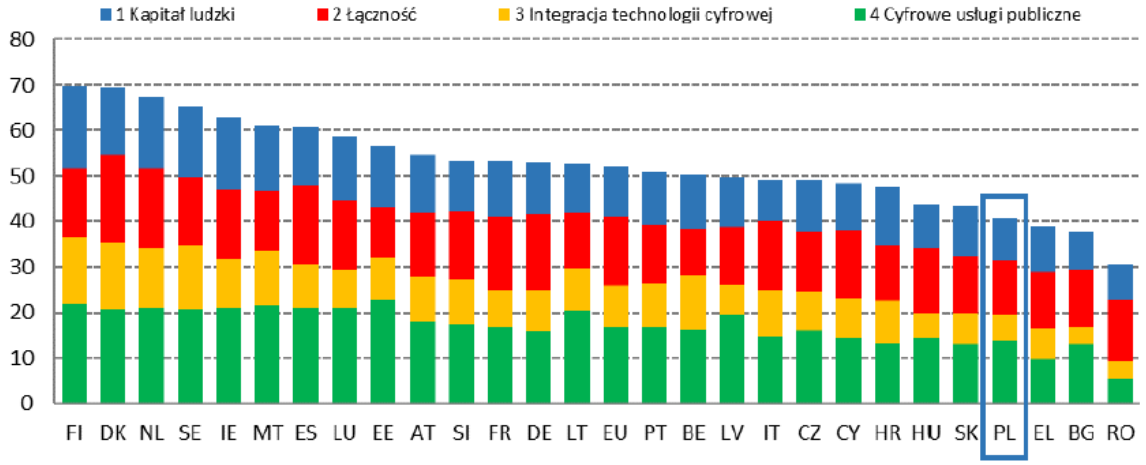
[272] https://www.digcomp.pl/wp-content/uploads/2023/03/DigComp2.2_TEXT_pl_.pdf [dostęp 17.02.2024 r.].



Rys. 5.3. Poziom indywidualnych umiejętności cyfrowych w krajach UE - 2021 r. (źródło:https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21__custom_2397093/bookmark/map?lang=en&bookmarkId=dc481686-c938-4e07-b03c-8e039f532857 [dostęp 17.12.2023 r.])

Poniższy wykres przedstawia, iż wynik *DESI* przekroczył nieco średnią unijną, co może świadczyć o tym, że Polska powoli zbliża się do średniej UE i kierunek ten jest jak najbardziej właściwy. Nadal jednak występuje luka w kategorii „Kapitał ludzki", w której to Polska plasuje się na 24. pozycji niespełniającej średniej. Polska nadal zajmuje niskie miejsce w dziedzinie absolwentów kierunków w dziedzinie *ICT*, niedobór ten ma istotny wpływ na implementację technologii cyfrowych przez instytucje i przedsiębiorstwa. Przyszłość nie rysuje się niestety w jasnych barwach zważając na realnie niski wskaźnik naboru na studia[273]. Cyfryzacja stanowi jeden z priorytetów rządzących, jak już wspomniano powyżej przykładem tego działania jest ustanowienie Programu Rozwoju Kompetencji Cyfrowych.

[273] https://digital-strategy.ec.europa.eu/pl/policies/desi-poland [dostęp 17.12.2023 r.].



Wykres 5.1. Ranking indeksu gospodarki cyfrowej i społ. cyfrowego w krajach UE - 2022 r. (źródło: https://digital-strategy.ec.europa.eu/pl/policies/desi-poland– [dostęp 17.12.2023 r.])

Wskaźnik umiejętności cyfrowych 2.0 (*Digital Skills Indicator - DSI*) jest złożonym wskaźnikiem opartym na wybranych czynnościach związanych z korzystaniem z sieci (Internetu) bądź oprogramowania, które osoby w wieku od 16 do 74 lat wykonują w określonych obszarach (umiejętność korzystania z informacji oraz danych, komunikacja i współpraca, tworzenie cyfrowych treści, bezpieczeństwo oraz rozwiązywanie problemów). Założenie jest następujące: osoby, które wykonały określone czynności, posiadają właściwe - odpowiednie umiejętności. Dlatego wskaźniki te uznawane są za przybliżenie umiejętności cyfrowych dla poszczególnych osób. Zależnie od różnorodności wykonywanych czynności, dla każdego z pięciu obszarów wyróżnia się dwa poziomy umiejętności ("podstawowe" i "ponadpodstawowe"). Ponadto, dzięki wskaźnikom składowym dla każdego obszaru, wyliczany jest ogólny wskaźnik umiejętności cyfrowych stanowiący przybliżenie umiejętności cyfrowych poszczególnych osób ("brak umiejętności", "ograniczone", "wąskie", "niskie", "podstawowe", "powyżej podstawowych" lub "co najmniej podstawowe umiejętności")[274].

Poniżej wskazano i opisano poszczególne obszary:

1. Umiejętność korzystania z danych i informacji.

Jest to wyrażanie potrzeb informacyjnych, wyszukiwanie i lokalizowanie danych cyfrowych, informacji i treści. Ocena i opinia przydatności źródła, a także jego zawartości. Magazynowanie (przechowywanie), zarządzanie, organizowanie danych, informacji oraz treści. Działania niezbędne do obliczania umiejętności korzystania z danych i informacji:

- wyszukiwanie informacji o usługach lub towarach;

[274] https://ec.europa.eu/eurostat/cache/metadata/en/isoc_sk_dskl_i21_esmsip2.htm [dostęp 10.06.2023 r.].

- poszukiwanie informacji dotyczących zdrowia;
- czytanie serwisów informacyjnych, gazet lub magazynów informacyjnych;
- czynności związane ze sprawdzaniem informacji online oraz ich źródeł.

2. Umiejętności komunikacji i współpracy.

Opisywane są w interakcji, komunikacji, współpracy przy wsparciu technologii cyfrowych przy jednoczesnej świadomości różnorodności pokoleniowej i kulturowej. Uczestnictwo w życiu społecznym przez prywatne oraz publiczne usługi cyfrowe, a także tzw. obywatelstwo partycypacyjne. Działania wykorzystywane do wyliczania umiejętności komunikacji i współpracy:

- odbieranie/ wysyłanie wiadomości e-mail;
- rozmowy/ telefonowanie wideo przez internet;
- uczestnictwo w sieciach społecznościowych – tzw. social media;
- komunikatory internetowe;
- wyrażanie opinii na tematy polityczne (obywatelskie) na stronach internetowych albo w mediach społecznościowych;
- udział online w konsultacjach lub głosowanie.

3. Umiejętność tworzenia treści cyfrowych.

Obejmuje działania tworzenia i edytowania treści cyfrowych, ulepszania i integrowania informacji i treści ze zbiorem wiedzy przy jednoczesnym zrozumieniu, jak należy stosować licencje i prawa autorskie. Umiejętność wydawania zrozumiałych instrukcji dla systemu komputerowego.

Czynności wykorzystywane do obliczania umiejętności tworzenia cyfrowych treści:

- korzystanie z arkusza kalkulacyjnego i edytora tekstu;
- edycja zdjęć, plików audio lub wideo;
- kopiowanie bądź przenoszenie plików (dokumenty, dane, obrazy, wideo) między urządzeniami i folderami (poprzez e-mail, komunikator, usb) lub w chmurze;
- tworzenie i organizowanie plików (dokumenty, obrazy, filmy) zawierających kilka elementów, np. tekst, wykres, obraz, tabela, animacja albo dźwięk;
- korzystanie z funkcji zaawansowanych oprogramowania arkusza kalkulacyjnego (formuł, funkcji, makr i pozostałych programistycznych funkcji) celem analizowania, organizowania, modyfikowania lub strukturyzowania danych;
- pisanie kodu językiem programowania.

4. Umiejętności związane z bezpieczeństwem.

Obejmuje ochronę urządzeń, treści, danych osobowych oraz prywatności w środowiskach cyfrowych. Ponadto, ochronę zdrowia fizycznego i psychicznego, a także świadomość technologii cyfrowych w zakresie integracji społecznej. Samoświadomość wykorzystania technologii cyfrowych i ich wpływ na środowisko.

Działania wykorzystywane do obliczania bezpieczeństwa:

- zarządzanie dostępem do danych osobowych (własnych) przez czytanie oświadczeń o ochronie prywatności przed podaniem danych;
- zarządzanie dostępem do danych osobowych (własnych) przez sprawdzenie, czy dana strona internetowa, na której respondent podał dane osobowe była bezpieczna;
- zarządzanie dostępem do danych osobowych (własnych) przez ograniczenie bądź odmowę dostępu do lokalizacji geograficznej (własnej);
- zarządzanie dostępem do danych osobowych (własnych) przez odmowę zgody na wykorzystanie danych osobowych w celach reklamowych;
- zmiana ustawień w przeglądarce internetowej celem uniemożliwienia bądź ograniczenia plików *cookie* na dowolnym urządzeniu właściciela;
- zarządzanie dostępem do danych osobowych (własnych) przez ograniczenie dostępu do profilu lub treści w serwisach społecznościowych lub współdzielonej pamięci online.

5. Umiejętność rozwiązywania problemów.

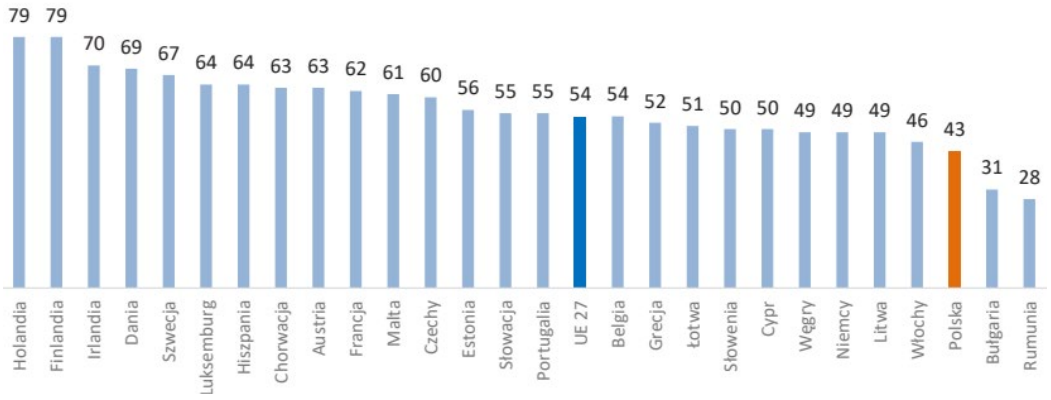
Umiejętność ta związana jest z właściwym identyfikowaniem potrzeb i problemów, a także rozwiązywaniem problemów koncepcyjnych i sytuacji problemowych w cyfrowych środowiskach. Oznacza wykorzystywanie narzędzi cyfrowych do wprowadzania innowacji w produktach oraz procesach. Rozumie się przez to również bycie na bieżąco z ewolucją cyfrową.

Działania wykorzystywane do wyliczania umiejętności rozwiązywania problemów:

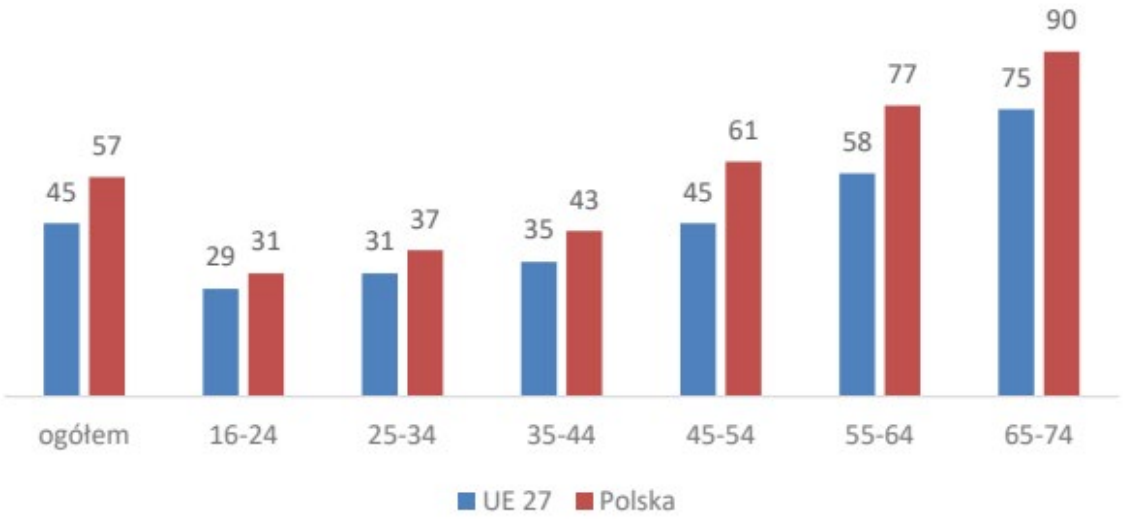
- pobieranie/ instalowanie oprogramowania lub aplikacji;
- zakupy i sprzedaż online;
- zmiana ustawień urządzenia, oprogramowania, aplikacji;
- używanie zasobów edukacyjnych - online;
- szukanie pracy bądź wysyłanie podania o pracę;
- korzystanie z usług bankowości internetowej.

Poniższy wykres przedstawia odsetek osób z podstawowymi ogólnymi umiejętnościami cyfrowymi (wszystkie pięć wskaźników składowych jest na poziomie podstawowym lub powyżej podstawowego, ale nie wszystkie są powyżej podstawowego).

Do najsłabiej rozwiniętych państw w tym zakresie należą: Rumunia (28%), Bułgaria (31%) oraz Polska (43%). Natomiast najwyżej w wybranej klasyfikacji są: Niderlandy, Finlandia (po 79%) oraz Irlandia (70%).



Wykres 5.2. Poziom indywidualnych umiejętności cyfrowych w krajach UE- 2021 r. (źródło: https://www.weforum.org/agenda/2022/04/europe-basic-digital-skills/ [dostęp-03.05.2023 r.])



Wykres 5.3. Odsetek osób nieposiadających co najmniej podstawowych umiejętności cyfrowych wg wieku w Polsce, w porównaniu do średniej z krajów UE- 2021 r. (źródło: Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.), s. 23)

Osoby najmłodsze (16-24 lata) mieszkające w Polsce – w porównaniu do państw UE i tak wypadają z nich najsłabiej. Z biegiem lat – ta różnica się pogłębia, to znaczy, że im Polacy są starsi, tym posiadają mniej podstawowych umiejętności cyfrowych. 90 % polskich seniorów (65-74) nie posiadało co najmniej podstawowych umiejętności cyfrowych, przy czym średnia w 27 krajach UE – to 75 %.

Przy diagnozie kompetencji cyfrowych warto również podkreślić, iż jednym z zasadniczych warunków ich rozwoju jest stały dostęp do łączności internetowej i sprzętu, dzięki czemu możliwe jest podłączenie się do Internetu. Dane Eurostatu

wskazują, w 2021 roku około 92% gospodarstw domowych w Polsce wyposażonych było w dostęp do Internetu, co ulokowało Polskę na 12. miejscu spośród 26 krajów UE. Ranking otwierają Holandia i Luksemburg, w których to aż 99% gospodarstw domowych ma dostęp do sieci. Kluczowym dla integracji cyfrowej jest stwierdzenie, że 92% gospodarstw domowych (wiejskich) dysponowało Internetem. Gospodarstwa domowe, w których dochód na członka rodziny był najniższy - najrzadziej były wyposażone w dostęp do sieci (79%) oraz te - zlokalizowane w województwie świętokrzyskim (86%)[275].

92 % polskich gospodarstw bazuje na połączeniu szerokopasmowym z Internetem, 72 % - mobilnym, zaś łącze stacjonarne występuje w 69 % przypadków – to o 8 p.p. mniej na tle innych państw UE. Należy jednak zaznaczyć znaczący postęp w zakresie dostępu do infrastruktury, ponieważ jeszcze w 2010 roku dostęp do sieci był czymś nieosiągalnym w co trzecim gospodarstwie domowym. Dane na rok 2021 wskazują, iż 99 % gospodarstw w PL wyposażonych było w telefon komórkowy, prawie 90 % w urządzenie z dostępem do sieci, zaś 75 % - komputer osobisty. Wyzwania związane z dostępem do sprzętu i sieci spotęgowała pandemia Covid-19, co wymusiło w wielu przypadkach przejście na zdalną pracę i jednocześnie przymus współdzielenia sprzętu z rodziną. Co czwarty polski uczeń musiał dzielić sprzęt z rodzicami bądź rodzeństwem[276]. Rozwój technologii sprawił, iż aby być podłączonym z Internetem nie trzeba już posiadać komputera stacjonarnego. Jest to na tyle budujące rozwiązanie, iż obecnie nawet budżetowe smartfony są już w stanie uzyskiwać łączność cyfrową, a to natomiast przekłada się rosnąco na ilość użytkowników sieci. Pytanie tylko w jaki sposób społeczeństwo wykorzysta tę możliwość?

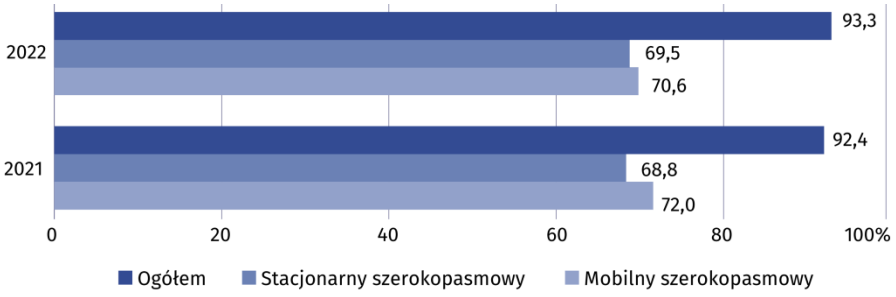
W 2022 r. dostęp do Internetu zapewniony był w 93,3% gospodarstw domowych i stanowiło to o 0,9 p. proc. więcej niż w roku 2021. W skali roku udział gospodarstw domowych mających dostęp do Internetu przez łącze stacjonarne - szerokopasmowe zwiększył się o 0,7 p. proc.

Dostęp przez mobilne szerokopasmowe łącze wykazało o 1,4 p. proc. gospodarstw mniej w porównaniu do roku poprzedniego. Dostęp do Internetu oraz rodzaj posiadanych łączy internetowych był zróżnicowany ze względu na klasę miejsca zamiesz-

[275] Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.), s. 23.

[276] Centrum Cyfrowe. Lekcja: Enter. 2020. Online, https://www.isp.org.pl/uploads/drive/aktualnosci/RAPORT_Dyrektorzy_do_zadan_specjalnych_08.06.pdf [dostęp 21.12.2023 r.].

kania, typ gospodarstwa i stopień urbanizacji. Częściej dostęp do Internetu posiadały gospodarstwa w skład których wchodzili rodzicie z dziećmi niż bez nich. Biorąc pod uwagę klasę miejsca zamieszkania, odsetek gospodarstw z dostępem do sieci był większy w dużych miastach aniżeli w mniejszych i na obszarach wiejskich, uwzględniając zaś stopień urbanizacji – najwyższy zarejestrowano na terenach wysoko zurbanizowanych[277]. Porównanie ilustruje poniższy wykres.



Wykres 5.4. Dostęp do Internetu w gospodarstwach domowych w latach 2021-2022 [w % ogółu gospodarstw] (źródło: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html [dostęp 18.02.2024 r.])

U dzieci w wieku przedszkolnym kształtowanych jest wiele podstawowych nawyków i umiejętności funkcjonowania w społeczeństwie, a także, a może przede wszystkim – rozwój kompetencji cyfrowych. Następuje on bowiem dość wcześnie, głównie w środowisku domowym w wyniku naśladowania rodziców, starszego rodzeństwa i obserwacji. Najmłodsi niezwykle szybko i biegle uczą się nowych umiejętności i przyswajają wiedzę, nawet jeśli urządzenia nie są dostosowane do ich potrzeb[278]. Stąd, istotne jest aby dzieci czerpały właściwe wzorce i przykłady z otaczającego je środowiska, w znacznej mierze, jak wspomniano – z domu. Jeśli zachowania najbliższych budzić będą wątpliwości w zakresie kompetencji cyfrowych, dzieci również takie zachowania przyjmą, co może mieć odzwierciedlenia w przyszłych ich postępowaniach.

Badania Urzędu Komunikacji Elektronicznej z 2020 roku wskazują, że blisko 1/3 polskich dzieci korzystanie z Internetu rozpoczyna przed 6. rokiem życia. Niestety, ich świadomość zagrożeń w obszarze korzystania z nowych technologii jest niewielka. To bowiem od rodziców zależą różne strategie udostępniania technologii swoim pociechom, od otwartych, przez wspierające czy restrykcyjne. Rodzice wybierają strategie biorąc pod uwagę różne czynniki np. czas, pieniądze, pracę, własną wiedzę i umiejętno-

[277] https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html [dostęp 18.02.2024 r.].
[278] S. Chaudron, R. Di Gioia, M. Gemo, 2018, *Young Children (0-8) and Digital Technology. A qualitative study across Europe*, Luxembourg.

ści. Rodzic nieposiadający wysokich kompetencji cyfrowych najczęściej w sposób znikomy wspiera rozwój cyfrowy swojego dziecka, postrzegając elektronikę jako źródło uzależniające, choć jednocześnie obserwując jej przydatność jako formę wsparcia w opiece nad dzieckiem[279]. Stąd, obserwowane jest częstokroć przekazywanie urządzeń dziecku w celu zajęcia jego uwagi i jednocześnie znalezienia czasu dla samego siebie.

Działania na rzecz rozwoju cyfrowego wśród najmłodszych kierować należy do rodziców (prawnych opiekunów) i starszego rodzeństwa, mogącego przekazywać najważniejsze wzorce i podstawy ku lepszej przyszłości. Ponieważ to kompetentni wychowawcy potrafią świadomie wspierać rozwój dziecka przy udziale instytucji edukacji i państwowych. Polscy rodzice (osoby w wieku 25-44 lat) niestety rzadziej dysponują umiejętnościami cyfrowymi w porównaniu do ich odpowiedników w UE – różnica w 2019 roku sięgnęła 10 p.p. Umiejętności podstawowych nie posiadała co trzecia osoba w tym zakresie wiekowym[280].

Kolejna, istotna dla dalszych rozważań grupa to nauczyciele. Przed okresem pandemii kompetencje cyfrowe nauczycieli były jedynie w niewielkim stopniu przedmiotem badań. Badanie *EU Kids Online* z roku 2018 ujawniło, iż nauczyciele nie przekazują odpowiedniego wsparcia uczniom w trakcie uzyskiwania kompetencji cyfrowych. Np. blisko połowa badanych stwierdziła brak wyjaśnienia przez nauczyciela, dlaczego akurat niektóre treści w sieci są dobre, a inne złe, czy też około 65 % uczniów nie otrzymało w przeszłości pomocy mentora, kiedy coś ucznia w sieci zaniepokoiło. Niemalże 45 % ankietowanych stwierdziło, że edukator nigdy bądź prawie nigdy nie zachęcał do uczenia się i korzystania z Internetu[281].

Swego rodzaju sprawdzianem umiejętności cyfrowych stała się potrzeba przejścia do nauczania zdalnego. Badanie przeprowadzone wiosną 2020 roku (na próbie blisko trzech tys. nauczycieli) pokazało, że tylko 5% z nich czuło się właściwie przygotowanych do przeprowadzania zajęć w formule online; podobnie uznali uczniowie, zdaniem których jedynie 8% wskazało zdolności nauczycieli jako wysokie, zaś co piąty uznał je po prostu za złe. Nieco później, ponieważ w grudniu tego samego roku kolejne ankiety wykazały, że jedynie 15% nauczycieli zadeklarowało brak umiejętności cyfrowych jako przeszkodę w prowadzeniu zajęć online, a rok później ta wartość zmniejszyła

[279] https://uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html [dostęp 23.12.2023 r.].
[280] Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.), s. 29.
[281] K. Abramczuk *et al.*, 2019, *Polskie badanie EU Kids Online 2018*, Wydawnictwo naukowe UAM, Poznań, s. 48.

się do 12%[282]. Dwa ostatnie wyniki są zaskakujące, ponieważ zdaniem autora mogą wynikać z braku wystarczającej świadomości dotyczącej kompetencji cyfrowych (bądź po prostu zrozumienia terminu kompetencji cyfrowych i ich składowych).

Wspomniany już wcześniej raport NASK *Nastolatki 3.0* obrazuje ogromne wyzwanie, jakie ujrzało światło dzienne przez pandemię: co trzeci badany uczeń negatywnie ocenił umiejętności nauczycieli w obszarze rozwiązywania problemów technicznych (a do takich zaliczono np. radzenie sobie z problemem połączenia w trakcie lekcji) i przygotowania do obsługi urządzeń elektronicznych (31%). Prawie 1/3 uczniów stwierdziła, że brakowało im wsparcia od nauczycieli w zakresie właśnie technicznym (np. podczas instalacji zdalnego oprogramowania)[283]. Wyzwaniem, które jeszcze mocniej uwidoczniła pandemia jest potrzeba ciągłego budowania kompetencji cyfrowych. Ten niezwykle wymagający czas wskazał, że istotna w zdalnym nauczaniu jest nie tylko komunikacja z uczniem, ale także - bądź przede wszystkim zdolność do utrzymywania cyfrowej higieny, łączenia pracy z życiem domowym i zachowania niezbędnej równowagi w tym obszarze.

Należy podkreślić, że edukacja cyfrowa i stopień integracji technologii w programach nauczania mogą się znacznie różnić w różnych miejscach. Niektóre kraje wprowadziły konkretne programy edukacji cyfrowej, podczas gdy inne nadal dążą do dostosowania swojego systemu edukacyjnego do nowoczesnych wymagań.

Warto zaznaczyć, że ze względu na szybkość zmian w technologii i edukacji cyfrowej, ocena kompetencji cyfrowych jest procesem dynamicznym i wymaga regularnych aktualizacji. Ocena ta służy również identyfikacji obszarów wymagających dalszego rozwoju, a także dostosowaniu programów nauczania do bieżących potrzeb uczniów.

5.4. Wnioski

Poziom kompetencji cyfrowych może różnić się w zależności od wielu czynników takich, jak: lokalizacja geograficzna, dostęp do zasobów cyfrowych, jakość szkolenia nauczycieli i polityki oświatowej.

---

[282] https://cik.uke.gov.pl/aktualnosci-cik/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2021,21.html [dostęp 17.12.2023 r.]. Zob.: https://uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html [dostęp 17.12.2023 r.].

[283] https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html [dostęp 13.12.2023 r.].

Stosunkowo niski poziom kompetencji cyfrowych polskiego społeczeństwa może negatywnie odbić się na skali oraz tempie cyfrowej transformacji, a także wzroście gospodarczym, jak również niższym komforcie życia obywateli. W związku z tym koniecznym jest zapewnienie każdemu mieszkańcowi Polski właściwych warunków do stałego rozwoju kompetencji cyfrowych. Spójna i jednolita polityka rozwoju kompetencji cyfrowych, mająca niebagatelny wpływ na świadomych (i aktywnych cyfrowo) obywateli, jest podstawą do rozwoju nowoczesnego państwa, gospodarki i przemysłu przyszłości. Szczególnie ważna jest w tym aspekcie zgoda polityczna i chęć do kontynuowania działań podejmowanych przez poprzedników (oczywiście uwzględniając analizę dotychczasowych przedsięwzięć).

Badania Europejskiego Urzędu Statystycznego wskazują jednoznacznie: to miejsce zamieszkania w ogromnym stopniu determinuje kompetencje cyfrowe obywateli. Największy odsetek osób z umiejętnościami cyfrowymi (ogólnymi) klasyfikowanymi powyżej określonego poziomu podstawowego mają miasta (29% mieszkańców), podczas gdy najmniejszy — obszary wiejskie (14%), przedmieścia i miasteczka plasują się pomiędzy z wynikiem 19%[284].

Jednakże istnieją badania i raporty dotyczące poziomu kompetencji cyfrowych wśród uczniów i nauczycieli. Na przykład, jak już wspomniano, w Europie funkcjonuje program badawczy: *Digital Competence Framework for Citizens (DigComp)* opracowany przez Komisję Europejską, który ma na celu mierzenie i rozwijanie kompetencji cyfrowych wśród obywateli.

International Society for Technology in Education (ISTE): ISTE opracowało standardy kompetencji cyfrowych dla nauczycieli i uczniów, obejmujące umiejętności związane z korzystaniem z technologii w nauczaniu i nauce.

Common Sense Education - Digital Citizenship Curriculum: Common Sense Education oferuje program edukacji cyfrowej, który obejmuje pięć obszarów kompetencji cyfrowych: bezpieczeństwo online, etyka online, umiejętność korzystania z technologii, umiejętność komunikacji online i umiejętność rozwiązania problemu online.

W Polsce Ministerstwo Edukacji i Nauki (MEiN) prowadzi badania i inicjatywy mające na celu ocenę poziomu kompetencji cyfrowych uczniów i nauczycieli. MEiN

[284] https://aktualnosci.komputronik.com/253528-przepasc-w-zakresie-umiejetnosci-cyfrowych-miasta-deklasuja-obszary-wiejskie [dostęp 17.12.2023 r.].

wspiera również programy szkoleniowe dla nauczycieli w zakresie kompetencji cyfrowych oraz wprowadza zmiany programowe w celu wzmocnienia edukacji cyfrowej.

Ważne jest, aby systematycznie monitorować i oceniać poziom kompetencji cyfrowych uczniów i nauczycieli, aby identyfikować obszary wymagające poprawy i dostosowywać programy nauczania oraz szkolenia nauczycieli w celu lepszego przygotowania do wyzwań cyfrowego świata.

6. Wyniki badań własnych

6.1. Wywiady eksperckie

W ramach wywiadów eksperckich przeprowadzonych zostało kilka spotkań z wybranymi osobami. Są specjalistami w analizowanej tematyce i z bogatym doświadczeniem. Wywiady zrealizowano zarówno w formie stacjonarnej, jak i zdalnej z użyciem platform *Zoom* oraz *MS Teams*.

Indywidualny wywiad pogłębiony *(IDI)* w Polskim Towarzystwie Informatycznym, jako najstarszej polskiej organizacji zrzeszającej profesjonalistów branży informatycznej. Celem badania było poznanie opinii Pracownika PTI dotyczących:

1) Oceny kierunków i kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa;
2) Oceny sposobów edukacji użytkowników sieci;
3) Oceny efektywności kluczowych kompetencji cyfrowych mogących wpływać na cały System cyberbezpieczeństwa RP;
4) Opinii na temat realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji – zadań realizowanych przez Towarzystwo.

Ekspert- Pani Wiceprezes Oddziału Małopolskiego PTI: Beata Chodacka. Nauczyciel informatyki w V LO i SP 33 w Krakowie. Animatorka działań na rzecz edukacji informatycznej, takich jak konkursy (m.in. TIK?-TAK!), Małopolski Dzień Uczenia się, "Małopolska koduje". Ambasadorka kodowania. Pasjonat e-learningu, autorka kursów e-learningowych dla dzieci i młodzieży, współtwórca zbioru zadań z informatyki exeBOOK. Współtwórca i współorganizator projektu „Klasa z ECDL".

Tab. 6.1

Wywiad ekspercki nr 1. Opinia Pracownika PTI

Pytanie badawcze	Odpowiedzi eksperta
1) Jakie kluczowe zadania i cele realizuje Towarzystwo?	Zadania ukierunkowane są na rozwój informatyki, PTI zrzesza specjalistów tej dziedziny. Obecnie trwa dyskusja na temat kogo nazwać możemy informatykiem, czy będzie to osoba po studiach informatycznych, czy jest to także specjalista z zakresu cyberbezpieczeństwa? Podczas organizowania konferencji czy spotkań, oprócz pracowników PTI, zapraszane są również inne osoby ze świata IT. PTI zajmuje się publikowaniem, wydawaniem kwartalnika Domena, tworzeniem artykułów. Ponadto, występuje certyfikacja na poziomie średniozaawansowanym ECDL, certyfikacja bezpieczeństwa, krajowego systemu certyfikacji cyberbezpieczeństwa. Są to osoby doświadczone. PTI realizuje wsparcie projektów, audyty, ekspertyzy w ramach izby rzeczoznawców. Wsparcie edukacji informatycznej uczniów i nauczycieli. Organizacja zajęć. PTI działa w sekcjach, m.in. sekcja informatyki szkolnej, zrzesza około setki nauczycieli z całej Polski. Sekcja cyberbezpieczeństwa - zajmuje się cyfrowym bezpieczeństwem, jego techniczną stroną.

2) Co według Pani oznacza zagrożenie w dziedzinie cyberbezpieczeństwa? Na które z zagrożeń mogą być najbardziej narażeni najmłodsi użytkownicy sieci (Internetu)?	Zagrożeń jest wiele. Niezamknięte konta, informacje mające charakter publiczny, widoczny dla kogokolwiek. Kwestią wymagającą jest również pozostawianie niewylogowanych komputerów. Pojawiają się rozterki w głowach uczniów. Czy mogę spojrzeć co kolega zostawił włączonego, czy mogę wejść na jego konto? Największym zagrożeniem jest człowiek, który czasami nieświadomie publikuje zbyt wiele informacji o sobie (konkursy, zainteresowania). Podczas badania, uczniowie byli zdziwieni, iż jest to widoczne dla osób z zewnątrz grona znajomych. Zauważalna jest poprawa w kwestii edukacji od zera, ponieważ coraz więcej młodych osób interesuje się tym, co zamieszcza w sieci. Ponadto, serwisy społecznościowe rozwinęły się pod kątem zabezpieczeń (np. opcja sprawdzenia co jest widoczne publicznie, podgląd). Żyjemy w dobie czatu GPT, sztucznej inteligencji, a tego procesu nie da się już zatrzymać. Pytanie jakie konsekwencje to za sobą pociągnie. Fake newsy, korzystanie z informacji które nas otaczają powodują trudność weryfikacji. Dorosła osoba ma inny próg weryfikacji wiedzy, w oparciu o własną wiedzę, doświadczenie. Nastolatek będąc na innym etapie dojrzałości emocjonalnej większość sytuacji będzie traktował, przyjmował jaki absolutny pewnik. Dużo łatwiej jest go na to nabrać. Naciąganie ludzi, wciąganie ich do sekt, samobójstwa, praca za granicą. Najmłodsi są narażeni na praktycznie wszystkie zagrożenia, z wyjątkiem finansowych.
3) Jakie programy / konferencje / działania realizuje Towarzystwo w ramach podnoszenia kompetencji cyfrowych użytkowników sieci (Internetu)? Kto może wziąć w nich udział?	Konferencja SaferInternet – Dzień Bezpiecznego Internetu. Konferencje, w których informacje przekazywane są ludzkim językiem. Każdy jest w stanie zrozumieć to co się mówi i jest w stanie tym się zainteresować. Tematy poruszane są szczególnie ważne dla aktualnych sytuacji w sieci. Np. seksting, młodzież (starsza) rozbiera się, zarabia… ukazuje się ich motywacje i skutki, konsekwencje tych działań. Udział w konferencji biorą znakomici goście. Uczestnicy mediów typu facebook, policjanci, wydział kryminalny, w jaki sposób rozmawiać z dziećmi, jak zapobiegać. Kolejny element to światowy dzień społeczeństwa informacyjnego, występuje podczas niego część poświęcona cyberbezpieczeństwu. Poruszane są tematy, które mogą dać w dalszym działaniu konsekwencje. PTI szkoli dorosłych, rodziców, wspomina o tym, co jest istotne w cyberprzestrzeni oraz co się zmienia. Od 17 lat jest organizowana konferencja Informatyka, jest wskazanie różnych poziomów nauczania informatyki. Konferencje stricto informatyczne, inżynieria kko, tworzenie programowania. Cyberbezpieczeństwo, sztuczna inteligencja. Organizowanie konkursów, podkreślenie roli bezpieczeństwa. Współpraca z NASK, PIIT (Polska Izba Informatyki). Miesięcznik IT Administracja. Dbanie o jakość kadr IT, Sektorowa Rada ds. Kompetencji Telekomunikacji Cyberbezpieczeństwa – konferencja międzynarodowa, wspierana „Uwaga Smartfon", konferencje lokalne również się odbywają. Certyfikacja umiejętności jest wyzwaniem. Certyfikat RODO, certyfikat bezpieczeństwa w sieci, certyfikat bezpieczeństwa komputerowego, certyfikaty *ECDL*. Np. w klasie VI uczniowie zdają certyfikat podstaw pracy w sieci, związany z zagadnieniami praw autorskich, netykiety, zagadnień cyberbezpieczeństwa. PTI tworzy artykuły, wydaje czasopisma dotyczące bezpieczeństwa w sieci. Opisywana działalność trafia do szerokiego grona odbiorców.
4) Czy istnieje potrzeba zmiany sposobu edukacji uczniów lub nauczycieli w zakresie informatyki? Jeśli tak – które obszary byłyby newralgiczne?	Zakazywanie używania telefonów, smartfonów w szkołach jest bezcelowe. Do niczego nie prowadzi. Młodzież i tak będzie tego używać. Nie chodzi o to, aby zakazać tego całkowicie. Sensem jest nauczenie prawidłowego i bezpiecznego użytkowania tego rodzaju urządzeń, z pełną świadomością zagrożeń i wykształcenie pewnych nawyków. Posługując się przykładem, rodzice nie pozwalają dzieciom samym wychodzić na rynek główny w Krakowie w późnych godzinach nocnych. Nikt nie „puszcza" samego dziecka, aby tam przebywał. Natomiast do Internetu

	rodzice wpuszczają sami. Kwestia kontroli rodzicielskiej, świadomości. Edukacja musi często iść w kierunku rodziców. Czasami dzieci wiedzą nawet więcej – mają hasła do różnych portali, z których korzystają rodzice, ale z pomocą dzieci. Tak więc w pewnych obszarach można stwierdzić, iż nawet dzieci wyprzedzają rodziców. Stąd potrzeba rozwijania wiedzy i umiejętności u rodziców. Czasami rodzice nie są w stanie pewnych rzeczy i czynności wykonać. To jest proces, nie da się tego zrobić raz i skończyć. Nie jest to wiedza, którą można zdobyć jednorazowo, ponieważ jest ona cały czas zmienna. Strona Niebezpiecznik, niby informacje i doświadczenia banalnie proste, aczkolwiek jakże istotne w zabezpieczaniu sieci. Profilaktyka. Temat haseł. Każdy uczeń ma świadomość, że hasło powinno zawierać znaki specjalne etc. Wchodzenie na niewylogowane konto. Uczenie kultury, „wszedłeś po koledze, to go wyloguj". Informacje w różnych serialach, nawet one uczą. Ludzie niegdyś mieli zapisane hasła na kartach kredytowych (z tyłu), obecnie coraz więcej osób ma świadomość błędnego zachowania. Istnieje potrzeba edukacji rodziców. Ilość świadectw z paskiem, umieszczanych w sieci. Na koniec roku szkolnego rodzice bądź dzieci samodzielnie wrzucają do Internetu zdjęcia świadectw nie zasłaniając częstokroć wrażliwych danych, od peselu począwszy. Przewidywane są zmiany w podstawie programowej. Podstawa jest elastyczna i dość ogólnie sformułowana. Daje dowolność nauczycielom. Nie tylko na lekcjach informatyki powinno się kształtować kompetencje cyfrowe i świadomość w sieci. Lekcje WOS-u, historii współczesnej, lekcje wychowawcze. Wspominanie o zabezpieczaniu się jest ważne. To co nas spotyka w zakresie cyberprzemocy i cyberataku, co najmniej ¾ wynika z winy użytkownika. Znacznie mniejszy % nie zależy od nas. Kroki edukacji: ➢ Co złego może spotkać użytkownika? ➢ Co grozi jeśli takie zachowanie będzie stałe, częste? ➢ Jak zareagować kiedy zdarzenie wystąpi? ➢ Ucząc się pierwszej pomocy, człowiek powinien tę wiedzę odnawiać stale. To powoduje, że należy uczyć reagować. Utraciłeś dane, co powinieneś zrobić, jak je zabezpieczyć? Np. kradzież komputera. Natychmiast zmiana haseł, wylogowanie ze wszystkich miejsc. Świadomość gdzie można zadzwonić, do kogo zgłosić. Gdzie zgłosić szantaż. *CSIRTy* działają skutecznie. Szybka, sprawna reakcja w ramach reagowania na incydent. Przesłuchanie dziecka z policją robi na innych wrażenie. Nigdy użytkownik nie jest bezpieczny. Cyfrowy świat, zostawianie informacji na mapach. Śledzenie, gdzie jedliśmy, gdzie byliśmy, ile pieniędzy wydajemy, kiedy jesteśmy nieobecni. Jest to również zagrożenie, któremu należy próbować sprostać. Mówić o tym, opowiadać i przytaczać przykłady, analizować informacje.
5) Jak istotne jest edukowanie użytkowników sieci i najmłodszych uczniów do właściwych zachowań w cyberprzestrzeni? Jakie działania są Pani zdaniem najważniejsze w edukacji najmłodszego pokolenia?	Cyberbezpieczeństwo ma sens jeśli ten czynnik ludzki jest świadomy. Czasami niewiedza czy niefrasobliwość może mieć tragiczne skutki. Im lepsza będzie edukacja od podstaw, im bardziej nauczymy dbania o cyfrowy świat, o hasła, o zabezpieczanie swoich danych, o sprzęt, tym lepiej ludzie będą działali w przyszłości. Zmienia się otaczająca nas rzeczywistość i tym samym środowisko cyberprzestrzeni. Zagrożenia niebezpieczeństwa są inne niż dekadę temu. Z jednej strony banki są bezpieczniejsze, z drugiej jednej istnieje coraz więcej danych wrażliwych w sieci, coraz łatwiej jest kogoś skompromitować. Obecnie chyba łatwiej jest zmienić nazwisko i tożsamość, aniżeli wykasować wszystko z sieci. Zawsze zostaje pewien ślad. Uświadamianie społeczeństwu, że raz wrzucona informacja do sieci, pozostaje tam na zawsze. Szczególnie ważne są takie elementy i czynniki jak:

	➢ wiedza jakie są zagrożenia; ➢ jakie są konsekwencje za swoje działania, uczeń nie jest bezkarny; ➢ lekcje o cyfrowym świecie, nikt nie jest anonimowy. Przeglądarka w trybie incognito jest dla rodziców można rzec, ale nie jest w stanie ukryć przed systemem gdzie się było, jakie strony zostały odwiedzone; ➢ nękanie i hejt – największy problem jakie młodzież spotyka. Hejt stanowi przestępstwo; ➢ seksting, również karalne; ➢ strach przed ukaraniem może prowadzić do zatrzymania agresji. Największa plaga, klasa 5,6,7, w starszych klasach nie ma nasilenia hejtu; ➢ dalej wynika: szukanie pocieszenia, akceptacji, poszukiwania grupy rówieśniczej. Jeśli nie grupa rówieśnicza, to może być zewnętrzna, gdzie inne osoby mogą namawiać do różnego rodzaju zaburzeń, są strony instruujące, jak się odchudzać do stanów szpitalnych, jak się ciąć; ➢ edukacja powinna być kierowana zarówno do uczniów, rodziców jak i nauczycieli, żeby każdy wiedział jak się należy zachować, jak reagować. ➢ skutki nękania i hejtu mogą doprowadzić do wykluczenia z grupy, wyrzucenia z grupy klasowej, jest to największa cyberprzemoc; ➢ uczniowie mają świadomość, że nie powinni chodzić na spotkania z obcą osobą, poznaną w sieci; większe miasto, pytanie jak jest w mniejszych miejscowo. Różnego rodzaju negatywne sytuacje w sieci mogą mieć poważne implikacje, nawet w zakresie uszczerbku na zdrowiu czy życiu. Publikowanie treści nienawiści w stosunku do jednego ucznia, tworzenie tzw. hejtu w grupie. Publikowanie fałszywych informacji na temat danej osoby w mediach, podszywanie się, tworzenie nowej tożsamości. Są to naprawdę ciężkie sytuacje. Miał być to w założeniu dowcip, kawał. Osoba pokrzywdzona, a sprawcy – stali się także ofiarami konsekwencji swoich działań. Dokuczanie zawsze miało miejsce, natomiast to się działo tu i teraz. Dziecko po powrocie do domu odcinało się od rzeczywistości. Natomiast obecnie, dziecko może mieć stale kontakt z hejtem, jest obecne w sieci, koledzy – hejterzy nadal są. Różnego rodzaju informacje, smsy, wiadomości, dziecko może otrzymywać. Skutki bywają rzeczywiście silne, głębokie depresje, anoreksje, próby samobójcze. Algorytm pewnego zdarzenia: dochodzi do sytuacji, rodzic jest wezwany do szkoły, wysłuchuje zebranych informacji. Następnego dnia z prawnikami, nabuzowany, przedstawia katalog win, które popełniła szkoła. Dalej, szkoła musi się chronić i pisać elaboraty, iż pewne działania były podejmowane. Gdzie jest w tym wszystkim dziecko? Jest samo. Odosobnione. Wszyscy próbują powiedzieć „nie ja jestem winien". Czasami, po tym przebudzeniu okazuje się, że dziecko właśnie znalazło innych przyjaciół tj. sekta, narkotyki, alkohol… Tam dziecko znajduje akceptację, wsparcie, tam jest lubiany i jest znajdowany dla niego czas. Propozycje rozmowy z dzieckiem, terapii (pokrzywdzonemu bądź krzywdzącemu) spotyka się najczęściej z odrzuceniem ze strony rodziców i stwierdzeniem, iż nie jest to potrzebne. W szkołach są psycholodzy, natomiast często rodzice nie chcą skorzystać z tej możliwości. Proces bardzo długo trwający i pytanie kiedy się zaczął. Nie jest łatwo określić kiedy problem się pojawił. Cyberprzemoc w sieci ma charakterystyczne to, iż nie da się od niej odciąć.
6) Czy kompetencje cyfrowe pojedynczego użytkownika sieci mogą wpływać na System cyberbezpieczeństwa	Tak, mają znaczenie w całym systemie. Przykład. Uczniowie wykonywali zadanie związane z tematem *fake newsów*. Najwięcej takich informacji jest w mediach społecznościowych, ponieważ łańcuszkowo są powtarzane i plotkarsko czasami dodawane od siebie są pewne dane.

RP? Które z tych kompetencji są najważniejsze?	Największa wiarygodność według uczniów jest właśnie na portalach. Mimo świadomości, że tam ktoś może kłamać. Istotne jest krytyczne myślenie, podejście zdroworozsądkowe. Jeśli nauczyciel będzie wiedział na co zwrócić uwagę, rodzic tak samo, a uczeń, dziecko zostanie wyposażone we właściwe umiejętności i wiedzę – jest szansa, że społeczeństwo zostanie wyedukowane. To musi być proces, nie jednorazowe działanie „od święta".
7) Jak Pan / Pani ocenia poziom kompetencji cyfrowych polskich uczniów i nauczycieli w porównaniu do innych państw (bądź ogółem poziom społeczeństwa)?	PTI takich badań nie prowadzi, aczkolwiek podczas *Safe Internet* – pojawiają się osoby z innych państw, Włoch, USA, są ukazywane takie porównania. Profesor Pyżalski jest specjalistą od kondycji psychicznej uczniów, cyberkondycji. Prowadzi różnego rodzaju szeroko zakrojone badania. Nasza młodzież nie różni się niczym innym od zagranicznej młodzieży. Każdy ma ten sam dostęp do sieci. W Anglii testowany jest eksperyment, gdzie w szkołach nie używa się komputerów. Całkowicie zamierza się odcięcie od smartfonów, komputerów. Minister edukacji we Włoszech kilka lat temu wprowadziła *smartfon* na zajęcia jako narzędzie dydaktyczne, uczeń powinien mieć takie urządzenie dostępne stale. Najbardziej znane aplikacje do tworzenia quizów, sprawdzianów online są pochodzenia włoskiego. We Włoszech taki rodzaj aktywności podczas nauczania sprawdza się znakomicie. W Polsce różne ograniczenia są dopiero wprowadzane, natomiast zabranianie ich jest bezcelowe. Ukazanie, do czego może być przydatny smartfon jest niezwykle ważne. Wówczas będzie to skuteczne. Uczeń zacznie wykorzystywać takie urządzenie zgodnie z przeznaczeniem oraz ze świadomością co mu może zagrażać. Jak wspomniano wcześniej, w porównaniu do innych nacji, nie ma różnicy. Młodzież polska kontaktuje się z młodzieżą z zagranicy, kontakt jest prowadzony stale, ciągle. Świat realny i cyfrowy jest wymieszany, wszystko w zasadzie może odbywać się w Internecie. Kontakty między znajomymi na całym świecie nie jest problemem. To jest plus bez wątpienia.

Źródło: opracowanie własne wyników badań

Indywidualny wywiad pogłębiony *(IDI)* w NASK - PIB, czyli Naukowej i Akademickiej Sieci Komputerowej, Państwowym Instytucie Badawczym nadzorowanym przez Kancelarię Prezesa Rady Ministrów. Celem badania było poznanie opinii pracownika instytucji w zakresie:

1) Realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji – zadań realizowanych przez NASK – PIB;
2) Sposobów edukacji użytkowników sieci;
3) Struktury Systemu cyberbezpieczeństwa RP;
4) Kierunków i kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa.

Tab. 6.2

Wywiad ekspercki nr 2. Opinia Pracownika NASK - PIB

Pytanie badawcze	**Odpowiedzi eksperta**
1) Jakie kluczowe zadania i cele realizuje NASK - PIB?	NASK pełni bardzo ważną funkcję w systemie cyberbezpieczeństwa państwa. W ustawie o KSC jest określony jako CSIRT NASK, obok CSIRT MON – sprawy wojskowe, CSIRT GOV – obejmuje nadzór przez ABW, najważniejsze organy państwa, rządu i in-nych podmiotów na poziomie krajowym. NASK zajmuje się pozostałymi podmiotami,

	w taki sposób żeby zapewnić cyberbezpieczeństwo na najwyższym poziomie.
2) Czy P. instytucja realizuje zadania w obszarze budowania świadomości i cyfrowych kompetencji?	Poza reagowaniem na incydenty, NASK zajmuje się także budowaniem świadomości i kompetencji cyfrowych, co jest jednym z kluczowych zadań. W NASK istnieją zespoły zajmujące się szkoleniem, ale nie tylko, celem tych grup jest także budowanie kompetencji cyfrowych, które nie zawsze są szkoleniami. Wiele osób w NASK zajmuje się tym obszarem. Działania dotyczą zarówno dzieci (szkolenia, podnoszenie kompetencji cyfrowych), jak i osób dorosłych, profesjonalistów zajmujących się ważnymi funkcjami w państwie (jak np. politycy, są organizowane specjalnie adresowane szkolenia do tychże osób). Szkolenie ma szeroki zakres, osoby związane z medycyną również są edukowane przez specjalistów z NASK. Powstało konsorcjum cyber science, na które składa się NASK, Uniwersystet Śląski, Politechnika Śląska i Uniwersystet Ekonomiczny w Katowicach. Dzięki współpracy zostało przeszkolonych 100 % studentów pierwszego roku studiów. Szkolenie obejmowało przede wszystkim cyber higienę i zostało zakończone egzaminem. Na tej samej zasadzie, kiedy to studenci przechodzą szkolenie BHP. Prognoza jest taka, iż w następnym roku ilość uczelni zaangażowanych wzrośnie nawet do ośmiu. Budowanie świadomości jest w NASK od samego początku, podmiot ten prowadzi działania Safer Internet, Dni Bezpiecznego Internetu. Stanowi to dużo więcej niż kampania, jest to cała sieć, a program działa od 2005 roku. Systemowe działanie, współpraca m.in. z *NGO*, z roku na rok działania te są odnawiane. Szkolenia kierowane do nauczycieli, szkół, dzieci, młodzieży. To europejski program, którego NASK jest liderem w Polsce, razem z fundacją Dajemy Dzieciom Siłę.
3) Co według P. oznacza zagrożenie w dziedzinie cyberbezpieczeństwa? Na które z zagrożeń mogą być najbardziej narażeni najmłodsi użytkownicy sieci (Internetu)?	Zajmuję się zagrożeniami w Dyżurnecie, w którym to te zagrożenia są najbardziej poważne. Dyżurnet zajmuje się usuwaniem tzw. *CSAMu, Child Sexual Abusement Materials*. Są to treści pedofilskie, pornograficzne z udziałem dzieci. Często zajmują się tym grupy przestępcze, celem czerpania korzyści nie tyle seksualnych, co po prostu finansowych (majątkowych). Pedofilów jest zdecydowanie mniej, którzy zajmują się propagowaniem tych treści, wyłudzaniem, rozpowszechnianiem. Największe zagrożenie stanowi szantaż dzieciaków, wyłudzanie od nich zdjęć, którymi można ich później szantażować (zdjęcia natury erotycznej). Tego zjawiska wcześniej nie było, dopóki nie było kamer w telefonach, nie stanowiło to tak ogromnego wyzwania. Znaczący procent treści *CSAM* stanowią materiały wykonane samodzielnie przez właśnie dzieci. To dzieci same, osobiście nagrywają, kręcą, robią zdjęcia ze swoim udziałem. Tych materiałów jest lawinowy skok. Jest to naprawdę znaczący problem. Dla dzieciaków – zagrożenie to nie jest umiejscowione na samym szczycie. Trudniejszy dla nich jest hejt i uzależnienie od Internetu. Są osoby, które cały swój świat skupiają na działaniu w sieci, cały swój wolny czas przeznaczają na scrollowanie Internetu. Spędzając kilka godzin przed komputerem, dziecko uzależnia się od użytkowania sieci. Podsumowując: ➢ skala, która powoduje uzależnienie, ilość czasu spędzanego w sieci; ➢ hejt stale obecny, nawet mimo zmiany miejsca przebywania; język jest bardzo ostry i potrafi ranić, przeniósł się do języka powszechnego, który stosuje się podczas np. przerw czy robiąc zakupy w sklepie; ➢ treści *CSAM*, niegodziwe traktowanie dzieci w Internecie, treści bardzo szkodliwe.
4) Czy w obszarze P. instytucji funkcjonuje pojęcie kompetencji cyfrowych? I jak jest ono definiowane?	Jak najbardziej funkcjonuje i jest niezwykle ważne. Kompetencje cyfrowe to nie tylko sprawne korzystanie z technologii cyfrowych, ale przede wszystkim bezpieczne korzystanie. Podkreślam szczególnie ten element bezpieczeństwa.

5) Które z zagrożeń w obszarze cyberbezpieczeństwa mogą oznaczać największe wyzwanie dla funkcjonowania państwa i jakie inne mogą powstać w przyszłości?	Cyberwojna czy cyberterroryzm tak naprawdę są obecne aktualnie, to dzieje się na naszych oczach. Skala zapewne mogłaby być większa, pytanie na jakim jesteśmy etapie, jaki jest zakres tych działań. Największe wyzwanie stanowić mogą ataki na elementy infrastruktury krytycznej. Atak ransomware np. na klinikę, która została odcięta od Internetu, spowodował wstrzymanie jakichkolwiek prac. Niemożliwe było uzyskanie dostępu do bazy danych, pracownicy mieli problemy z ustaleniem np. historii pacjenta czy leków jakie powinny być podane, w jaki sposób trzeba go leczyć. Skala mogłaby być większa. Zbieranie informacji jak działa społeczeństwo, co jest istotne w danym państwie, swobodne dzielenie się danymi na swój temat, stanowi również poważne wyzwanie. Big data – coraz łatwiej zarządza się dużymi zasobami danych, zaś niektóre państwa celowo zbierają informacje o obywatelach innych państw, jest to można rzec swego rodzaju przykład cyberszpiegostwa.
6) Czy istnieje potrzeba zmiany sposobu edukacji użytkowników sieci? Jeśli tak – w które obszary byłyby newralgiczne?	Ta potrzeba jest, zdecydowanie. Kampanie są cały czas dostosowywane, NASK nie kopiuje swoich kampanii czyniąc tak, żeby jedna kampania trwała przez kilka lat. Co roku jest przygotowywany nowy program, w nawiązaniu oczywiście do poprzedniego i uwzględniający wnioski z poprzednich programów. Work in Progress, nie ma takiej sytuacji, że program jest stale taki sam. W NASK co roku prowadzone są badania, jest refleksja, jest badanie satysfakcji. Z jednej strony się szkoli, z drugiej – się bada. Badania nastolatków. Szkolenie i badania są połączone razem. Nie ma szkolenia „na ślepo". Nigdy za mało, nigdy dość, zgodnie z maksymą trzeba stale trenować żeby widzieć efekty. Takie potrzeby są, zdecydowanie, potrzeba coraz więcej. Łatwo mówić, że trzeba szkolić. Trzeba pamiętać przede wszystkim o tych szkolących. Warto zastanowić się nad rolą nauczycieli w szkoleniu młodych pokoleń. Z jednej strony uświadomić nauczycieli, dać możliwości rozwoju, dać im wiedzę. Nie jest to takie łatwe znaleźć specjalistów. Częstokroć nauczyciel posiadający taką wiedzę, jest dodatkowo obciążony np. wychowawstwem czy innymi zadaniami. Ta podstawowa wiedza, związana ze świadomością cyberzagrożeń nie musi być przekazywana uczniom przez nauczycieli informatyki. Równie dobrze mogą to wykonywać inni nauczyciele, nauczając jakie są zagrożenia, jak sobie z nimi radzić, na czym powinna polegać cyber higiena, na co zwracać uwagę, co więcej, które strony odwiedzać, jak reagować na incydenty. Zauważam potencjał w nauczycielach, którzy niekoniecznie są techniczni. Wiele osób może włączyć się w ten proces (uświadamiania) i czerpać z niego dużą satysfakcję (np. pedagodzy szkolni, wychowawcy).
7) Jak istotne jest edukowanie użytkowników sieci i najmłodszych uczniów do właściwych zachowań w cyberprzestrzeni?	Poradnik „Uczeń w cyfrowym świecie" stworzony przez NASK jest świetnym przykładem tego w jaki sposób uczniowie powinni poruszać się w sieci. Pod koniec września 2023 roku miała miejsca konferencja dot. bezpiecznego Internetu. Sala pękała w szwach, wiele osób przyjechało z Warszawy, ale także masa osób łączyła się online. Prace częstokroć są dwujęzyczne. Konferencje są prowadzone dodatkowo w języku ukraińskim. Od dwóch lat nastąpiła gigantyczna zmiana, dzieci z Ukrainy jest coraz więcej. Ponadto, nie znają one języka polskiego. W związku z tym NASK reaguje na bieżąco na potrzeby, które pojawiają się w naszym państwie. NASK wychodzi naprzeciw potrzebom edukacji.
8) Czy kompetencje cyfrowe pojedynczego użytkownika sieci mogą wpływać na System cyberbezpieczeństwa RP? Które z tych kompetencji są najważniejsze?	Można porównać to do głosowania. Z reguły jeden głos ma niewielkie znaczenie, ale jeden głos dodać do kolejnego, już zaczyna się tworzyć pewna całość. Jeśli powinno się poprawić, to właśnie przez najmłodszych. Nie wolno odpuścić jakiejkolwiek jednostki w budowaniu świadomości i kompetencji cyfrowych. Nie powinno się nikogo pomijać, nie jest istotne czy te osoby są z dużego miasta czy ze wsi. Potrzeby budowania świadomości są wszędzie te same. Od 2008 roku 99% danych generowanych jest elektronicznie. W związku z tym czy chcemy czy nie, jesteśmy na nie skazani.

	Musimy o nie dbać.
9) Jakie czynniki i działania mogą wpływać na budowanie świadomości oraz cyfrowych kompetencji w zakresie cyberbezpieczeństwa?	Działania programowe mają duże znaczenie, w skali całego kraju. Odpowiednie działania samorządu terytorialnego albo instytucji centralnej, np. prowadzone przez resort edukacji narodowej, tak żeby miały one większą skalę. Ogromna rola samorządu terytorialnego jako autonomicznego regionu. Jeśli chodzi o kwestie cyfrowe, informatyzację. Powielanie tego samego programu w samorządach, to szkoda czasu, energii i pieniędzy. Dlatego też np. mamy jednego Google, jednego Facebooka. Na rynku jest potrzeba konkurencji. Programy o zasięgu krajowym, a co najmniej regionalnym są przyszłością. Przecież potrzeby kompetencji cyfrowych na Śląsku są identyczne, jak te na Pomorzu w przeciwieństwie np. do kwestii ochrony zdrowia, różna jest natura, obecność przemysłu, obecność morza etc. W przypadku kompetencji cyfrowych ich potrzeba jest ta sama.
10) Czy obecną strukturę Systemu cyberbezpieczeństwa RP można określić jako adekwatną do aktualnych zadań i ewentualnych przyszłych wyzwań, jakie pojawić się mogą w obszarze cyberbezpieczeństwa? (Proszę przedstawić propozycje ewentualnych możliwych udoskonaleń).	Jest to część polityki. To i tak zostanie zmienione. Obecnie KSC jest stworzone na podstawie *Dyrektywy NIS 1*. Za rok czeka nas implementacja *Dyrektywy NIS 2*. System zostanie przebudowany dość znacząco. System krajowy jest niezmiernie istotny. Czy *CSIRTy* będą trzy czy będzie ich więcej to osobna kwestia. Już wiadomo, iż będzie ich więcej, *CSIRTy* sektorowe. Podział wielkiej trójki oczywiście zostanie. Jest szczególnie istotne, żeby dzięki regulacji, te *CSIRTy* sektorowe (w związku z nowym KSC) powstały nie tylko na papierze. Żeby za tą regulacją szły konkretne działania mające u podstaw właściwy budżet. Nie da się wybudować cyberbezpieczeństwa za darmo. Niezbędni są eksperci, odpowiedzialni za kwestie cyberbezpieczeństwa. Są podmioty, które wyłączono poza *CSIRT* czy KSC i dobrze, ale dobrze by było, żeby w tym systemie KSC znalazło się jak najwięcej podmiotów. Ale żeby te wyłączone z systemu, wiedziały jaki jest podział kompetencji, obowiązków, jakie są procedury. Nie same finanse są ważne, ale konkretnie wypisane i określone kompetencje podmiotów publicznych, tak jak i prywatnych, żeby miały jasno wskazane zobowiązania do reagowania, do działania – a nie tylko kiedy ktoś uzna, że jeśli trzeba, to jest reakcja. Zawsze można pracować nad systemem, doskonalić go. Im więcej wyspecjalizowanych *CSIRTów* sektorowych, tym lepiej. Np. obecnie KNF prowadzi *CSIRT* – nie jest to *CSIRT* krajowy, a sektorowy. Bardzo dobrze sobie radzi. Ma wysokie opinie ekspertów.

Źródło: opracowanie własne wyników badań

Indywidualny wywiad pogłębiony *(IDI)* w Ministerstwie Edukacji i Nauki[285], Departamencie Kształcenia Ogólnego i Podstaw Programowych. Ekspertem była Zastępca Dyrektora: Pani Małgorzata Szybalska.

Celem badania było poznanie opinii Pracownika dotyczących:

1) Przepisów regulujących kształcenie uczniów (szkół podstawowych);
2) Oceny sposobów edukacji i metod użytkowników sieci;
3) Sposobów kształcenia kompetencji cyfrowych;
4) Istoty edukacji najmłodszych użytkowników sieci.

[285] Jak już wspomniano powyżej, 1 stycznia 2024 r. nastąpił podział Ministerstwa Edukacji i Nauki na dwa odrębne resorty – Ministerstwo Edukacji Narodowej oraz Ministerstwo Nauki i Szkolnictwa Wyższego.

Tab. 6.3

Wywiad ekspercki nr 3. Opinia Pracownika MEiN

Pytanie badawcze	**Odpowiedzi eksperta**
1) Które przepisy regulują kwestie bezpieczeństwa (cyberbezpieczeństwa) w szkole?	Przepisy ogólne ustawy - prawo oświatowe stanowią, że system oświaty zapewnia wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej. Zadaniem systemu oświaty jest również upowszechnianie wśród dzieci i młodzieży wiedzy o cyberbezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych. Zadania szkoły oraz obowiązkowe cele kształcenia i treści nauczania dotyczące bezpieczeństwa, w tym priorytety wychowawcze, określa podstawa programowa kształcenia ogólnego[286]. Preambuła podstawy programowej kształcenia ogólnego wskazuje, że zadaniem szkoły jest zapewnienie uczniom bezpiecznych warunków oraz przyjaznej atmosfery do nauki. Najważniejszym celem kształcenia w szkole podstawowej jest dbałość o integralny rozwój biologiczny, poznawczy, emocjonalny, społeczny i moralny ucznia. Proces kształcenia i wychowania powinien wprowadzić uczniów w świat wartości, wskazać wzorce postępowania i budowania relacji społecznych sprzyjających bezpiecznemu rozwojowi ucznia (rodzina, przyjaciele), zbudować poczucie godności własnej osoby i szacunku dla godności innych osób, wyposażyć w zasób wiadomości oraz umiejętności, który pozwoli w sposób bardziej dojrzały i uporządkowany zrozumieć świat. Podstawa programowa podkreśla potrzebę rozwijania u uczniów postaw otwartości wobec świata i innych ludzi, aktywności w życiu społecznym oraz odpowiedzialności za zbiorowość.
2) Jakie istnieją metody i obszary edukacji użytkowników?	Szkoła ma stwarzać uczniom warunki do nabywania wiedzy i umiejętności potrzebnych do rozwiązywania problemów z wykorzystaniem metod i technik wywodzących się z informatyki, w tym logicznego i algorytmicznego myślenia, programowania, posługiwania się aplikacjami komputerowymi, wyszukiwania i wykorzystywania informacji z różnych źródeł, posługiwania się komputerem i podstawowymi urządzeniami cyfrowymi oraz stosowania tych umiejętności na zajęciach z różnych przedmiotów, m.in. do pracy nad tekstem, wykonywania obliczeń, przetwarzania informacji i jej prezentacji w różnych postaciach. Szkoła ma również przygotowywać uczniów do dokonywania świadomych i odpowiedzialnych wyborów w trakcie korzystania z zasobów dostępnych w Internecie, krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci. Podstawa programowa informatyki – wskazuje cel kształcenia, jakim jest przestrzeganie prawa i zasad bezpieczeństwa, respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią. Zgodnie z powyższym, wymagania szczegółowe wskazują, że uczeń: ➢ postępuje zgodnie z zasadami netykiety oraz regulacjami prawnymi

[286] Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz. U. poz. 356 z późn.zm.) oraz rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz.U. z 2018 r. poz. 467 z późn.zm.).

	dotyczącymi: ochrony danych osobowych, ochrony informacji oraz prawa autorskiego i ochrony własności intelektualnej w dostępie do informacji; jest świadomy konsekwencji łamania tych zasad; ➢ respektuje obowiązujące prawo i normy etyczne dotyczące korzystania i rozpowszechniania oprogramowania komputerowego, aplikacji cudzych i własnych oraz dokumentów elektronicznych; ➢ stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji; ➢ opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa. W nauczaniu informatyki zaakcentowane zostały kompetencje społeczne. Wskazano np. bezpieczne budowanie swojego wizerunku w przestrzeni medialnej.
3) W jaki sposób szkoły podstawowe powinny kształtować kompetencje cyfrowe uczniów oraz nauczycieli? Czy punkt wyjścia stanowi podstawa programowa?	Podstawa programowa kształcenia ogólnego, kładzie nacisk na rozwijanie u uczniów kompetencji kluczowych, w tym kompetencji cyfrowych. Za jedną z najważniejszych umiejętności, które zdobywają uczniowie w ramach edukacji szkolnej, uznano sprawne i odpowiedzialne posługiwanie się technologiami informacyjno-komunikacyjnymi w procesie uczenia się. Szkoła powinna przygotować uczniów do świadomego i odpowiedzialnego korzystania z technologii informacyjno-komunikacyjnych, wyposażyć ich w kompetencje potrzebne do korzystania z różnych cyfrowych zasobów informacyjnych, wyszukiwania i krytycznej analizy informacji, bezpiecznego poruszania się w przestrzeni cyfrowej, w tym nawiązywania i utrzymywania opartych na wzajemnym szacunku relacji z innymi użytkownikami sieci.
4) W której klasie szkoły podstawowej uczniowie po raz pierwszy zapoznawani są z tematem bezpiecznego zachowania w Internecie? Czy edukacja dot. cyberzagrożeń powinna zostać rozszerzona już w I etapie edukacyjnym?	Na etapie edukacji wczesnoszkolnej (klasy I-III szkoły podstawowej) uczniowie rozwijają umiejętności w zakresie rozumienia, analizowania i rozwiązywania problemów, programowania i rozwiązywania problemów z wykorzystaniem komputera i innych urządzeń cyfrowych, posługiwania się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, rozwijania kompetencji społecznych, przestrzegania prawa i zasad bezpieczeństwa. W klasach IV-VIII szkoły podstawowej uczniowie zapoznają się m.in. z: ➢ przyjętymi zasadami i prawem, ➢ prawem do prywatności danych i informacji oraz prawem do własności intelektualnej, ➢ zagrożeniami związanymi z powszechnym dostępem do technologii oraz do informacji, metodami wystrzegania się ich, ➢ profilaktyką antywirusową, zabezpieczeniami przed zagrożeniem komputera wraz z zawartymi w nim informacjami, ➢ kwestiami etycznymi związanymi z wykorzystaniem komputerów i sieci, takimi jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją.
5) Jak istotne jest edukowanie użytkowników sieci i najmłodszych uczniów do właściwych zachowań w cyberprzestrzeni?	Uczniowie klas I-III realizują treści nauczania obszaru edukacja informatyczna w formie kształcenia zintegrowanego, w którym nie określa się liczby godzin dla poszczególnych obszarów nauczania. W klasach IV-VIII szkoły podstawowej na zajęcia informatyki przeznaczono po 1 godzinie tygodniowo. Zajęcia informatyki w szkołach ponadpodstawowych (lo, technikum) w zakresie podstawowym realizowane są w wymiarze trzech godzin w okresie nauczania. Zakres rozszerzony informatyki uczniowie realizują w wymiarze dodatkowo zwiększonym o sześć godzin tygodniowo w okresie nauczania. Zachowaniom bezpiecznym i odpowiedzialnym podczas korzystania z portali i mediów społecznościowych sprzyja ponadto realizacja treści nauczania zawartych w innych przedmiotach, jak: język polski, język

	obcy nowożytny, wiedza o społeczeństwie, etyka, wychowanie do życia w rodzinie. Cele kształcenia informatycznego – wymagania ogólne – są takie same dla wszystkich etapów edukacyjnych i dla wszystkich typów szkół. Ich interpretacja jest zapisana w postaci wymagań szczegółowych. Treści podstawy programowej z informatyki mają charakter przyrostowy, sugerując w ten sposób spiralny rozwój wiedzy, umiejętności i kompetencji uczniów przez wszystkie lata nauki szkolnej. Cele kształcenia Informatyki zdefiniowane w podstawie programowej obejmują: 1) rozumienie, analizowanie i rozwiązywanie problemów na bazie logicznego i abstrakcyjnego myślenia, myślenia algorytmicznego i sposobów reprezentowania informacji, 2) programowanie i rozwiązywanie problemów z wykorzystaniem komputera oraz innych urządzeń cyfrowych: układanie i programowanie algorytmów, organizowanie, wyszukiwanie i udostępnianie informacji, posługiwanie się aplikacjami komputerowymi, 3) posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów, 4) rozwijanie kompetencji społecznych, takich jak komunikacja i współpraca w grupie, w tym w środowiskach wirtualnych, udział w projektach zespołowych oraz zarządzanie projektami, 5) przestrzeganie prawa i zasad bezpieczeństwa; respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych. Przyjęte cele mają swoje odzwierciedlenie w treściach nauczania - wymaganiach szczegółowych określonych dla uczniów szkoły podstawowej i dla uczniów szkół ponadpodstawowych. W porównaniu ze szkołą podstawową w liceum ogólnokształcącym i technikum wymagania z zakresu informatyki mają odpowiednio wyższy stopień trudności i są bardziej sproblematyzowane.

Źródło: opracowanie własne wyników badań

Indywidualny wywiad pogłębiony *(IDI)* w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni, czyli specjalistycznym komponencie SZ RP powołanym 8 lutego 2022 r. Ekspertem był Dyrektor: Pan gen. dyw. Karol Molenda. Wywiad przeprowadzony na platformie *YouTube* w ramach programu Didaskalia przez pana Patrycjusza Wyżgę[287].

Celem badania było poznanie opinii Dyrektora dotyczących:

1) Opinii na temat realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji – zadań realizowanych przez DKWOC;
2) Oceny kierunków i kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa;
3) Istoty edukacji użytkowników sieci.

[287] *https://www.youtube.com/watch?v=rwDbiKutDbc&t=2792s&ab_channel=didaskalia* [dostęp z dnia 03.05.2024 r.].

Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni, gen. dyw. Karol Molenda. Od 2016 roku cyberprzestrzeń jest domeną wojny, obok lądu, powietrza, morza. Jest to kolejna domena operacyjna. Powinno się jej bronić na równi z pozostałymi. W tradycyjnym konflikcie kiedy przeciwnik przekracza granicę, narusza integralność granicy, mamy jasno wskazany atak. Z cyberprzestrzenią jest inaczej, bowiem w cyberprzestrzeni takich granic nie ma.

Tab. 6.4

Wywiad ekspercki nr 4. Opinia Pracownika DKWOC

Pytanie badawcze	**Odpowiedzi eksperta**
1) Czy obecnie jesteśmy w trakcie konfliktu, wojny w cyberprzestrzeni?	Jestem przekonany i zawsze podnosiłem, że też nie ma pokoju, nie ma czasu pokoju, ten czas możemy podzielić na czas rywalizacji konfliktu i wojny. Cyberprzestrzeń to szersze pojęcie natomiast chociażby jak zwrócimy uwagę na to co dzieje się w Internecie. W chwili obecnej tam jest rywalizacja. A jestem przekonany, że w wielu momentach jest konflikt w naszych systemach. Przeciwnicy próbują oddziaływać na nasze systemy każdego dnia. Jestem przekonany, że to jest konflikt. Nie definiowałbym tego jeszcze jako cyberwojna, bo to wielokrotnie niektórzy podnoszą że jest cyberwojna- no nie ma jeszcze, oby nigdy nie było żadnych skutków takich namacalnych czyli materialnych czy zniszczenia. W chwili obecnej mamy konflikt, czyli tu jest bardziej działanie pewnych grup i te grupy można podzielić na grupy cyberprzestępcze ale też na grupy tak zwane *„apt advance persistent”* to są grupy, które są dobrze fundowane i które działają pod egidą obcych służb specjalnych i ich cel to oddziaływanie na infrastrukturę danego kraju i uzyskiwanie efektów. No jednym takich namacalnych efektów może być pozyskiwanie informacji i uzupełnianie, przekazywanie tej informacji do tych służb. My w naszej infrastrukturze broniąc jej na co dzień spotykamy się właśnie z takimi grupami czy grupami apt, które każdego dnia próbują tzn. wielokrotnie w ciągu dnia próbują oddziaływać na nasze systemy. Dlatego też na naszych salach operacyjnych służba trwa 24 na 7, więc byliśmy pierwszym zespołem w Polsce, który od stycznia 2020 roku uruchomił właśnie takie zespoły monitorujące nasze systemy w trybie 24/7, bo trudno sobie wyobrazić taką sytuację, że eksperci od cyberbezpieczeństwa w piątek o 15:30 idą do domu, a nieprzyjaciel też idzie do domu, więc zazwyczaj te incydenty miały miejsce właśnie w weekendy w piątek wieczorem, stąd zwróciliśmy na to uwagę.
2) Co można zaznaczyć w kwestii współpracy międzynarodowej?	Współpraca międzynarodowa ale też wewnątrz kraju się zmieniła i zmieniliśmy nasz punkt odniesienia z *need To Know* na *need to share*, czyli co wiesz informuj- bo być może inni dzięki twojej informacji zabezpieczą swoją infrastrukturę, więc w tej chwili dość głośno też na naszych internetowych portalach informujemy, że głównymi takimi grupami chociażby to grupa apt28 czy apt 29, grupy które są kojarzone z FSB czy Gru czyli FSB Służba Bezpieczeństwa Wewnętrznego Federacji Rosyjskiej wywiad wojskowy rosyjski, czyli dwa razy Służby specjalne Rosji, które sponsorują te grupy i te grupy próbują oddziaływać na naszą infrastrukturę ale też to co robimy to uczymy się tego nieprzyjaciela, uczymy się taktyk technik procedur, narzędzi i informujemy innych naszych partnerów o tym co pozwala zabezpieczyć, podnieść poziom cyberbezpieczeństwa w naszym kraju ale też u naszych partnerów. Jestem przekonany, że w chwili obecnej włodarze rosyjscy skupiają się głównie na szpiegostwie, czyli próbie uzyskania informacji, co można

	sobie też powiązać z naszym wsparciem dla Ukrainy, czyli chociażby fakt, że w Polsce funkcjonuje *Hub,* przez który przechodzi większość wsparcia o ile nie całe. Jeżeli mówimy o militarnym wsparciu, to powoduje, że te grupy są zainteresowane by uzyskać informacje, co będzie wysyłane i kiedy, więc nasze systemy są pod ogromnym ostrzałem, ale co zauważyłem i co my zauważyliśmy, to też systemy firm i instytucji, które z nami współpracują w tym całym procesie, dlatego też od zeszłego roku dość intensywnie nie tylko zabezpieczamy siebie i monitorujemy nasze systemy, ale również wspomagamy naszych partnerów wysyłając chociażby nasze tak zwane grupy szybkiego reagowania *Rapid reaction teams*, które mogą pomóc tam gdzie jakaś infrastruktura jest atakowana przez wspólnego wroga. Mamy ustawę z 2018 roku, która odpowiedzialność za cyberprzestrzeń dzieli na takie trzy grupy poziomu krajowego: mamy taką wojsku w mojej strukturze, mamy kolejną w ABW i w NASKu w instytucie badawczym i to są trzy grupy. Każdy ma swój zakres odpowiedzialności, ale tutaj mówimy wówczas o koordynowaniu obsługi incydentów, czyli incydent musi się zmaterializować i wówczas odpowiedni zespół koordynuje jego obsługę. Moje podejście i mojego zespołu od samego początku było trochę inne, bardziej proaktywne czyli oprócz tego, że mamy ten zespół, który właśnie odpowiada za koordynację jeżeli incydent ma miejsce, to mamy też zespoły, które polują na adwersarzy czyli wychodzimy z założenia że w danej sieci zawsze jest nieprzyjaciel czy jakieś grupy hakerskie, które tam operują i mamy zespoły, które mają odpowiednią wiedzę i zestaw narzędzi, tak by wpiąć się w tą sieć i polować na adwersarza, sprawdzać kto się tam pojawia lub w nieznanych różnych fragmentach logach czy tam nie ma obecności adwersarza. Jeżeli jest, to spowodować tak żeby go nie było i utwardzić tą sieć ale też znaleźć przyczyny w jaki sposób tam wszedł szkolić administratorów ale też użytkowników więc szereg różnych wyzwań. To jest jedno z naszych głównych zadań i takimi zespołami dysponujemy, czyli to jest takie polowania na adwersarza czyli ale to jest wciąż w domenie obrony prawda. Czyli szukanie tego kto nas atakuje w ten sposób się bronimy, no najlepszą broną jest atak ale atakowanie tego, który nas chce zaatakować przynajmniej zbliża się do naszych granic żeby w nas uderzyć. Ustawa o broni ojczyzny definiuje w artykule 15 nas jako wojska obrony cyberprzestrzeni i definiuje, że jesteśmy specjalistycznym komponentem uprawnionym do prowadzenia operacji w pełnym spektrum. NATO definiuje działania w cyberprzestrzeni na trzy główne grupy, czyli mamy *Defense Cyber Operations* – obronne, to jest *Intelligence Recon*, czyli takie bardziej Cyber rozpoznanie i *Offensive Cyber Operations*, więc budujemy kompetencje do tego by działać w pełnym Spektrum i to ja też podnoszę i od samego początku, gdy pisałem koncepcję utworzenia wojsk obronny cyberprzestrzeni zakładałem, że musimy posiadać takie kompetencje kraje w NATO są podzielone, część definiuje że takowe buduje, choć nie wszystkie kraje tak definiują. Natomiast, te które największe doświadczenie mają i autorytet w kraju i możliwości, czyli chociażby Amerykanie, Brytyjczycy, Francuzi czy Niemcy zdefiniowali sobie również, że mogą prowadzić operacje ofensywne w cyberprzestrzeni w odpowiedzi na atak. Naszym założeniem było też by takie zespoły posiadały takie kompetencje, takie zdolności. Pozostaje aspekt prawny, bo nie do końca zostało to zdefiniowane, nie mamy kontratypu, czyli nikt nas nie zwolnił z odpowiedzialności za pewne działanie. Tutaj już jest to teraz doprecyzowane, mam nadzieję, że w przyszłości zostanie to uregulowane w ustawie, jeszcze by w odpowiedzi na atak- wojsko w czasie pokoju było w stanie odpowiedzieć atakując adekwatnie do ataku, skoro my jesteśmy obiektem ataku.
3) Jak istotne jest budowanie świadomości zagrożeń?	Ten proces budowania świadomości pośród też decydentów, no musi trwać, bo bo nie wszyscy tak dokładnie rozumieją, co się dzieje w cy-

	berprzestrzeni, to że nam dobrze idzie i nie ma żółtego pasku że Polska została zhakowana, to z drugiej strony nie pomaga trochę, no bo też nie wszyscy dostrzegają, co się dzieje, a to nie znaczy, że nie była potężna próba czy nie ma cały czas prób zhakowania. Po prostu zostały odparte te próby. Rozmowy prowadzę z zarówno z ministrem Obrony Narodowej, ale również z BBN ta świadomość już jest, że te uprawnienia wojska obrony cyberprzestrzeni powinny mieć bazując chociażby na doświadczeniu naszych partnerów zagranicznych. No ale można sobie wyobrazić sytuację, że do ataku dochodzi, jakiś serwer gromadzi dane z zagranicy z danego kraju i ten serwer będzie aktywny dwie godziny. No nie sposób uzyskać zgodę prezydenta na chociażby wejście na ten serwer i usunięcie danych z danego kraju. Stąd Amerykanie już to przepracowali i dowódca *US Command* ma uprawnienia, że jeżeli jest atak na jego kraj, by wykorzystywać wojsko do odpowiedzenia na ten atak. Wiadomo, że system prawny jest inny, więc to też nie można kalki brać z tego. Niemniej jednak te same dyskusje w Polsce trwają, w przypadku ataku na nasz kraj, aby nie uruchamiać jakieś takiej machiny uzyskiwania zgód odpowiednich, tylko by było to w stałych planach obronnych, że jest atak- wojsko odpowiada i właśnie zdefiniowanie, że nie musimy tu nikomu wojny wypowiadać jak to teraz jest tam. Historycznie, historycy pewnie lepiej wiedzą ile razy kiedy na świecie, kto komu wojnę wypowiedział, natomiast cyberprzestrzeni podkreślam ja cały czas że tego stanu pokoju nie ma, rywalizacja konflikt wojna i można sobie założyć taki scenariusz że atak kraj jest atakowany no i teraz dobrze by było nie poświęcać zbyt dużo czasu na uzyskiwanie odpowiednich zgód na działanie, biorąc pod uwagę fakt, że mamy zespoły gotowe by działać. To jest niesamowite, my jesteśmy zupełnie tego nieświadomi, za naszymi granicami trwa wojna ale my mamy tutaj pokój, doskonale będziemy wiedzieli kiedy wojna się zacznie, a nawet kiedy zacznie się zbliżać, co nie znaczy, że nie ma pokoju w cyberprzestrzeni. A my w cyberprzestrzeni jesteśmy dzisiaj zanurzeni. No można sprawdzić jak głęboko, po kilka godzin przynajmniej na dobę siedząc w naszych telefonach, laptopach. Tak to statystycznie ja sprawdzałem swego czasu na ponad 8 miliardów ludzi a świecie, 5,2 miliarda dysponuje urządzeniami mobilnymi, więc jest aktywnych online, a ciekawostka, 4,2 miliarda ma szczoteczki do zębów, więc teoretycznie więcej osób ma urządzenia mobilne i korzysta z internetu niż myje zęby, co jest ciekawą statystyką. To znaczy, że bardziej potrzebujemy cyber żołnierzy niż dentystów. My jesteśmy na celowniku, faktycznie nasi analitycy bazując na danych od naszych partnerów zdefiniowali i zauważyli, że jeżeli chodzi o jeden z typów ataków, czyli tak zwany atak DDOS, to ostatnie tygodnie wskazują, że Polska jest najbardziej atakowanym krajem na świecie. To jest niesamowite, no bo jak popatrzy się na skalę tych ataków DDOS, czyli odmowy usługi- to są ataki, to że nie widzimy konsekwencji, wielokrotnie jak my śpimy, oni się pocą, tak by te usługi działały, to w ostatnich dniach Polska znalazła się na pierwszym miejscu najczęściej atakowanych państw świata, a w okresie całego stycznia 2024 znajduje się na drugim miejscu.
4) Jaki jest poziom wiedzy i umiejętności specjalistów w DKWOC?	Polacy należą do elity jeżeli chodzi o te umiejętności te twarde umiejętności związane z informatyką, matematyką, kryptologią. Ja znam mój zespół, więc to jest fantastyczny zespół młodych osób, które działają nietuzinkowo. My nie mamy takiej broni, nie ma nas na defiladach i nie widać nas może tak bardzo, natomiast siła nasza to nie siła mięśni, a intelektu. Na pokładzie są osoby, które są światowej klasy ekspertami w zakresie cyberbezpieczeństwa. W grudniu 2022 roku był taki raport, został napisany przez ekspertów z uczelni amerykańskiej, który definiował Polskę na szóstym miejscu w zakresie cyberbezpieczeństwa. Wiadomo, że to jest takie uznaniowe, bo tam były punkty, ale wojska obrony cyberprzestrzeni były tam zdefiniowane wręcz z nazwy wpisane w tym raporcie, jako te które wspomagają bardzo Ukrainę w tym zakresie.

	Udowodniono matematycznie, zdefiniowano ilość Polaków na olimpiadach zagranicznych zdobywających trofea i na pierwsze miejsca i *per capita* stwierdzono, że Polacy są najlepsi i udowodniono to wzorem. Mamy takie ćwiczenia w NATO, które nazywają się lock, to są największe ćwiczenia z zakresu *Cyber* bezpieczeństwa na świecie. W trakcie dwóch dni broni się infrastruktury bardzo złożonej, która jest cały czas atakowana i Polska zajęła w zeszłym roku trzecie miejsce, dwa lata wcześniej drugie miejsce na świecie. No to też powoduje, że jeżeli chodzi tą Cyber obronę możemy czuć się dumni, ale jest zawsze ale- cyberbezpieczeństwo jest procesem, nie stanem. Niestety ja bardzo lubię informatykę, bo tam jest 01 póki co. Należy być czujnym i rozwijać swoje kompetencje. Systemy każdego dnia dość mocno są atakowane, więc te zespoły które są na salach operacyjnych zyskują niesamowitą wiedzę na temat najnowszych taktyk technik i procedur, którymi operują przeciwnicy, ale też my rozwijamy, inwestujemy w kapitał, szkolenia, które moi cyber żołnierze mogą mieć i mają. No są naprawdę niespotykane na świecie, łącznie z tym, że współpracujemy z kilkoma międzynarodowymi partnerami, chociażby Stanami Zjednoczonymi, gdzie moi żołnierze razem z żołnierzami wojsk amerykańskich się szkolą czy Izraela, to najlepsi z najlepszych szkolą naszych cyber żołnierzy, więc oni budują swój kapitał, ale też wychodziliśmy z założenia, że za talent należy płacić, więc być może nie jest to adekwatne do rynku cywilnego i to jest zawsze wyzwaniem, natomiast od samego początku była decyzja ministra obrony narodowej, że są specjalne dodatki dla osób, które realizują zadania z zakresu cyberbezpieczeństwa, ale również jest ustawa o świadczeniach teleinformatycznych dla całej administracji publicznej państwowej która i ekspertów, którzy zajmują się cyberbezpieczeństwem. My też jesteśmy beneficjentem tych środków. O ile dobrze pamiętam za zeszły rok maksymalna wysokość dodatku było chyba 48000 brutto miesięcznie, to już pozwala nam utrzymać najlepszych w naszych szeregach, a konkurencja jest ogromna. No właśnie brakuje około 3 milionów ekspertów zakresu cyberbezpieczeństwa na całym świecie. Tak się szacuje na chwilę obecną więc niesamowite liczby. Po prostu chodzi o to żeby tych ludzi nie wypuszczać do prywatnego biznesu, gdzie zarobią więcej. Cel jest jeden, żeby po prostu bronili nas wszystkich, żebyśmy sobie spokojnie mogli spać, jest zrozumienie wśród polityków szczególnie.
5) Jak można opisać rolę Pana jednostki w systemie cyberbezpieczeństwa?	To jest cyberprzestrzeń, gdzie normalnie można toczyć wojnę, skoro tak, to potrzebna jest armia która toczy wojny czy prowadzi konflikt. Niestety Rosjanie atakują, my się bronimy, może to się kiedyś zmieni, będziemy bardzie pro aktywnie działać. Oby tak kiedyś w istocie było, byśmy potrafili odpierać ataki jeszcze skuteczniej także w cyberprzestrzeni, więc proszę to zwyczajnie docenić. A co jest karabinem maszynowym żołnierza wojsk obrony cyberprzestrzeni? Żołnierz, piechota używa karabinków, a żołnierz cyber, obrony cyberprzestrzeni jakiego używa arsenału? Jego bronią jest laptop i wiedza jest jego bronią, przede wszystkim. Ja zawsze podkreślam, że mój zespół inwestował w wiedzę, bo tylko bycie lepszym od przeciwnika pozwala nam utrzymać nasz poziom. Natomiast DKWOC, to nie tylko monitorowanie i prowadzenie działań operacji w cyberprzestrzeni, ale również jesteśmy dostawcą usług te informatycznych wszystkich systemów i wszystkich sieci do całych sił zbrojnych, więc my budujemy. Nie ma komputera, komórki, serwera, który nie zostałby zakupiony i skonfigurowany, utrzymywany przez naszych specjalistów i dostarczamy te usługi dla całych sił zbrojnych do wszystkich dowództw i tu nie chodzi o jawną sieć tylko, ale też systemy niejawne, w tym system zastrzeżony system tajny i to są systemy gdzie mamy po 160 - 170 tys. użytkowników. To my utrzymujemy to wszystko, co pozwala nam właśnie też odpowiedni poziom cyberbezpieczeństwa wdrożyć, bo zawsze jest taki delikatny konflikt pomiędzy bezpieczeństwem, a funkcjonalnością. Swego

	czasu w resorcie obrony narodowej w siłach zbrojnych były instytucje, które z jednej strony albo budowały systemy albo odpowiadały za cyberbezpieczeństwo, natomiast one ze sobą nie chciałbym powiedzieć, że zwalczały, ale konkurowały czy bezpieczeństwo ponad funkcjonalność czy funkcjonalność ponad bezpieczeństwo. W chwili obecnej jest to pod jednym dachem, więc tak naprawdę my bazując na analizie ryzyka, ale też właśnie na tej wiedzy, którą mamy o przeciwniku, o jego zdolnościach możemy ten balans zachować, więc to jest to jest bardzo istotny aspekt, którego nie chciałbym pominąć, bo mamy w całym kraju jednostki, które dostarczają systemy usługi do wszystkich jednostek wojskowych, to jest ponad 700 jednostek, stąd ogromne wyzwanie ale też mamy krypto analizę, mamy osoby, które piszą kod i które łamią kody, więc te chlubne tradycje naszych kryptologów kultywujemy w dalszym ciągu i mam właśnie przyjemność przewodzić nie zink osobom posiadającym nietuzinkową wiedzę chyba jednym z najlepszych w Polsce, którzy tworzą algorytmy kryptograficzne, tak by zapewnić odpowiednią poufność przesyłania danych lub tworzą szyfratory, bo to też są urządzenia, które są niezbędne do tego by systemy niejawne mogły funkcjonować. A sama konstrukcja takiego szyfratora jest specyficzna. bo on teoretycznie powinien być tak skonfigurowany. że nawet gdyby wpadł w dłonie ręce nieprzyjaciela to próba ingerencji powinna usunąć wszystko co jest w środku. Więc niesamowite procesy, nie za dużo o nich pewnie możemy mówić, ale zachęcam wszystkich, którzy mają tą ciekawość tej domeny i tych działań, żeby do nas dołączyli. To są tradycje, które w Polsce są od lat kultywowane i w dalszym ciągu mamy taki potencjał wszyscy wiemy i chlubimy się i pamiętamy i opowiadamy oglądamy filmy, o tym jak polscy naukowcy potrafili rozwikłać niemiecką Enigmę, więc to jest taka chlubna historia. To o czym wspominałem, n*eed To Know*, na *need to share*. Amerykanie informowali głośno nawet, że dojdzie do tego konfliktu dojdzie do wojny w Ukrainie. My przygotowaliśmy się do tego od dłuższego czasu, czyli właśnie bardzo dobrze znaliśmy tych przeciwników którzy operują w cyberprzestrzeni kilka dni przed wybuchem wojny z Polsce przez premiera na *Charlie CRP*, czyli stan alarmowy w cyberprzestrzeni na trzeci z czwartego najwyższych i on obowiązuje cały czas ponad 700 dni. Tak obowiązuje ten stan stopień trzeci, znaczy że administratorzy czy właściciele infrastruktury krytycznej systemów, które tam działają mają 24 na 7 dostępnych ekspertów, ale również regularnie przeglądają stan bezpieczeństwa tych systemów. U nas to się nie zmieniło, bo tak jak wspominałem już dwa lata wcześniej w naszych salach operacyjnych, w trybie *Charlie CRP* funkcjonowali i funkcjonujemy dalej. Natomiast jest to dość duże wyzwanie dla wielu zwłaszcza mniejszych podmiotów, by taką kadrę utrzymać, ale to dlatego że były informacje o tym że infrastruktura krytyczna może być atakowana, że te grupy zadziałają czy jeszcze przed wybuchem wojny, natomiast bardzo ciekawy aspekt, który właśnie tego 24 w cyberprzestrzeni się pojawił, a nie jest dość głośny, znaczy eksperci o nim wiedzą ale jakby publicznie nie rozszedł się: to wówczas w trakcie inwazji Rosjanie wykorzystali cyberprzestrzeń, bo zaatakowali visat, czyli komunikację satelitarną wykorzystaną wykorzystywaną przez wojsko ukraińskie, czyli odcięli ich od komunikacji, to był dobry przykład integracji efektu takiego Sił Zbrojnych rosyjskich z tym efektem *Cyber* i no tylko pomoc tak naprawdę zachodu, z tych krajów które stanęły za Ukrainą spowodowała, że starlinki się pojawiły, że inne alternatywne środki komunikacji dostęp do Internetu, bo inaczej to te działania Cyber by odcięły Ukrainę od możliwości wysyłania informacji, czyli tak naprawdę moglibyśmy do końca nie wiedzieć co tam się dzieje. Doskonały przykład na to, że ta domena cyberprzestrzeni została wykorzystana. Rozpoczęto agresywne działania wojenne, właśnie w tej domenie, nie tylko wjechały czołgi głębiej w terytorium Ukrainy, wleciały

	śmigłowce z desantem, ale po prostu zaatakowana też w cyberprzestrzeń. Tak niemniej jednak też pragnę zauważyć, że Ukraińcy dość dobrze się do tego przygotowywali. Znam te zespoły ukraińskie, które od 2014 roku kiedy tak spektakularnie *Blackout* był i odcięcie energii przez atak *Cyber* cyberprzestrzeni budowały swoje kompetencje pozyskiwał informacje wsparcie ze strony USA. Jak budować odporność swoich systemów u nas, my też szkoliliśmy naszych kolegów z Ukrainy jak z informacji, których posiadamy na temat właśnie taktyk technik procedur tego tych adwersarzy narzędzi w dalszym ciągu tą informację z tą informacją się z nimi dzielimy, co więcej oni kilka razy nawet medialnie i oficjalnie podziękowali, że dzięki informacji którą otrzymali od Polski mogli przeciwdziałać atakowi, który miał u nich miejsce, więc ta wymiana informacji jest tutaj krytyczna i niezbędna w cyberprzestrzeni, bo wielokrotnie widzimy, że wszyscy zmagamy się z tym samym adwersarzem, każdy kraj z osobna, a przez to, że ta informacja nie przechodziła tak elastycznie pomiędzy i tak szybko pomiędzy naszymi krajami. Wyszedłem w 2021 roku z pewną inicjatywą, gdzie zaprosiłem ekspertów z NATO, by spotkali się u nas w dowództwie na sali w trybie niejawnym i zaproszenie nazwaliśmy to summit. W tym zaproszeniu było zdefiniowane, że każdy z uczestników, który usiądzie do stołu ma obowiązek przedstawić *Case* swojego kraju on może być na poziomie tajnym, czyli, że wiadomo tego nie opublikujemy, ale by wymienić informacjami, jak był atak, jakie narzędzia przeciwnika były wykorzystane, co oni z tym zrobili. Ta wymiana informacji i wnioski wskazywały jednoznacznie, że w większości przeciwnicy są ci sami, wykorzystują dokładnie te same narzędzia, te same taktyki i tylko te braki komunikacyjne powodują, że są skuteczni. Szereg różnych inicjatyw mających na celu podpisanie różnych porozumień z krajami bilateralnymi też aby ten przepływ informacji był każdego dnia, spowodował że teraz nam może jest łatwiej wszystkim się bronić, ale też bardzo na przykład czerpiemy informacji z Ukrainy gdzie jak oni są atakowani to ta informacja do nas wpływa, dzięki temu my możemy zaimplementować z wyprzedzeniem pewne mechanizmy obronne i by ten atak, który ma miejsce w Ukrainie nie mógł mieć miejsca w Polsce.
6) W jaki sposób można zachęcać „normalnego" użytkownika do właściwych zachowań w sieci?	Higienę cyfrową staram się nie tylko przestrzegać, ale również zachęcać moich bliskich. Jedno z większych moich życiowych wyzwań by zachęcić do zwrócenia uwagi, zwłaszcza te pokolenie Z, które urodziło się z komórką można powiedzieć. Urządzenia cyfrowe, które są online i oni cały czas online, więc zachęcenie kogokolwiek z bliskiego żeby miał różne hasła do różnych portali, żeby nie to samo właśnie we wszystkich miejscach lub żeby była zaimplementowana *MFA*, czyli *multifactor* - wieloskładnikowe uwierzytelnienie, czyli coś co wiem plus coś co mam, to dla nich jest wyzwaniem. To było życiowym wyzwaniem wobec bliskich, natomiast też współpracowników, my jedno właśnie z takich pierwszych działań mających na celu utwardzenie naszej infrastruktury, to było zaimplementowanie w siłach zbrojnych i to też w 2020 roku *MFA*. Właśnie nie ma możliwości żeby było same hasło w naszych systemach pocztowych. Natomiast jeżeli spojrzy się na tak dużą instytucję, gdzie właśnie mamy sieci po ponad 100 000 kont użytkowników, to implementacja w tak dużej sieci i w ogóle przekonanie użytkowników do pewnej cyber higieny, czy wręcz jej wymuszenie w niektórych aspektach, jest wyzwaniem takim też dla każdego z osób które tym się zajmują. Utworzyliśmy wojskowe ogólnokształcące liceum, informatyczne, które jest przy WAT-cie i to był strzał w dziesiątkę, bo ponad 10 osób na miejsce, a absolwenci tego liceum wychodzą, mają poziom programowania, drugi rok studiów, więc no oczywiście z założenia zachęcamy, te osoby, następny krok to Wojskowa Akademia Techniczna, ale również szereg różnych inicjatyw, cybermil z klasą. W każdym województwie jest klasa, w szkole, którą promujemy, gdzie

	kształtujemy program szkolenia i też zachęcamy, żeby kolejny krok, to była Wojskowa Akademia Techniczna lub inna wojskowa uczelnia. Akademia Marynarki Wojennej to jest kolejna uczelnia, która też w zakresie cyberbezpieczeństwa kształci, więc ja od razu zakładałem, że nie będę konkurował tu z rynkiem prywatnym i kradł czy kłusował tam ale bardziej, że będziemy tworzyć ten talent, wychowywać trochę od podstaw i te projekty teraz przynoszą jakieś wymierne skutki, naprawdę mam grupę osób, które przychodzą magister inżynier podporucznik, piękny początek kariery, który od razu wie, że po uczelni nie trafi do jednostki liniowej, tylko trafi tutaj do sali operacyjnej, będzie się uczył. On myśli wtedy, że skończy uczelnię, wie już wszystko, przychodzi drugiego dnia dowiaduje się, że jest na samym początku drogi, jeszcze dużo nauki przed nim, ale tak kształtuje się właśnie intelekt, tutaj u nas w dowództwie.

Źródło: opracowanie własne wyników badań

Indywidualny wywiad pogłębiony *(IDI)* z prokuratorem i biegłym sądowym w śladach cyfrowych. Ekspert- Pan dr. inż. Paweł Opitek.

Głównymi celami badania było poznanie opinii Pana Prokuratora dotyczących:

1) Oceny kierunków i kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa;
2) Oceny sposobów edukacji użytkowników sieci;
3) Oceny efektywności w wykrywaniu cyberprzestępstw;
4) Opinii na temat wyzwań w reagowaniu na łamanie prawa w sieci.

Tab. 6.5

Wywiad ekspercki nr 5. Opinia Pracownika Prokuratury

Pytanie badawcze	**Odpowiedzi eksperta**
1) Jakie kluczowe zadania i cele realizuje Pan w swojej pracy?	Wykonuję zawód prokuratora, a więc kluczowe cele, jakie realizuję w swojej pracy, to zadania postawione prokuraturze, tj. zwalczanie przestępczości i ściganie sprawców przestępstw. Jest to szereg czynności: operacyjno-rozpoznawczych, obejmujących postępowanie przygotowawcze i sądowe. Przy realizacji tych zadań bardzo ważną rolę odgrywają ślady i dowody cyfrowe. Każde przestępstwo może być dokonane przy wykorzystaniu świata wirtualnego np. groźby karalne, znęcanie, podżeganie do zabójstwa niekiedy posiadają odnośniki do świata cyfrowego. Nie tylko w cyberprzestępstwach ale również w typowych przestępstwach badane są ślady cyfrowe. W tym kontekście istotne jest także cyberbezpieczeństwo. Cyberprzestępczość jest powiązana z cyberbezpieczeństwem np. czyn karalny może dotyczyć działania administratora systemu informatycznego lub teleinformatycznego. Wówczas należy poznać reguły i regulaminy obowiązujące w danym podmiocie, określić kto był odpowiedzialny za bezpieczeństwo systemu, aby ewentualnie wskazać przyczynę, wskazać sprawcę ataku lub incydentu.
2) Co rozumie Pan pod pojęciem Systemu cyberbezpieczeństwa RP? Czy istnieją podmioty, które Pana zdaniem warto włączyć w ten system?	System cyberbezpieczeństwa obejmuje podmioty wyznaczone przez ustawę, zobligowane do raportowania w zakresie cyberbezpieczeństwa i ochrony użytkowanych systemów i sieci przed zagrożeniami. System zaczyna się od pojedynczego użytkownika komputera, a kończy na instytucjonalnych rozwiązaniach zarządzanych w pierwszej kolejności przez ABW, MON i NASK. Jak powiedział sławny *hacker Kevin Mitcnick* „najsłabsze ogniwo systemu to człowiek". Jeśli nawet będziemy posiadać najlepsze zabezpieczenia, serwery, wydajne komputery, szczegółowe procedury, a pracownik „zawali sprawę", to cały system stanie się niewydolny. Stanie się tak np., jeśli pracownik

	podłączy „coś” niepożądanego do komputera i zainfekuje cały system, jeśli uruchomi niepożądaną funkcję. System cyberbezpieczeństwa dotyczy każdego użytkownika, każdego podmiotu, firmy, korporacji, podmiotów publicznych. Ale ostatecznie wszystko zaczyna się od człowieka i kończy na człowieku. To nie dzieje się tak, że maszyna popełnia przestępstwo czy błąd, zawsze – pośrednio lub bezpośrednio – dochodzi czynnik ludzki, zarówno, gdy mówimy o błahym incydencie, a kończąc na poważnych atakach, jak chociażby włamanie na stronę Komisji Nadzoru Finansowego. Wtedy „aktorzy” zainstalowali złośliwe oprogramowanie na serwerze KNF, pobierane następnie przez użytkowników witryny internetowej strony. Jako źródło ataku wskazuje się Koreę Północną lub Chiny. Każdy podmiot z poszczególnych dziedzinach życia pracuje na rzecz wspólnego cyberbezpieczeństwa: od inżyniera, który tworzy bezpieczny program antywirusowy, rodzica, socjologa, psychologa, nauczyciela, który naucza w szkole czy księdza, który nawet na katechezie może wspomnieć o świecie cyfrowym. Cyberprzestępczość jest wszędzie, zagrożenia są wszędzie, dotknąć mogą każdego, każdej sfery życia. I każdy ma coś do powiedzenia w obszarze zapobiegania tym zagrożeniom.
3) Co według Pana Prokuratora oznacza zagrożenie w dziedzinie cyberbezpieczeństwa? Na które z zagrożeń mogą być najbardziej narażeni najmłodsi użytkownicy sieci (Internetu)?	Nie wskażę tutaj jednego obszaru bo jest ich kilka, a najpoważniejsze cyberzagrożenia wiążą się z „czynnikiem ludzkim” czyli osobą znajdującą się po drugiej stronie ekranu. W przypadku *groomin'u*, czy *love scam*, dziecko chciałoby mieć kontakt dokładnie z kimś takim, kogo widzi na ekranie monitora, tak wyobraża sobie partnera do rozmów, nie dopuszcza możliwości, że po drugiej stronie może znajdować się ktoś zupełnie inny. Opowiem historię: kobieta poznaje żołnierza *Marines* z USA, wspaniałego mężczyznę, piszącego do niej wiersze. Rząd nagle wzywa żołnierza na misję i musi on wyjechać do Afganistanu. Tam znajduje walizkę pełną pieniędzy, chce z nią przyjechać do naszej bohaterki, do Krakowa, razem z nią mieszkać, spędzić resztę życia. Zaczyna się dalsza gra socjotechniczna. Na początku Marines potrzebuje pieniędzy żeby wydostać się z obszaru wojny, później na opłacenie cła za transportowane pieniądze i tak pojawiają się kolejne „potrzeby” i prośby kierowane do kobiety o następne transze środków. Ta kobieta była emerytowaną nauczycielką, wykształconą osobą, i zdawać by się mogło, że realnie oceni tą całą sytuację, jako oszustwo. Jednak dzieje się zupełnie inaczej i pomimo np. otrzymanej informacji w banku, iż konto na które zamierzała wysłać pieniądze jest kontem oflagowanym, czyli „niebezpiecznym”, kobieta decyduje się wykonać kolejny przelew. Wobec pokrzywdzonej wykorzystano zatem jedną z reguł manipulacji, świetnie opisanych przez słynnego psychologa *Cialdiniego*, tj. regułę słuszności: człowiek będący w kłopotach dotąd mami się nadzieją, że nie padł ofiarą oszustwa, dopóki nie straci wszystkich pieniędzy i brutalnie zderzymy się z prawdą. Niekiedy ludzie obawiają się sami przed sobą przyznać, że popełnili poważne błędy i dali się zwieść, jak dziecko. Zagrożenia dotyczące osób najmłodszych podzieliłbym na dwie grupy: związane z maszyną i człowiekiem. Pierwsze dotyczy sprzętu komputerowego użytkowanego przez nieletniego, np. instalacja trojana powoduje kradzież wrażliwych danych z komputera autoryzujących dostępu do konta czy aplikacji. W przypadku działania malware'a zdarzają się nawet mechaniczne uszkodzenia sprzętu np. podłączenie komputera do nielegalnej kopalni kryptowalut spowoduje, że laptop wolniej funkcjonuje, zawiesza się, a nawet całkowicie przestaje działać. Jednak najgroźniejsze są działania przestępcy ukierunkowane na psychikę młodego człowieka, jego integralność cielesną i poczucie bezpieczeństwa. Takie działania w zaawansowanym stadium mogą nawet zagrażać jego życiu i zdrowiu pokrzywdzonego. Niektóre „cyberzagrożenia” nie zawierają znamion przestępstwa, ale także mogą być niebezpieczne. Dotyczą ucieczki młodych ludzi do wir-

	tualnej rzeczywistości, jako alternatywy dla realnego świata. Sprowadza się to do „siedzenia w telefonie" i ograniczeniem kontaktów z osobami najbliższymi i rówieśnikami. Osoby takie częstokroć odseparowują się od innych, izolują od otoczenia, mają problem z samookreśleniem i prawidłową oceną własnej wartości. Podzielę się moim spostrzeżeniem: przeprowadzając „pogadanki" dla dzieci w szkole podstawowej, myślałem, że im starsze osoby, tym łatwiejsza oraz konkretniejsza wywiąże się dyskusja na temat cyberbezpieczeństwa. Ale okazało się, że z maluchami, będącymi w klasie I-III lepsza była komunikacja, niż z ich starszymi kolegami. Dzieci chętniej podnosiły rękę do odpowiedzi, rwały się do dyskusji. Na pytanie czy doświadczyły jakichś cyberprzestępstw, odpowiadały, iż mają świadomość np. kradzieży z kont bankowych. Osoby z klas IV-VIII były niekontaktowe, skupiały się na swoich telefonach, nie zgłaszały się, z oporem podejmowały jakąkolwiek dyskusję. Dlaczego tak to wyglądało, do końca nie wiem. Prowadzone są kampanie społeczne, a zapewne wielu rodziców także stara się propagować takie zachowania, aby ich pociechy nie spędzały całych godzin przed komputerem, nie zabierały ze sobą telefonu do szkoły. Z drugiej strony jednak wiele korporacji zmierza w kierunku metaverse, czyli sieci *3web*, do końca jeszcze niezdefiniowanej rzeczywistości składającej się ze stokenizowanych, cyfrowych dóbr i usług. Obecnie *2web* opiera się na komunikacji masowej na platformach społecznościowych ale fundamentami *3web* mają być: technologia *blockchain* i sztuczna inteligencja budująca wielowymiarowy świat stymulowany przez ludzkie neurony. Planuje się bezpośrednio skomunikować rzeczywistość wirtualną z korą mózgową tak aby zachodziła między nimi interakcja i jedno wtapiało się w drugie. Widać zatem paradoks: z jednej strony prowadzone są akcje na rzecz ograniczania przebywania ludzi w sieci, spędzania wolnego czasu poza *„cyber",* a de facto wszystko zmierza ku temu abyśmy przenieśli swoje życie do wirtualnego świata.
4) Które z zagrożeń w obszarze cyberbezpieczeństwa mogą oznaczać największe wyzwanie dla funkcjonowania państwa i jakie inne mogą powstać w przyszłości? W jaki sposób można zapobiegać zagrożeniom?	Nie chciałbym skupiać się tylko na hasłach znanych wszystkim z dyskusji społecznych, a bardziej skupić się na moich doświadczeniach zawodowych. Oczywistym jest, że nie ma nic za darmo i jeśli w jednym obszarze chcemy iść bardziej do przodu, to automatycznie ograniczymy się w jakimś innym segmencie rzeczywistości. Podam przykład anonimizacji. Z jednej strony dyskutuje są aby ograniczać anonimowość, do tego zmierzały np. przepisy nakazujące rejestrację kart SIM na zidentyfikowanego użytkownika. Z drugiej strony bezpieczeństwo dokumentów cyfrowych czy transfer danych informatycznych powinny się wiązać z szyfrowaniem, aby zapewnić ich bezpieczeństwo. Kolejna rzecz: ważny element dla cyberbezpieczeństwa oraz walki z wirtualną przestępczością stanowią pieniądze. Programy do analizy danych, nowoczesny sprzęt komputerowy, czy proces podnoszenia kompetencji funkcjonariuszy organów ścigania – to wszystko duże kosztuje i skądś na to trzeba znaleźć środki. Patrząc od strony policjanta czy prokuratora należy wiedzieć, jaką metodologię ścigania cyberprzestępców przyjąć oraz posługiwać się w procesie wykrywczym odpowiednimi narzędziami taktyki i techniki kryminalistycznej. Mówi się ponadto o konieczności edukacji społeczeństwa w dziedzinie cyberbezpieczeństwa, ale zauważam problem, że działania w tym obszarze spowszedniały ludziom i dlatego ich oddziaływanie jest słabe. Pomimo wielu akcji skierowanych do dzieci i dorosłych, które mówią i mówią o cyberbezpieczeństwie, to społeczeństwo się jakoś – rzekłbym – „uodporniło" na przyswajanie takiej wiedzy oraz jej stosowanie. Może dlatego, że czym więcej się o czymś mówi, to ludzie tym mniej zwracają na to uwagę. Ciekawa kwestia dotyczy np. haseł. Obecnie mam konto skrzynki mailowej, konto do komputera stacjonarnego w pracy, mam konto do innego komputera, na którym opracowuję informacje niejawne, mam konto w telefonie, konta do aplikacji bankowych, ale owych danych uwierzy-

	telniających jest zdecydowanie za dużo do zapamiętania. I chociaż głoszone są słuszne idee o konieczności posiadania odpowiednio zbudowanych haseł, to w rzeczywistości ludzie nie są w stanie kontrolować tych wszystkich kanałów uwierzytelnienia i poprzestają na najprostszych rozwiązaniach. Walka o cyberbezpieczeństwo nie jest prosta i często wiąże się także z brakiem wystarczającej wiedzy. Przykładowo, mamy telewizory podłączone do Internetu, ekspres do kawy lub *thermomix* działający w sieci i nie zdajemy sobie sprawy, że w gruncie rzeczy to są komputery tak samo, jak laptop czy telefon wyposażone w kamerkę lub głośnik. I chociaż kody producentów zabezpieczające wspomniane urządzenia są bardzo proste typu admin123, to nie zmieniamy ich zaraz po zakupie urządzenia. Proszę wskazać, ile osób ma świadomość konieczności zmiany takiego hasła i loginu? Podsumowując, kampanii dotyczących cyberbezpieczeństwa jest mnóstwo, ich postulaty są jak najbardziej słuszne, ale mam przeświadczenie, że skuteczność takich działań jest niewielka w porównaniu do istniejących zagrożeń. Ludzie nie mają siły, ochoty i czasu stosować najdalej idących zabezpieczeń dotyczących ich sprzętu i danych nawet wtedy, gdy są świadomi grożących niebezpieczeństw. I wcale za taki stan rzeczy nie winię tylko użytkowników internetu, ale po prostu sprostanie wszystkim wymogom cyberbezpieczeństwa okazuje się zbyt uciążliwe.
5) Jakie czynniki i działania państwa (kraju) mogą wpływać na budowanie świadomości zagrożeń oraz cyfrowych kompetencji w zakresie cyberbezpieczeństwa?	Prostego rozwiązania nie ma. Jesteśmy poniekąd w martwym punkcie. Wydaje się, że priorytety cyberbezpieczeństwa zostały zdefiniowane, dużo się o nich mówi, organizuje się kampanie społeczne, jak bezpiecznie poruszać się w sieci, mowa jest o odpowiedniej edukacji. Natomiast widać, że te wszystkie działania nie przynoszą do końca pożądanego skutku i ludzie nabierają się np. na proste oszustwa w internecie. Nasuwa się zatem pytanie, czy żyjąc w świecie, kiedy coraz intensywniej wkraczamy w cyberprzestrzeń, musimy pogodzić się z określonymi cyberzagrożeniami? A może powinniśmy dążyć nieustannie do coraz wyższego poziomu cyberbezpieczeństwa? To są rzeczywiście praktyczne pytania. Każdy powie, że druga odpowiedź jest właściwa. Ale może trzeba uznać, że mamy cyberbezpieczeństwo na takim poziomie, na jaki w tej chwili nas stać. Może trzeba powiedzieć, że poziom ten należy podnosić, mając jednocześnie świadomość, że radyklanie nie naprawimy wirtualnej rzeczywistości, a każde kolejne ograniczenia zmniejszają jednocześnie wolność w internecie. Twierdzenia o konieczności radykalnego podniesieniu poziomy cyberbezpieczeństwa, które nam stale towarzyszy, przy jednoczesnym przeświadczeniu, że jest bardzo źle na tym polu, są chyba przesadzone. Trzeba mieć świadomość, że wszystkim mankamentom nie będziemy w stanie sprostać i nie zlikwiduje się całkowicie zagrożeń. Należy zatem skupić się na najważniejszych kwestiach, związanych z ochroną dzieci w sieci, infrastruktury krytycznej przed atakami, a jednocześnie poprawiać bezpieczeństwo w innych obszarach na tyle, na ile jest to możliwe. Oprócz edukacji, wychowania w rodzinie, należy zastanowić się, co może zrobić każdy z nas indywidualnie, a ile prawnych i technicznych zabezpieczeń powinno wdrażyć państwo. Część wiedzy i nawyków możemy przyswoić sobie sami, aczkolwiek niektóre rozwiązania, np. blokada stron internetowych z nielegalnymi grami hazardowymi, leżą po stronie organów publicznych i powinny być forsowane odgórnie. I kolejne pytanie: jak daleko mogą sięgać ograniczenia i restrykcje, gdyż działania urzędników ograniczają niekiedy prywatność, swobodę wyboru. Trzeba dobrze wyważyć racje tak, aby kosztem jednego projektu nie zniszczyć sfery prywatności i wolności uczestników cyberprzestrzeni.
6) Czy istnieje potrzeba zmiany sposobu edukacji użytkowników sieci? Czy widzi Pan wpływ pojedynczego użytkownika na szerszą	Bez wątpienia edukacja jest ważna, ale jeszcze raz podkreślam, nie należy wszystkiego negować, to znaczy mówić, a nawet straszyć, że nasza aktywność w cyberprzestrzeni niesie same zagrożenia. Posłużę się przykładem. Moja córka mająca roczek samodzielnie surfuje już po sieci, przewija strony i robi to bardzo sprawnie, jak na swój wiek. Pojawia się

grupę społeczeństwa, na cały system cyberbezpieczeństwa?	pytanie, czy to właściwe podejście, że tak małe dziecko bawi się treściami w sieci tj. ogląda bajki, słucha piosenek? „Klasyczna" odpowiedź będzie brzmiała, że nie powinno się tak młodej osobie udostępniać do zabawy telefonu komórkowego. Z drugiej strony nie zmieni się świata i nie sposób wychowywać dzieci w oderwaniu od nowych technologii. Znam bowiem model wychowania najmłodszych, gdzie dzieciom zabrania się dostępu do internetu oferując tylko i wyłącznie „tradycyjny" sposób spędzania wolnego czasu. Rodzi się pytanie, czy takie dziecko, kiedy dorośnie, zacznie rywalizować ze swoimi rówieśnikami o pozycję w grupie, czy jego rozwój nie będzie opóźniony technologicznie? Czy nie będzie odczuwać dyskomfortu z tego powodu. Stąd jestem daleki od podejścia typu: zakazujemy synowi czy córce użytkowania telefonu komórkowego do któregoś roku życia, gdyż może to wpłynąć na nieprawidłowy rozwój dziecka. Należy wyrabiać u najmłodszych dobre praktyki w zakresie cyberbezpieczeństwa, ale nie sposób „zawróci kijem rzeki", a więc konkretne zmiany technologiczne zaszły w społeczeństwie i siłą rzeczy każdy, od najmłodszego do osób dorosłych korzysta z tych zmian. Edukacja młodzieży nie może polegać na tym, że jesteśmy ślepi na pewne trendy i zmieniający się świat ciągle tkwiąc w starych przyzwyczajeniach i stereotypach. Cyberprzestrzeń zagościła na stałe w naszym życiu i nawet, jeśli istnieją różne zagrożenia z nią związane, to całkowicie ich nie wyeliminujemy. Oprócz tego, co złe, należy pokazywać także „wartość dodaną" zmian, edukować, a nie straszyć.
7) Proszę wskazać najprostsze możliwości ochrony pojedynczego użytkownika, co należy czynić, żeby być bardziej bezpiecznym w sieci?	Możliwości owszem są i ponownie nazwę te działania: wzmacnianie wiedzy z zakresu cyberbezpieczeństwa, promowanie przydatnych narzędzi informatycznych, odpowiednie wychowanie w domu, szkole, bezpieczne zachowania w miejscu pracy. Ale do zagadnienia cyberbezpieczeństwa podejść należy z „chłodną głową" i ułudą jest, że jesteśmy w stanie całkowicie zlikwidować niebezpieczeństwa płynące z wirtualnego świata. Powinniśmy zatem wyznaczyć sobie pewne obszary, gdzie owe zagrożenia są najpoważniejsze, i tam działania muszą być najintensywniejsze, stanowić priorytety. Warto zastanowić się nad skutecznością działań. Mam wrażenie, że ta cała masa programów oraz kampanii mówiących o bezpieczeństwie w sieci jest nieefektywna i ludziom po prostu przejadł się ten sam sposób przekazu. Zachodzi konieczność stworzenia nowych kanałów komunikacyjnych i strategii marketingowych dotyczących cyberbezpieczeństwa. To pole do działania dla prawników, socjologów, psychologów, ludzi od marketingu, jak stworzyć nowe narzędzia przekazu, które się nie znudziły społeczeństwu swoją powtarzalnością, bo dzisiaj wiele z nich faktycznie nie robi żadnego wrażenia na odbiorcach komunikatów. Podejście do tego problemu powinno być eklektyczne i przemyślane. Ja, wykonując zawód prokuratora, działam na etapie, kiedy coś się wydarzyło, wykonuję bardzo ważną pracę, ale rzec można wtórną, sięgam do przeszłości. Pierwsza linia obrony obejmuje natomiast politykę informacyjną.
8) Czy może przedstawić Pan najczęściej występujące cyberprzestępstwa? Jakie wyzwania, trudności istnieją w wykrywaniu cyberprzestępstw?	W grudniu 2023 roku ukazała się moja monografia dotycząca kwalifikacji prawnej i opisu znamion przestępstw teleinformatycznych. Zbierając materiał badawczy zapoznałem się w krakowskich sądach z dziesiątkami postępowań karnych dotyczących takich przestępstw. Okazało się, że wielokrotnie obraz cyberprzestępczości jest o wiele bardziej banalny, niż nam się wydaje. Chodzi o podglądnięcie haseł dostępu do kont na platformach społecznościowych lub skrzynek mailowych i nieuprawnione zapoznanie się z informacjami, podsłuchiwanie kogoś za pomocą dyktafonu lub śledzenie go nadajnikiem *GPS*, czy bezprawny przelew środków pieniężnych z rachunku bankowego osoby pokrzywdzonej. Oczywiście zdarzają się cyberprzestępstwa o bardzo specyficznym i zaawansowanym modus operandi jak chociażby ataki ransomware lub wykorzystywanie trojanów lub keyloggerów do szpiegostwa komputerowego. Niemniej, tej „drobnicy" jest najwięcej. Prowadzenie spraw, szczególnie

	o poważne cyberprzestępstwa, to żmudna praca śledczych, trudny proces związany z gromadzeniem i analizą wielu dowodów, korzystanie z pomocy biegłych z zakresu informatyki śledczej i realizacją międzynarodowej pomocy prawnej. Finalnie jednak wielu sprawców najpoważniejszych przestępstw zostaje pociągniętych do odpowiedzialności karnej. Zmieniają się przy tym paradygmaty cyberprzestępczości i dzisiaj dużym sukcesem jest np. „aresztowanie" serwera służącego przestępcom do popełniania czynów zabronionych, który stanowi dla organów ścigania kopalnię „cyfrowej" wiedzy o działalności zorganizowanych grup przestępczych i osobach korzystających z ich usług np. kupujących narkotyki w *darknecie*.
9) Jak oceni Pan przydatność tzw. śladu cyfrowego w czynnościach operacyjnych jak i rozpoznawczych w obszarze cyberprzestępstw?	Ponieważ działalność przestępców realizowana jest w znacznym stopniu w cyberprzestrzeni, to pozostawiane przez nich ślady cyfrowe mają decydujące znaczenie w procesie wykrywczym. Za ich pomocą ustala się m.in. to, co wydarzyło się w badanym systemie informatycznym, jakie inne urządzenia łączyły się z komputerem, skąd pochodził ruch sieciowy, jak wyglądały transfery kryptowalutowe, co zarejestrowały kamery monitoringu, do jakiej stacji przekaźnikowej logował się telefon komórkowy. Prokurator powinien wiedzieć do jakich podmiotów zwrócić się o wydanie śladów cyfrowych oraz jakie procedury obowiązują w zakresie zabezpieczania takich śladów. Sam proces „przekuwania" śladów cyfrowych w dowody także ma swoją specyfikę. Podsumowując: bez badania śladów cyfrowych walka z cyberprzestępczością nie byłaby możliwa. Niestety, operowanie takimi śladami, zabezpieczanie ich pod względem procesowym i kryminalistycznym, wymaga doświadczenia i wiedzy. Niestety, do tej pory zdarzają się sytuacje, kiedy organ procesowy zabezpiecza stronę internetową w postaci wydrukowanej kartki papieru bez dokonanie jej oględzin i zabezpieczenia materiału cyfrowego. Dlatego sędziowie, prokuratorzy i funkcjonariusze służb powinni kierować się najlepszymi standardami metodycznymi w pracy z cyfrowymi śladami.
10) Czy można wykorzystać ślad cyfrowy do zabezpieczenia się przed cyfrowymi zagrożeniami? W jaki sposób można chronić swój ślad cyfrowy?	Wcześniej powiedziałem już, że przestępcy pozostawiają w wirtualnym świecie ślady cyfrowe związane z nielegalnymi działaniami. Ale ślady takie pozostawiają także inni użytkownicy internetu i szerzej – komputerów. Powinniśmy zatem szanować własne cyberbezpieczeństwo i stosować swoiste BHP w cyberprzestrzeni. Dbajmy o poufność naszych danych osobowych, nie ujawniajmy zbyt wiele informacji o naszej prywatności, odwiedzajmy bezpieczne strony internetowe, nie nawiązujmy bliższych relacji z nieznanymi osobami itd. To wszystko sprowadza się do ochrony naszego „śladu cyfrowego" w sieci.

Źródło: opracowanie własne wyników badań

Wywiady eksperckie stanowią jedną z najbardziej kluczowych części pracy. Dostarczyły wiedzy niezbędnej do dalszej analizy obszaru badawczego. Zdaniem ekspertów największym zagrożeniem może być człowiek, który będąc nieświadomym częstokroć publikuje zbyt wiele informacji o sobie, co może stanowić podstawę do stania się obiektem zainteresowania cyberprzestępców. Oczywistym jest, że charakter i nasilenie cyberzagrożeń zależeć będzie od wieku użytkownika sieci i w taki sposób może ewaluować, zgodnie z tym, iż dziecko prawdopodobnie będzie mniej podatne na ataki o zabarwieniu finansowym w porównaniu do osoby starszej. Rozwój technologii cyfrowych, dostęp do smartfonów od najmłodszych lat sprawia, że coraz poważniejszym zagrożeniem są treści tzw. *CSAM* (jak już wspomniano wcześniej, *Child Sexual Abuse-*

ment Material). Są to treści pornograficzne z udziałem dzieci, które często same nieświadomie takie treści tworzą. Następnie zostają ofiarami grup przestępczych, pedofilów wyłudzających od nich zdjęcia czy filmiki wideo.

Podmioty i instytucje właściwe w zakresie cyberbezpieczeństwa realizują szereg czynności i przedsięwzięć, których celem jest budowanie świadomości i kompetencji cyfrowych. Są to konferencje, które poprzedza się swoistym przeglądem i aktualizuje agendę o najnowsze doniesienia i przykłady w ramach doświadczeń ekspertów. Organizowane są światowe dni społeczeństwa informacyjnego, gdzie uczestnicy wielu profesji (media, policja, nauczyciele) przybliżają zagadnienia dotyczące tego w jaki sposób rozmawiać z dziećmi o bezpiecznym zachowaniu w Internecie, jak można zapobiegać pewnym zdarzeniom. Źródło wiedzy stanowią także artykuły czy netykiety. Inny ekspert zwrócił uwagę na szkolenie kadr, specjalistów, profesjonalistów zajmujących priorytetowe funkcje w państwie (np. politycy). Współpraca z uczelniami i szkolenie kadr dydaktycznych stanowi punkt wyjścia do lepszego zrozumienia specyfiki tematyki cyberbezpieczeństwa. Do przedmiotowego zadania wpisuje się także współpracę z *NGO,* w obszarze których szkoleniom podlegają uczniowie, nauczyciele, rodzice czy osoby starsze. Dostrzega się znaczenie lokalnych grup, samorządu terytorialnego w zakresie rozwijania wiedzy społeczeństwa poprzez „wyjście bezpośrednio do ludzi".

Jak najbardziej istnieje potrzeba zmiany edukacji uczniów czy nauczycieli. Począwszy od najmłodszych, istotna jest rola rodziców w zapewnieniu ograniczonego czasu korzystania z sieci oraz jego zasobów. Zdarza się tak, że to dzieci wiedzą więcej od rodziców, stąd należy również edukować właśnie wychowawców młodego pokolenia. Jest to proces, którego nie da się przeprowadzić jednokrotnie i o tym zapomnieć, zakończyć. Działania muszą mieć charakter ciągły, zaś profilaktyka odgrywa najbardziej kluczową rolę. Kultura w sieci to obszar jaki musi zostać dotknięty na lekcjach w szkole. Posługując się przykładem, kolega w klasie zapomniał wylogować się ze swojego konta, wówczas drugi po nim powinien niezwłocznie to wykonać, samodzielnie, bez nakazów pedagogów, z własnej potrzeby i świadomości. Zdaniem kolejnego eksperta, ponownie należy skupić się na kadrach, które prowadzą szkolenie. Muszą to być specjaliści odpowiedni do przekazania najbardziej potrzebnej wiedzy. W szkole, budować świadomość bezpiecznego zachowania w sieci mogą nie tylko nauczyciele informatyki, ale także innych przedmiotów. Wręcz jest to sugerowane. Potencjał nauczycieli nietechnicznych jest zauważany.

Warta uwagi w kontekście prewencji cyberzagrożeniom jest zasada *need to share*, traktująca o dzieleniu się zdobytą wiedzą z innymi, wcześniej obowiązująca *need to know*- oznaczała dostęp do danych dla węższego grona odbiorców. Szczególnie istotne jest to w zakresie przyszłych przewidywań z jakiego kierunku może np. nastąpić kolejny cyberatak i jakie podatności wykorzysta.

Skupiając się na pojedynczym użytkowniku sieci, warto pamiętać o zasadach tzw. higieny cyfrowej. Powinno się o tym wspominać zwłaszcza młodemu pokoleniu, które w sieci jest de facto całą dobę. Wieloskładnikowe uwierzytelnienie, czyli potwierdzenie logowania się do danej witryny poprzez użycie np. wiadomości sms.

Jednostka (człowiek) pełni w systemie cyberbezpieczeństwa szczególną rolę. Można to porównać do głosowania, jeden głos nie stanowi dużego znaczenia, jednak sumując poszczególne – tworzy się już pewna zbiorowość, która może wnosić określoną wartość. Tak więc w procesie budowania świadomości i kompetencji cyfrowych nie wolno zapominać o tym najmłodszym pokoleniu kreujące przyszłość. Potrzeby budowania świadomości wszędzie są takie same, niezależne od tego czy jest to wieś czy miasto.

Podstawę realizacji zadań na rzecz budowania cyberbezpieczeństwa stanowi wspomniana ustawa o KSC, według której główne trzy *CSIRTy* realizują określone zadania. Podział obowiązków jest klarowny i podmioty te działają sprawnie. Dodatkowo wsparciem są tzw. *CSIRT*y sektorowe, których funkcja jest również nieoceniona. Kluczowe są i pozostaną niezmienne finanse i właściwy budżet. Niezbędni są wyspecjalizowani eksperci i ich umiejętności w wymianie doświadczeń oraz wiedzy pomiędzy poszczególnymi podmiotami. Im więcej jest *CSIRTów* sektorowych tym lepiej z uwagi na częstszą i bardziej precyzyjną wymianę informacji priorytetowych ze względu na zapobieganie cyberzagrożeniom. Z pewnością w ramach implementacji założeń *Dyrektywy NIS 2* system zostanie poddany modyfikacjom, zgodnie z którymi powstanie więcej więcej komórek stanowiących wsparcie całego systemu cyberbezpieczeństwa.

6.2. Badanie sondażowe

W obszarze badań ankietowych, wstępne założenie było następujące: zasięg badań: 16 województw - Polska, charakterystyka próby: uczniowie i nauczyciele szkół podstawowych, okres badań: październik 2022 - grudzień 2022.

Do kuratorów oświaty 16 województw wysłano uwierzytelnioną prośbę o przekazanie ankiet do podległych szkół. Siedmiu z nich odmówiło, twierdząc, iż decyzja o przeprowadzeniu badań naukowych w szkołach nie leży w kompetencji kuratora, w związku z tym nie wyrazili zgody na to, aby przekazać dalej arkusze ankiet, inni natomiast zachęcali do skorzystania z internetowej, rządowej przeglądarki szkół podstawowych. Sześciu kuratorów nie odpowiedziało na zapytanie, pomimo niejednokrotnych kontaktów telefonicznych z sekretariatem placówki.

Finalnie, zgromadzono wyniki z trzech województw, z pozostałych nie udało się uzyskać odpowiedzi, co obrazuje poniższa tabela. W badaniu udział wzięło łącznie ponad 1500 nauczycieli oraz ponad 2500 uczniów. W związku z powyższym i innymi czynnikami (czas, przestrzeń), zrealizowanie badania w ramach dużej, ogólnopolskiej próby (liczebność ankietowanych) nie było możliwe. Pomimo decyzji zawężenia badań ankietowych do trzech województw, w których uzyskano ankiety, próba wyodrębniona drogą losową jest nadal reprezentatywna i wiarygodna.

Pierwszorzędnie zostaną przedstawione rezultaty wynikające z kwestionariusza ankiety w zakresie cyberbezpieczeństwa – dla nauczycieli szkół podstawowych, a następnie dla uczniów szkół podstawowych. Ze względów technicznych i celem zachowania przejrzystości wykresów zostały one umieszczone częściowo na oddzielnych stronach.

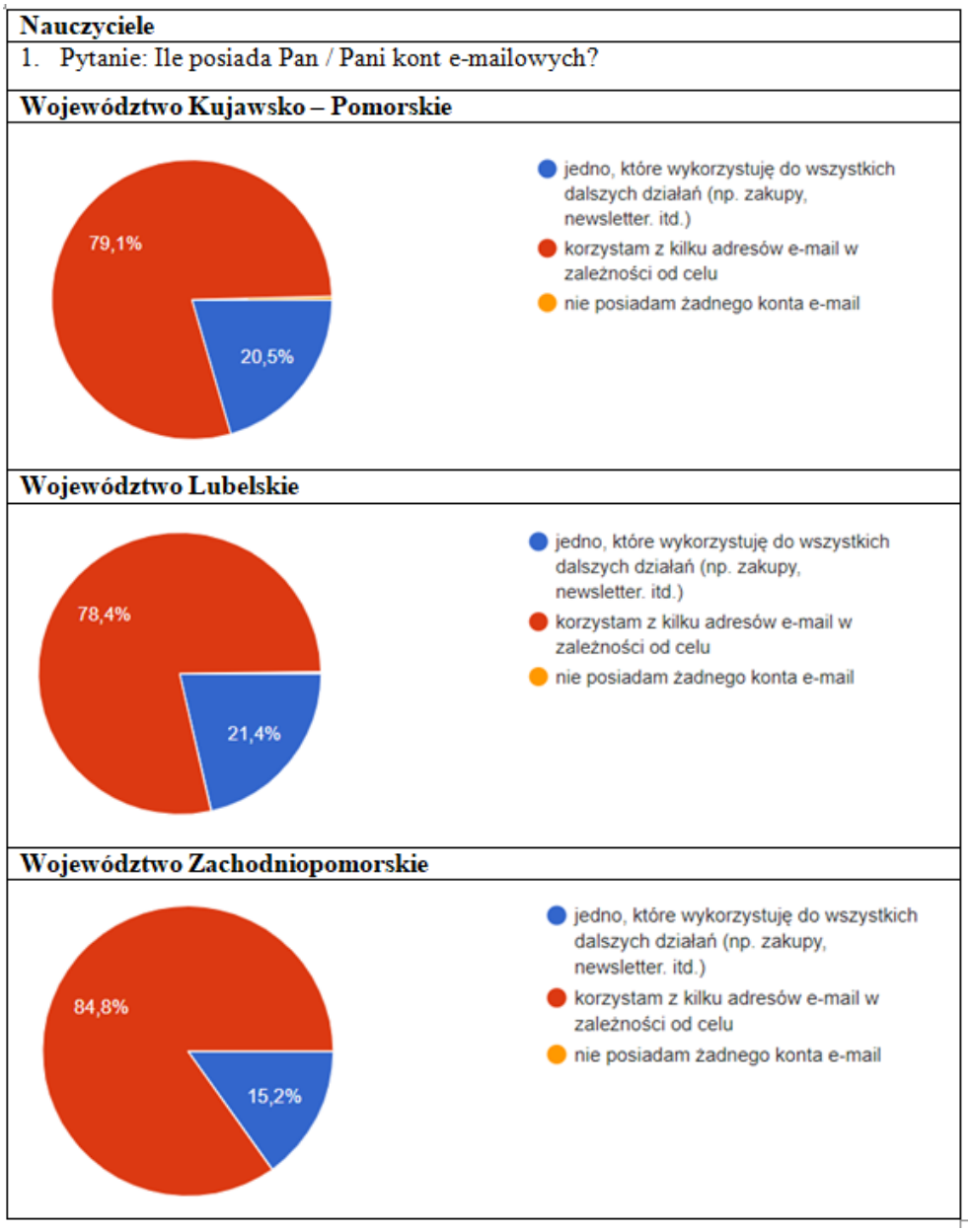
Tab. 6.6

Chęć zaangażowania kuratorów w badanie ankietowe w skali kraju

Lp.	Województwo	Decyzja kuratora o podjęciu badań	Ilość respondentów - nauczyciele	Ilość respondentów - uczniowie
1.	Dolnośląskie	Odmowa	-	-
2.	Podlaskie	Odmowa	-	-
3.	Śląskie	Odmowa	-	-
4.	Warmińsko - Mazurskie	Odmowa	-	-
5.	Wielkopolskie	Odmowa	-	-
6.	Kujawsko - Pomorskie	Zgoda	268	558
7.	Lubelskie	Zgoda	986	1585
8.	Zachodniopomorskie	Zgoda	264	539
9.	Lubuskie	Brak odpowiedzi	-	-
10.	Łódzkie	Brak odpowiedzi	-	-
11.	Małopolskie	Odmowa	-	-
12.	Podkarpackie	Odmowa	-	-
13.	Pomorskie	Brak odpowiedzi	-	-
14.	Mazowieckie	Brak odpowiedzi	-	-
15.	Opolskie	Brak odpowiedzi	-	-
16.	Świętokrzyskie	Brak odpowiedzi	-	-

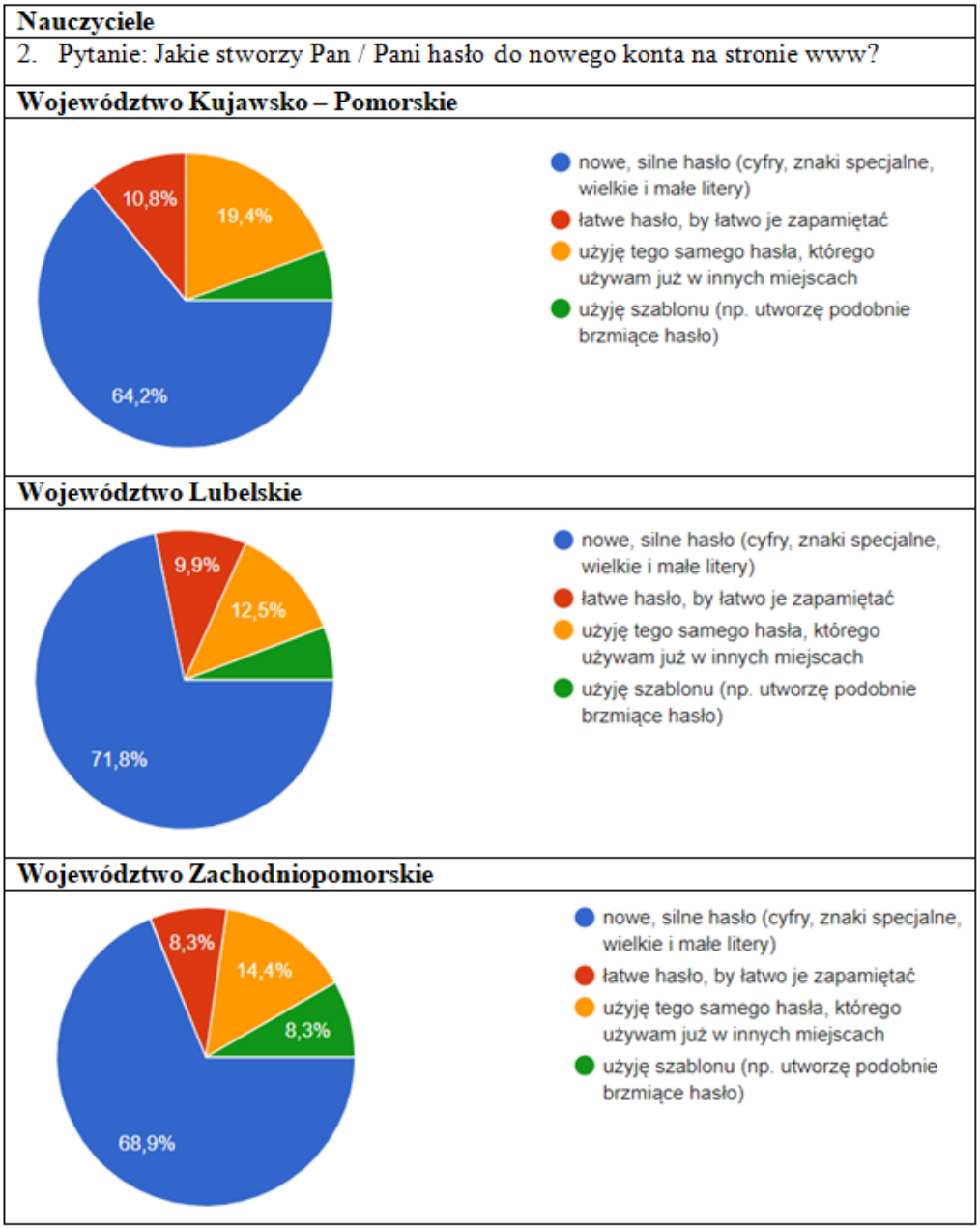
Źródło: opracowanie własne wyników badań

Zdecydowana większość nauczycieli korzysta z kilka adresów e-mail w zależności od celu (wartość oscyluje w granicach 80%), najbardziej świadomi w tym obszarze są przedstawiciele woj. Zachodniopomorskiego. Ponad 21% badanych w woj. Lubelskim dysponuje jedynie jednym kontem e-mail, które wykorzystuje do wszystkich działań w sieci. Powstaje pytanie, czy posiadanie jednego konta jest wystarczające? Informacje zaprezentowano na poniższym wykresie (6.1.).



Wykres 6.1. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- posiadanie kont e-mailowych (źródło: opracowanie własne)

Wyniki w trzech województwach są zbliżone. Nauczyciele woj. Lubelskiego dominują w kwestii tworzenia silnego hasła. Niepokojącym stanowi jednak fakt, iż blisko 1/5 badanych w woj. Kujawsko-Pomorskim używa jednego hasła w kilku miejscach. W sytuacji ataku hackerskiego (wyłudzenia hasła etc.), wszystkie portale/ aplikacje użytkownika mogą stać się zagrożone w tym samym momencie.



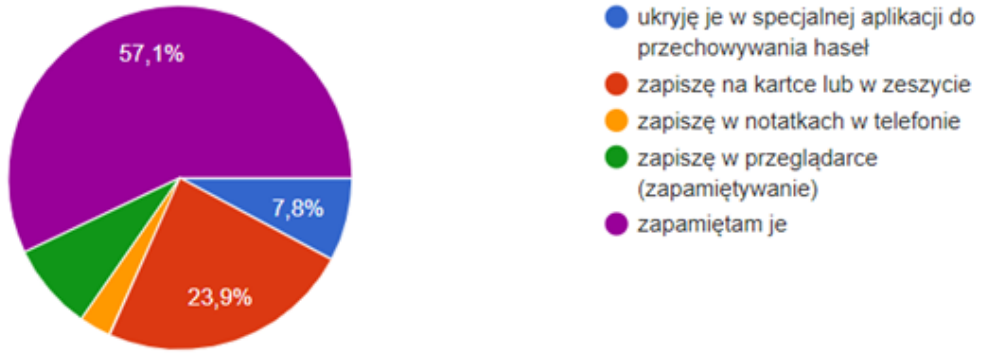
Wykres 6.2. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- tworzenie nowego silnego hasła (źródło: opracowanie własne)

Wśród przedstawionych sposobów przechowywania hasła respondenci w trzech województwach wykazali, że najczęściej hasła są przez nich po prostu zapamiętywane (blisko 60% badanych w każdym województwie). W woj. Lubelskim 29,9% ankietowanych wskazało, że zapisuje hasło na kartce, podobna ilość badanych odpowiedziała tak samo w pozostałych województwach, w woj. Zachodniopomorskim 22%, a w woj. Kujawsko - Pomorskim 23,9%. Pomimo rosnącej popularności specjalnych aplikacji do przechowywania haseł zaledwie 8,7% nauczycieli z woj. Zachodniopomorskiego z nich korzysta. Zbliżone są wyniki z pozostałych województw (Lubelskie 6%, Kujawsko - Pomorskie 7,8%). Pozostałe metody przechowywania haseł tj. zapisanie w notatkach w telefonie oraz zapisanie w przeglądarce zdobyły niewielki odsetek głosów respondentów. Wyniki wskazują, że pomimo ciągłego rozwoju aplikacji zabezpieczających nasze hasła czy też telefony i komputery, badani nauczyciele nadal nie darzą ich dostatecznym zaufaniem i wybierają metody tradycyjne takie jak zwyczajne zapamiętanie hasła lub zapisanie go w zeszycie.

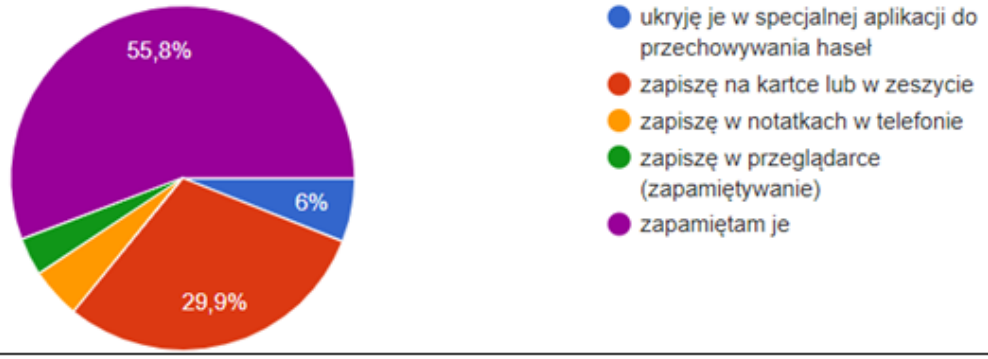
Nauczyciele

3. Pytanie: Jak zapamięta Pan / Pani nowo utworzone hasło?

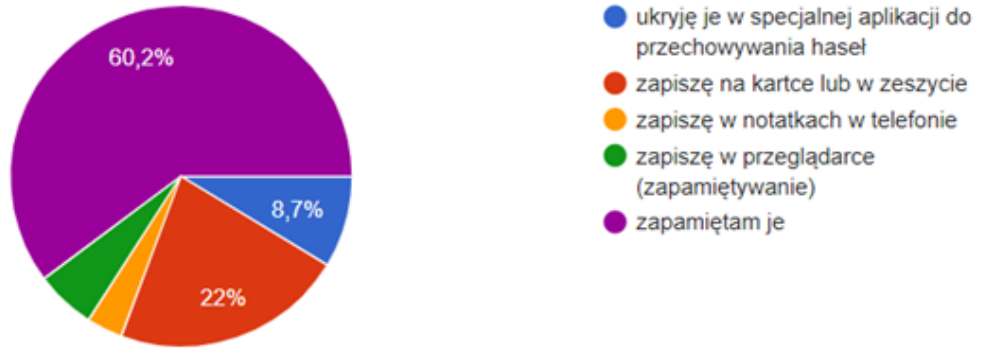
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

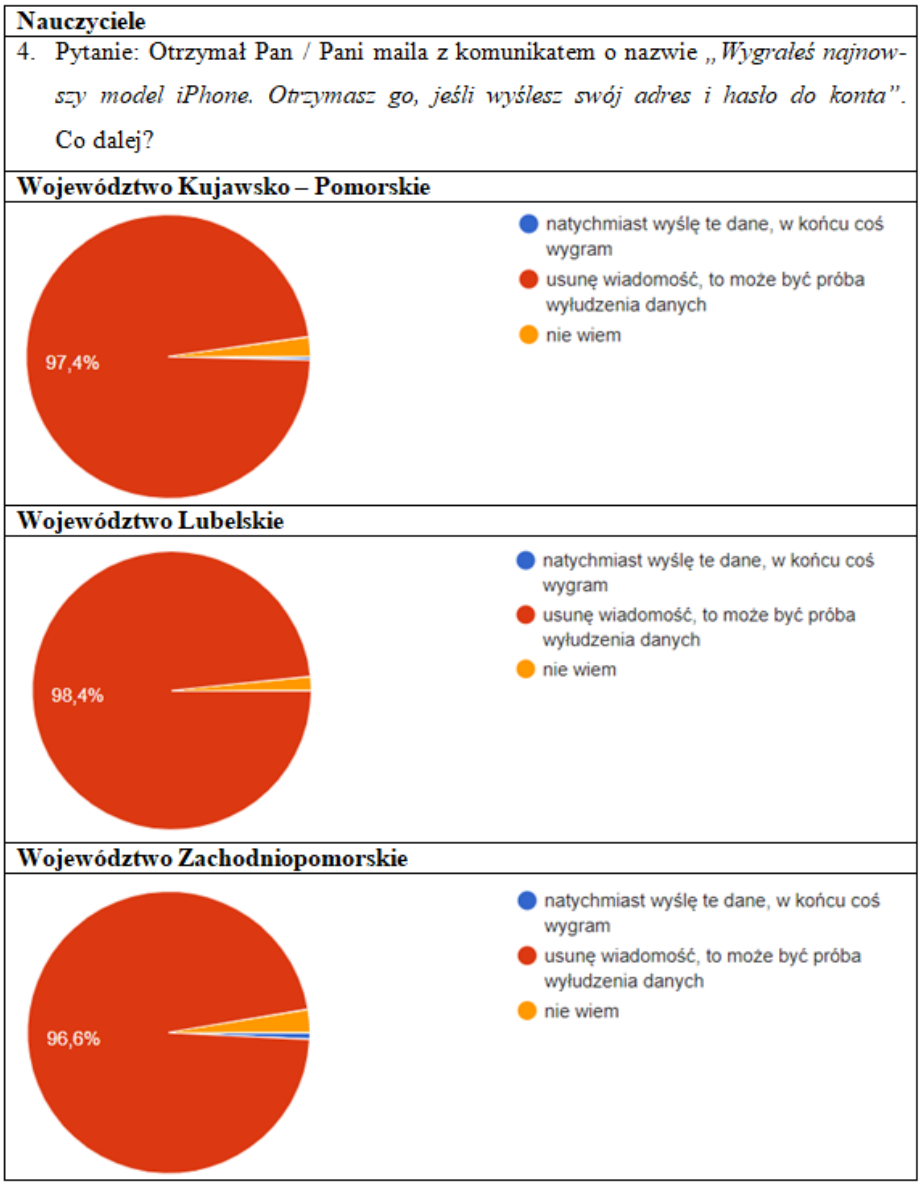


Województwo Zachodniopomorskie



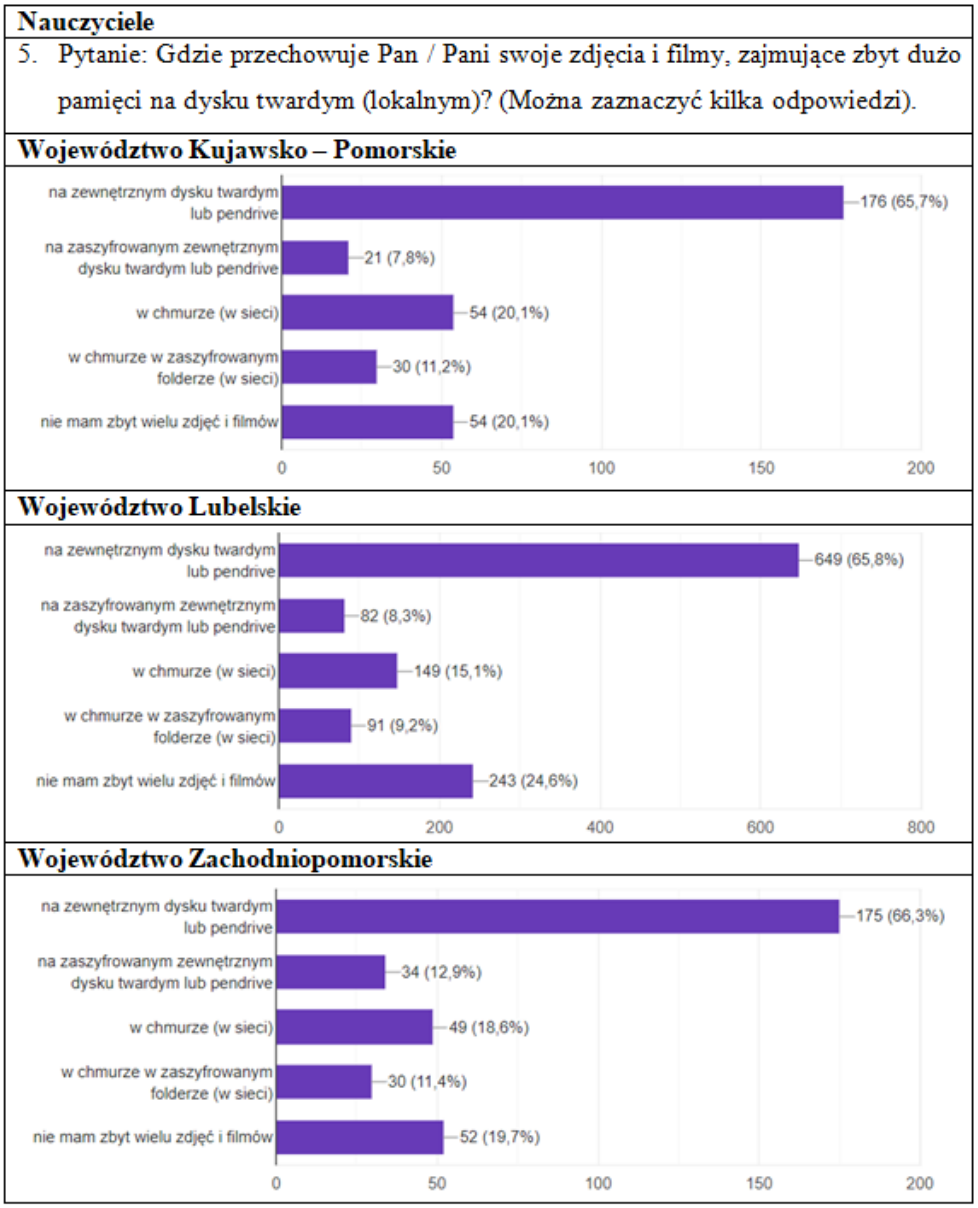
Wykres 6.3. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- zapamiętanie nowego hasła (źródło: opracowanie własne)

Respondenci zostali zapytani o postępowanie w przypadku otrzymania nietypowej wiadomości informującej o wygranej. Odpowiadali zgodnie we wszystkich badanych województwach, w tym w woj. Lubelskim, aż 98,4% wskazało, że usunie taką wiadomość. W pozostałych województwach wyniki są podobne. Inne odpowiedzi uzyskały tylko kilka procent głosów. Taki rozkład wyników może świadczyć o wysokiej świadomości badanych na temat potencjalnych zagrożeń jakie wiążą się z udostępnieniem swoich danych.



Wykres 6.4. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- reakcja na otrzymany komunikat (źródło: opracowanie własne)

Największą grupę badanych stanowią nauczyciele przechowujący swoje zdjęcia i filmy na zewnętrznych nośnikach danych (około 65%). Kolejnym powszechnym miejscem przechowywania dużych plików według nauczycieli jest chmura w sieci. Próbę dokładniejszego zabezpieczenia swoich plików poprzez szyfrowanie dysku zewnętrznego lub chmury podjęło ok 10% badanych na każdą z metod. Pozostali ankietowani nie wykazują konieczności wykorzystywania dodatkowych miejsc przechowywania swoich plików. Można zatem zauważyć, że nadal największą popularnością cieszą się metody tradycyjne niepowiązane z siecią internetową.



Wykres 6.5. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- przechowywanie danych (źródło: opracowanie własne)

Ankietowani we wszystkich trzech województwach (około 40% w każdym) w większości wykonują kopie zapasowe, jednak nie realizują tego regularnie. Należy zauważyć, że prawie jedna piąta respondentów w danym województwie dopiero planuje stworzenie kopii zapasowej, chociaż wcześniej tego nie robiła. Znaczny odsetek badanych wykonuje archiwizowanie tylko najważniejszych danych w woj. Kujawsko – Pomorskim 23,5%, Lubelskim 28,6%, a w Zachodniopomorskim aż 27,3%. Na uwagę zasługuje również fakt, jak niewielki odsetek nauczycieli wykonuje kopie zapasowe wszystkich danych. Niestety około 8% badanych uważa, że tworzenie kopii zapasowej za niepotrzebne. Zatem większość badanych zdaje sobie sprawę z konieczności tworzenia kopii zapasowej własnych danych. Jednak występują pewne różnice w podejściu do tego zagadnienia m.in. w zakresie regularności oraz ilości kopiowanych danych, co obrazuje poniższy wykres 6.6.

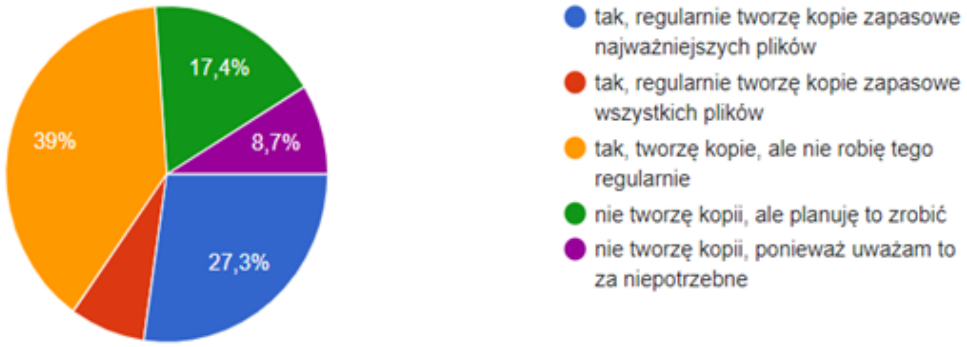
Nauczyciele

6. Pytanie: Czy wykonuje Pan / Pani kopie swoich plików (na wypadek utraty danych)?

Województwo Kujawsko – Pomorskie

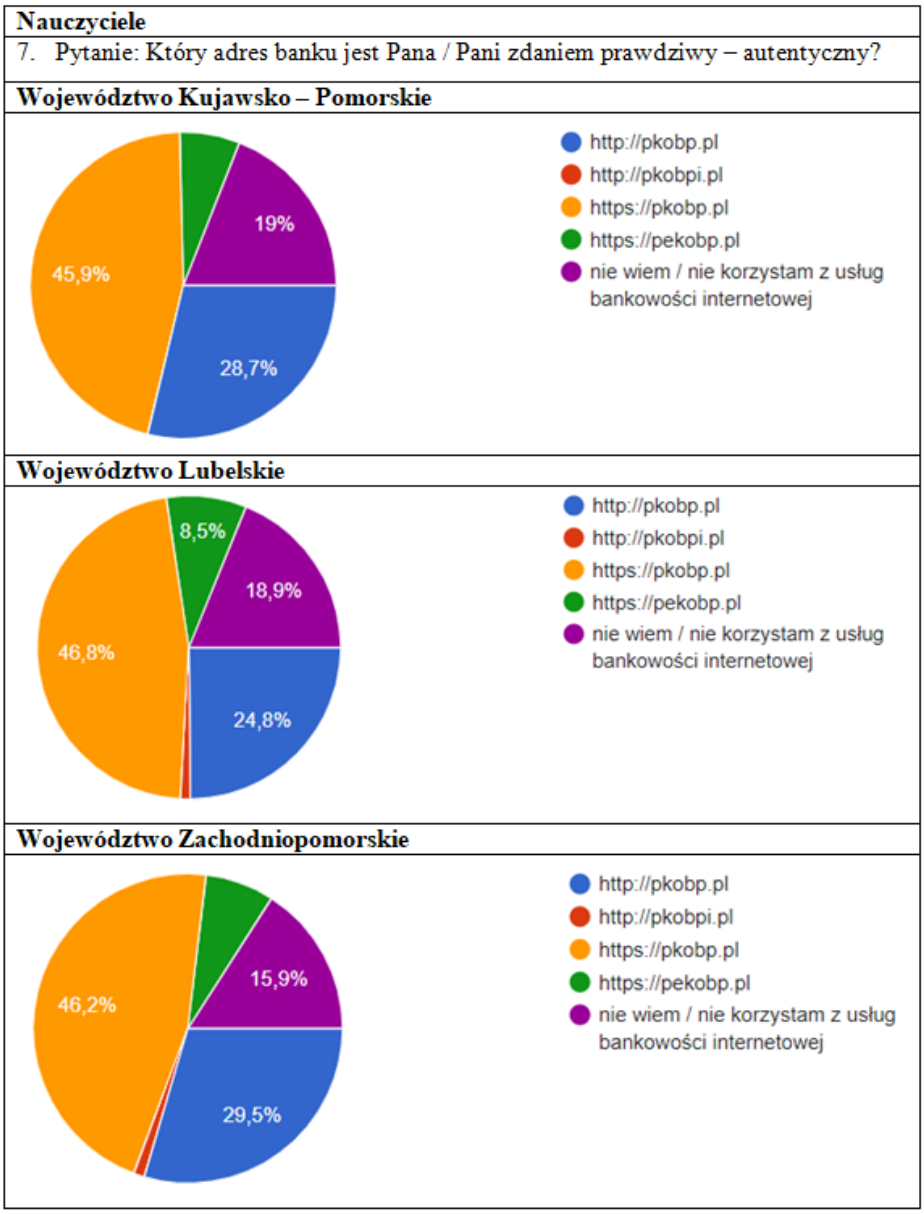
Województwo Lubelskie

Województwo Zachodniopomorskie



Wykres 6.6. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wykonywanie kopii plików (źródło: opracowanie własne)

W pytaniu numer siedem, ankietowani mieli wskazać ich zdaniem autentyczny adres strony internetowej popularnego banku. Udało się to tylko około 46 % badanych z każdego województwa. Aż 19% badanych z woj. Kujawsko – Pomorskiego, 18,9% z woj. Lubelskiego oraz 15,9% z woj. Zachodniopomorskiego nie było w stanie określić, który adres jest poprawny lub nie korzysta z bankowości internetowej. Pozostali respondenci nie potrafili wskazać prawidłowego zapisu adresu strony internetowej banku. W związku z tym można sądzić, że te osoby mogłyby się stać ofiarami potencjalnego ataku na ich bankowość internetową.



Wykres 6.7. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wskazanie prawdziwego adresu banku (źródło: opracowanie własne)

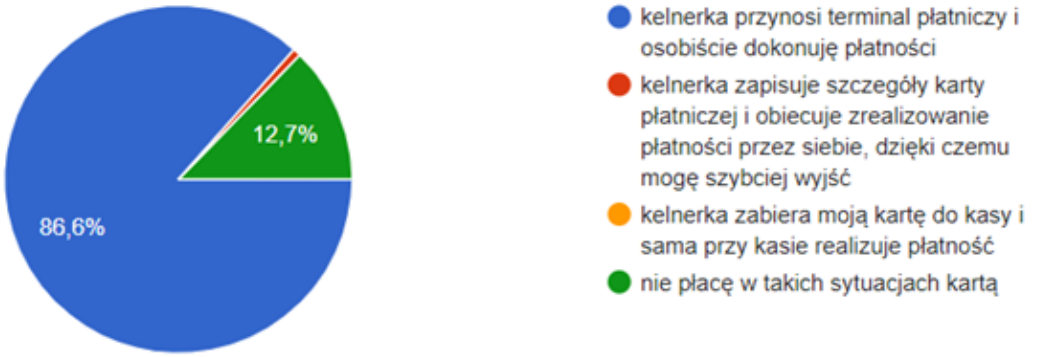
Następnie badani nauczyciele zostali zapytani o swoje postępowanie w przypadku płatności kartą płatniczą, mieli do wyboru cztery możliwości. W województwie Kujawsko- Pomorskim 86,6% badanych wskazało, że dokonuje płatności osobiście po tym jak kelnerka przyniesie terminal płatniczy. Na płacenie kartą nie zdecydowało się 12,7% badanych. Zaledwie 0,7% nauczycieli udostępniłoby kelnerce dane swojej karty płatniczej. Podobne wyniki otrzymano z woj. Lubelskiego. W większości badani wskazali na dokonanie płatności osobiście (79,6%), a 20,2% z nich wybrałoby inną formę płatności. W trzecim badanym województwie wyniki również były zbliżone do pozostałych. Aż 86,7% ankietowanych w przedstawionej sytuacji zapłaci osobiście, a 12,5 % nie wykorzysta do płatności karty.

W woj. Zachodniopomorskim niewielki odsetek badanych (0,8%) przekazałby swoją kartę kelnerce, aby ta dokonała płatności. Można zatem sądzić, że badani posiadają wysoki poziom świadomości na temat zagrożeń jakie niesie ze sobą udostępnienie danych kart płatniczej innym osobom. Informacje zawarto na wykresie 6.8.

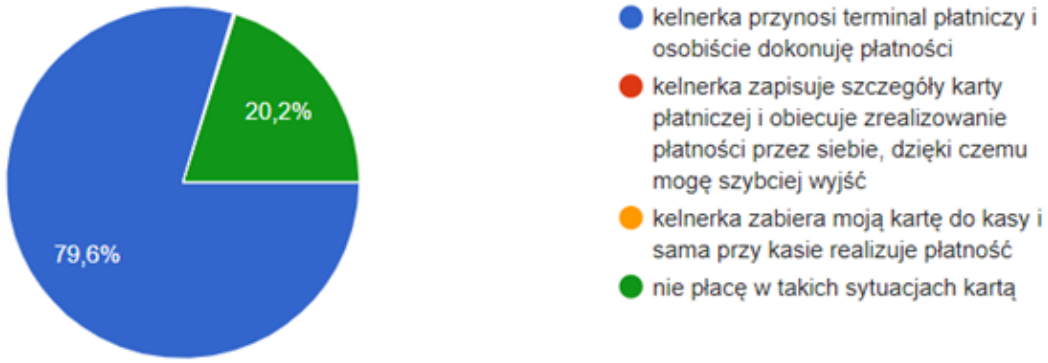
Nauczyciele

8. Pytanie: Którą opcję wybiera Pan / Pani płacąc w restauracji przy użyciu karty płatniczej?

Województwo Kujawsko – Pomorskie



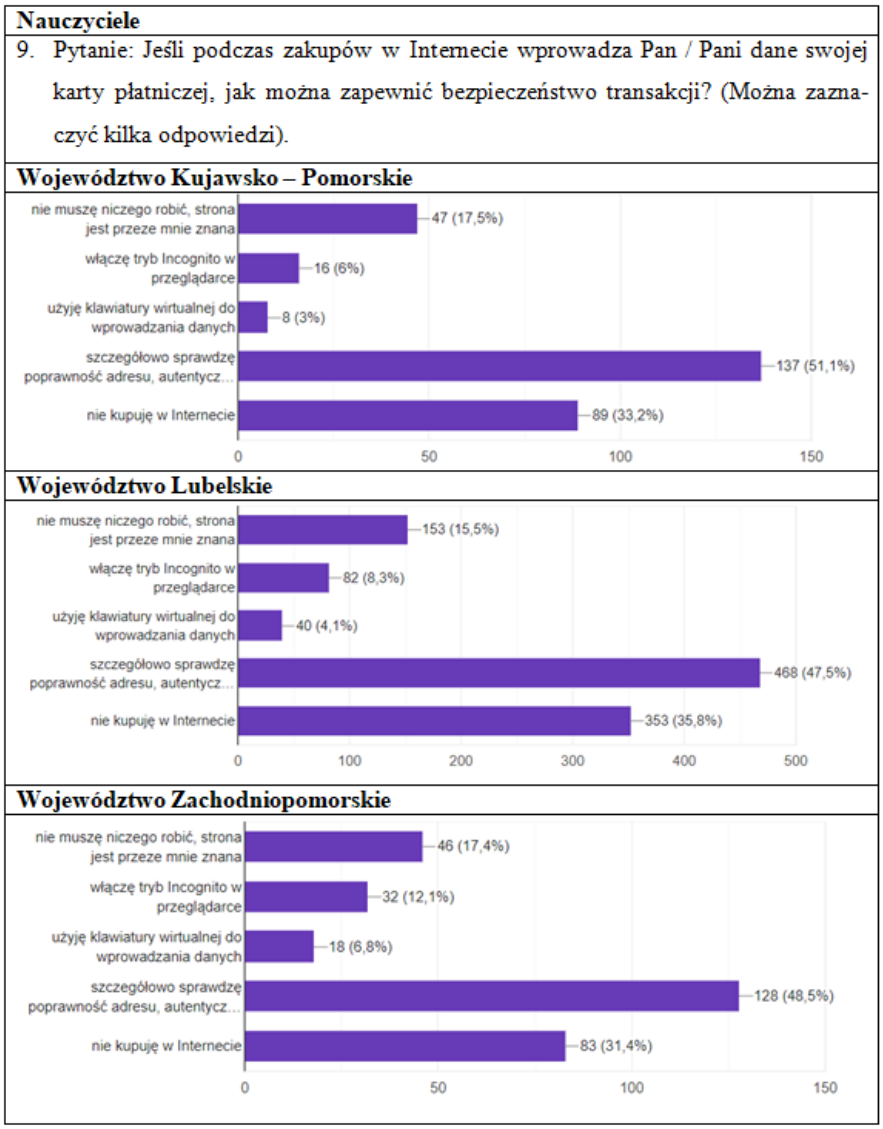
Województwo Lubelskie



Województwo Zachodniopomorskie

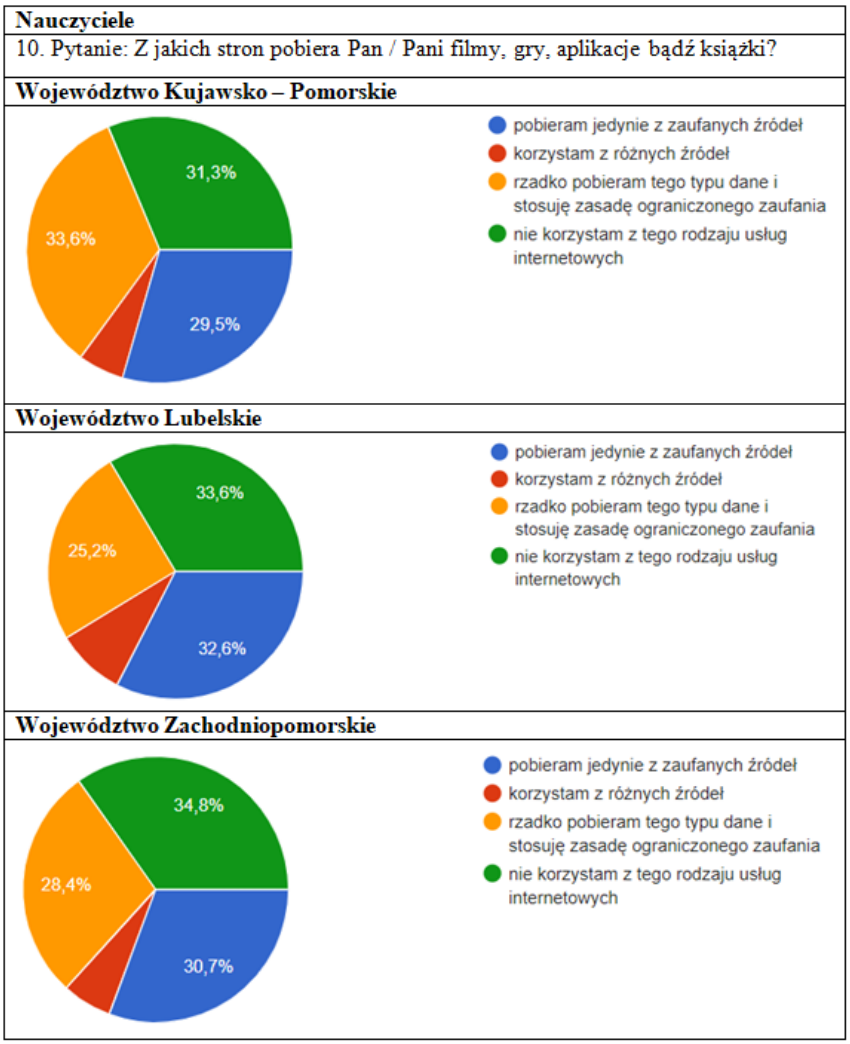
Wykres 6.8. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- płacenie w restauracji (źródło: opracowanie własne)

Pośród badanych około 30% z nich w każdym województwie wykazuje, że nie wykonuje zakupów w Internecie. Jeżeli jednak skupić się na nauczycielach, którzy takie zakupy wykonują, około 50% w każdym województwie przed dokonaniem zakupu dokładnie sprawdzi dane strony internetowej i jej autentyczność, co jest dobrą praktyką. W tej grupie występują nauczyciele dokonujący zakupów na zaufanych i dobrze im znanych stronach. Stanowią oni około 15%. Najmniej bezpieczną metodę wprowadzania danych swojej karty kredytowej, czyli wykorzystanie klawiatury wirtualnej wykazało 6,8% w woj. Zachodniopomorskim, w woj. Lubelskim 4,1% oraz w woj. Kujawsko – Pomorskim 3%. Zatem większość badanych podczas dokonywania płatności dokładnie weryfikuje stronę lub dokonuje zakupów na zaufanych platformach w trosce o swoje dane.



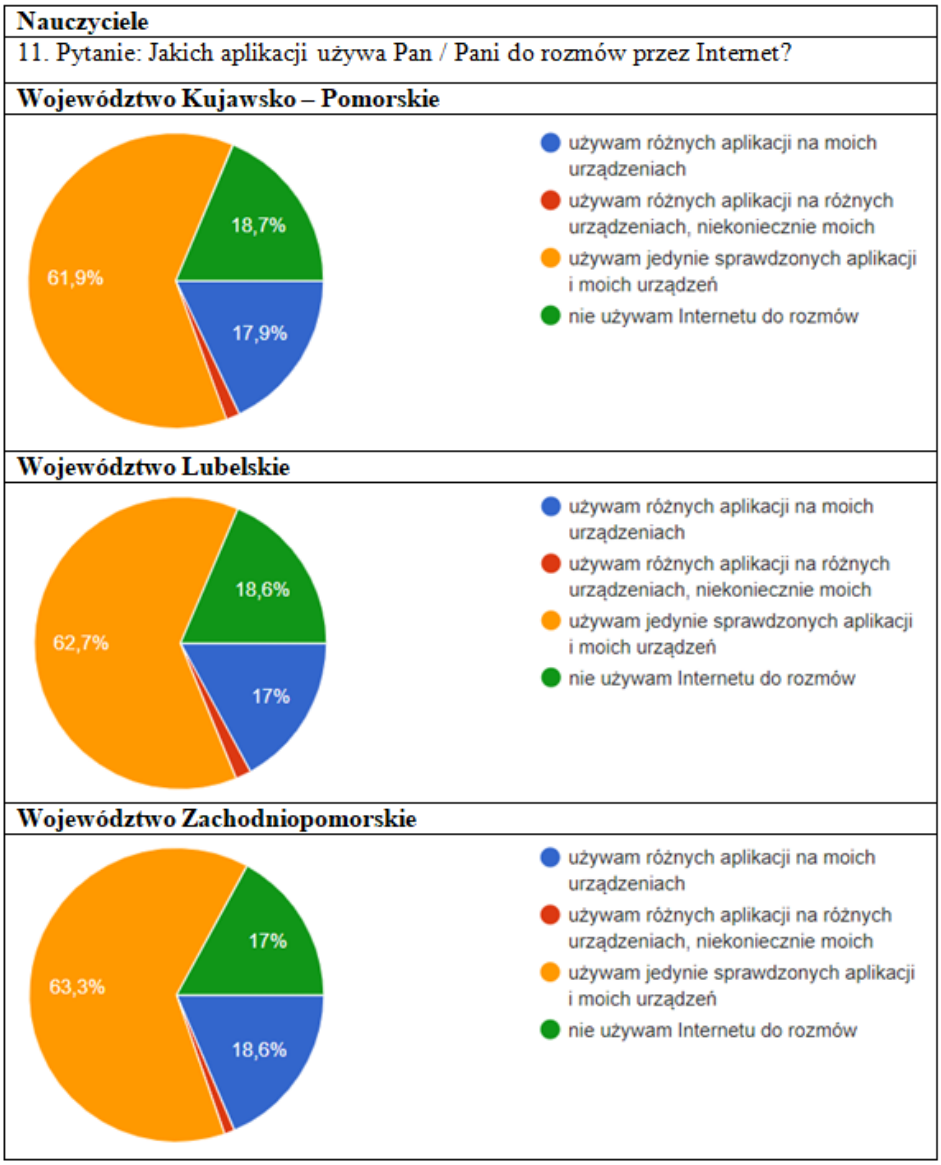
Wykres 6.9. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- zakupy w Internecie (źródło: opracowanie własne)

Respondenci wskazując źródło pobieranych aplikacji, książek itp. w woj. Kujawsko – Pomorskim w 33,6% odpowiedzieli, że rzadko korzystają z takiego sposobu pozyskiwania ww. treści. Prawie tak samo liczą grupę stanowiły osoby, które nie korzystają z takich usług – 31,3% oraz osoby, pobierające z zaufanych źródeł – 29,5%. Swoich źródeł nie sprecyzowało 5,6% badanych. W pozostałych województwach rozkład wyników był zbliżony. Jedna trzecia badanych z woj. Lubelskiego (33,6%) i Zachodniopomorskiego (34,8%) twierdzi, że nie korzysta z takich usług. Sporadyczne korzystanie wykazało 25,2% respondentów z woj. Lubelskiego oraz 28,4% z Zachodniopomorskiego. Korzystanie jedynie z zaufanych źródeł wskazało 32,6% ankietowanych w woj. Lubelskim, podobnie jak w woj. Zachodniopomorskim – 30,2 %. Pod korzystaniem z różnych źródeł podpisało się 8,6% Lubelskich nauczycieli i 6,1% z woj. Zachodniopomorskiego.



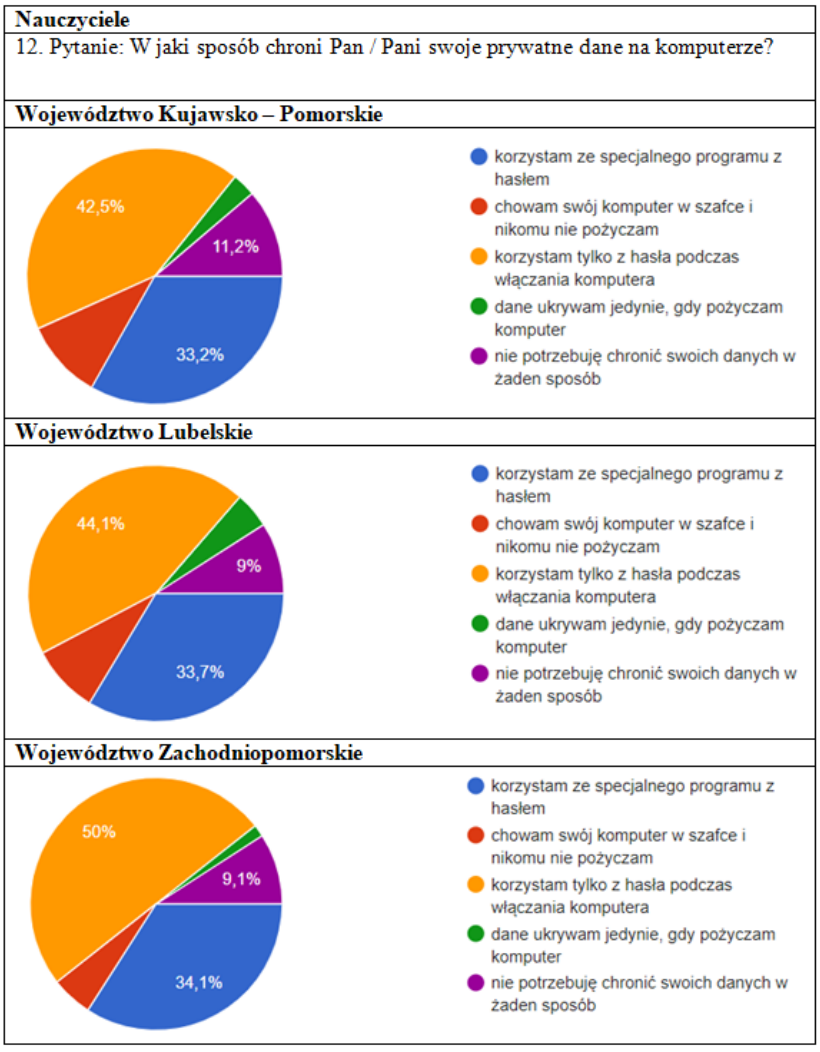
Wykres 6.10. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- pobieranie danych ze stron www (źródło: opracowanie własne)

Nauczyciele zapytani o aplikacje, z których korzystają do rozmów przez Internet, w każdym z badanych województw w większości wskazywali sprawdzone aplikacje (około 60% badanych). Około 18% respondtów w poszczególnych województwach stwierdziło, że nie korzysta z Internetu do rozmów. Również po około 18% wybiera różne aplikacje, ale korzysta tylko z własnych urządzeń. Niewielki ułamek badanych (około 1%) nie zachowuje się odpowiedzialnie i użytkuje różne aplikacje na różnych urządzeniach. Jak widać nauczyciele w większości dbają o swoją prywatność i są świadomi tego jak ważne jest korzystanie ze sprawdzonych aplikacji.



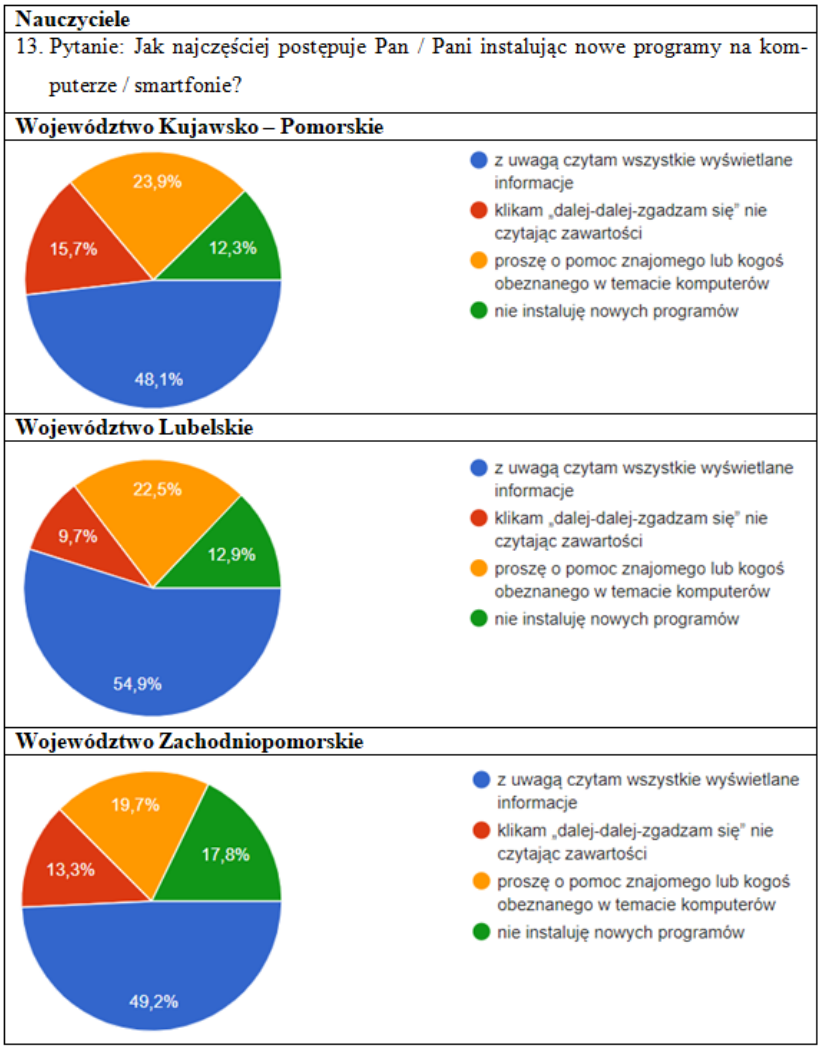
Wykres 6.11. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- aplikacje do rozmów przez Internet (źródło: opracowanie własne)

Najczęściej wybieraną metodą zabezpieczenia danych na komputerze według ankietowanych jest jedynie hasło wpisywane podczas uruchamiania komputera. Takiej odpowiedzi udzieliło, aż 50% nauczycieli z woj. Zachodniopomorskiego. W pozostałych województwach wynik ten był ponad czterdziestoprocentowy. Jako drugi najpopularniejszy sposób został wskazany specjalny program z hasłem zabezpieczającym. Ta odpowiedź uzyskała około 33% głosów w każdym województwie. Pośród badanych znalazły się również osoby, które wykorzystują szafkę jako zabezpieczenie komputera lub ukrywają dane tylko w przypadku, gdy udostępniają komputer innej osobie. Wystąpiła również około 10% grupa, która twierdzi, że nie odczuwa potrzeby zabezpieczenia danych na swoim komputerze. Warto zatem zauważyć, że wybór hasła (systemowego lub w specjalnym programie) jako formy zabezpieczenia jest najpopularniejszą metodą wśród badanej grupy.



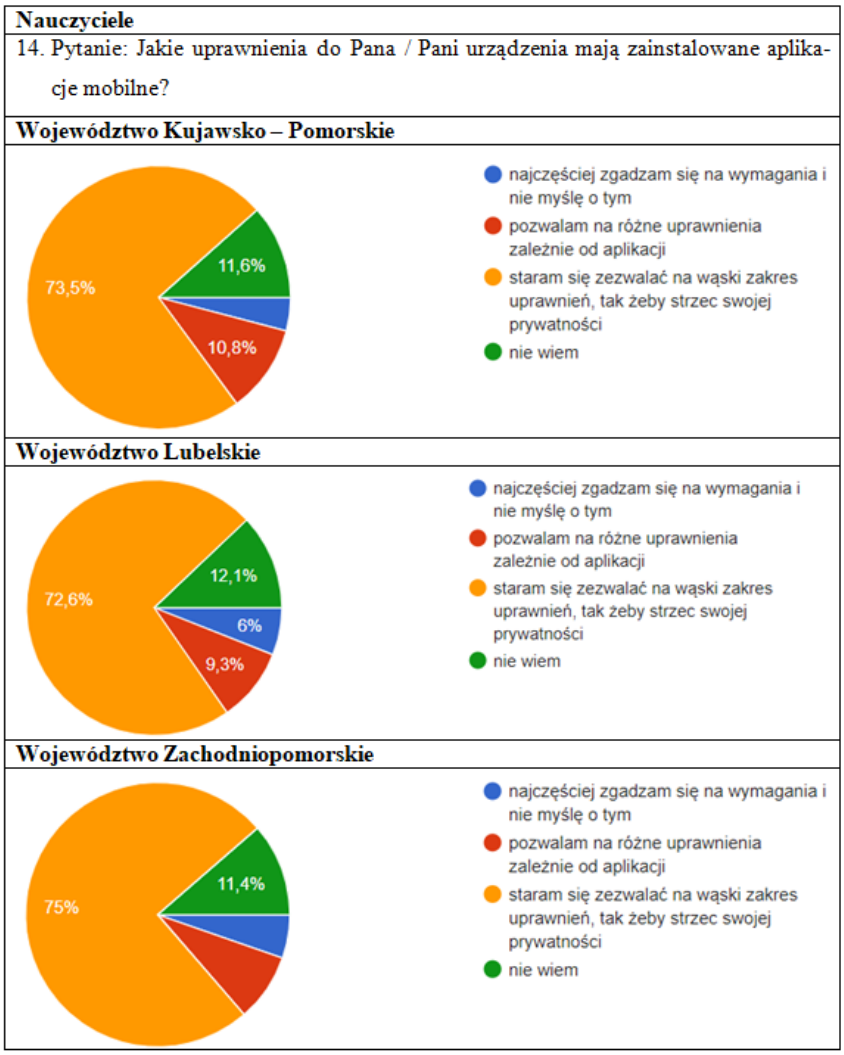
Wykres 6.12. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- ochrona prywatnych danych (źródło: opracowanie własne)

W kolejnej części kwestionariusza, nauczyciele zostali zapytani o ich postępowanie w przypadku instalowania nowych programów na swoich urządzeniach. Jak widać na wykresie poniżej (6.13), większość wykładowców zapoznaje się z informacjami wyświetlanymi podczas instalacji. Około jedna piąta badanych stosuje rozsądne podejście i prosi o pomoc bardziej doświadczonych znajomych. Najmniej odpowiedzialne zachowanie wykazuje, aż 15,7% nauczycieli z woj. Kujawsko – Pomorskiego, jest to najwyższy wynik spośród trzech województw (9,7% woj. Lubelskie, 13,1% woj. Zachodniopomorskie). Taki odsetek respondentów bez zastanowienia akceptuje wszystkie warunki. Wśród badanych znaleźli się również nauczyciele, którzy całkowicie rezygnują z instalacji aplikacji. Wyniki te stanowią o zróżnicowanym podejściu nauczycieli do wdrażania nowego oprogramowania, w skrajnych przypadkach całkowitym zaniechaniu jego instalacji, co może skutkować zatrzymaniem procesu rozwoju i ograniczeniem korzyści jakie niesie ze sobą testowanie coraz to nowszych narzędzi.



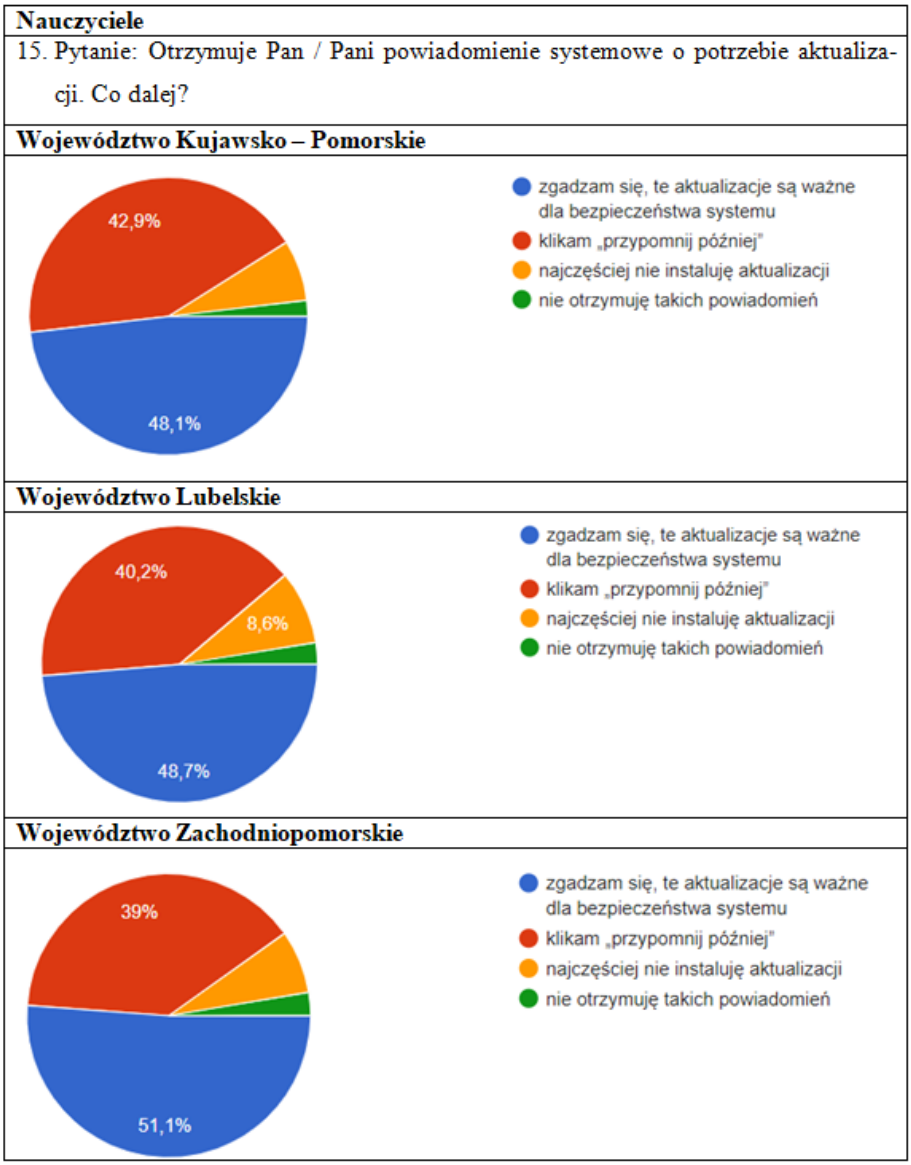
Wykres 6.13. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- instalowanie nowych programów (źródło: opracowanie własne)

Kolejnym zadaniem badanych było wskazanie zakresu uprawnień przyznawanych aplikacjom mobilnym. Większość z nich odpowiedziała, że świadomie ogranicza uprawienia aplikacji do minimum (po około 70%). Drugą grupę stanowią osoby, które nie wiedzą jakie uprawnienia posiadają zainstalowane na ich urządzeniach aplikacje. Trzecią, tak samo liczną grupę stanowią osoby ograniczające w pewnym stopniu uprawnienia aplikacji, w zależności od jej specyfiki. Najmniej odpowiedzialną grupę stanowi ok 5% badanych. Zgadzają się oni bez zastanowienia na sugerowane przez aplikacje uprawnienia. Jak widać pozytywne podejście stosuje większość respondentów, którzy ograniczają uprawnienia aplikacji lub dobierają je do specyfiki aplikacji. Niestety, również znaczna część badanych bez refleksji wyraża zgodę na większość czynności. Może to skutkować nieautoryzowanym „wyciekiem" danych i znacznie podnosi ryzyko korzystania z tych aplikacji.



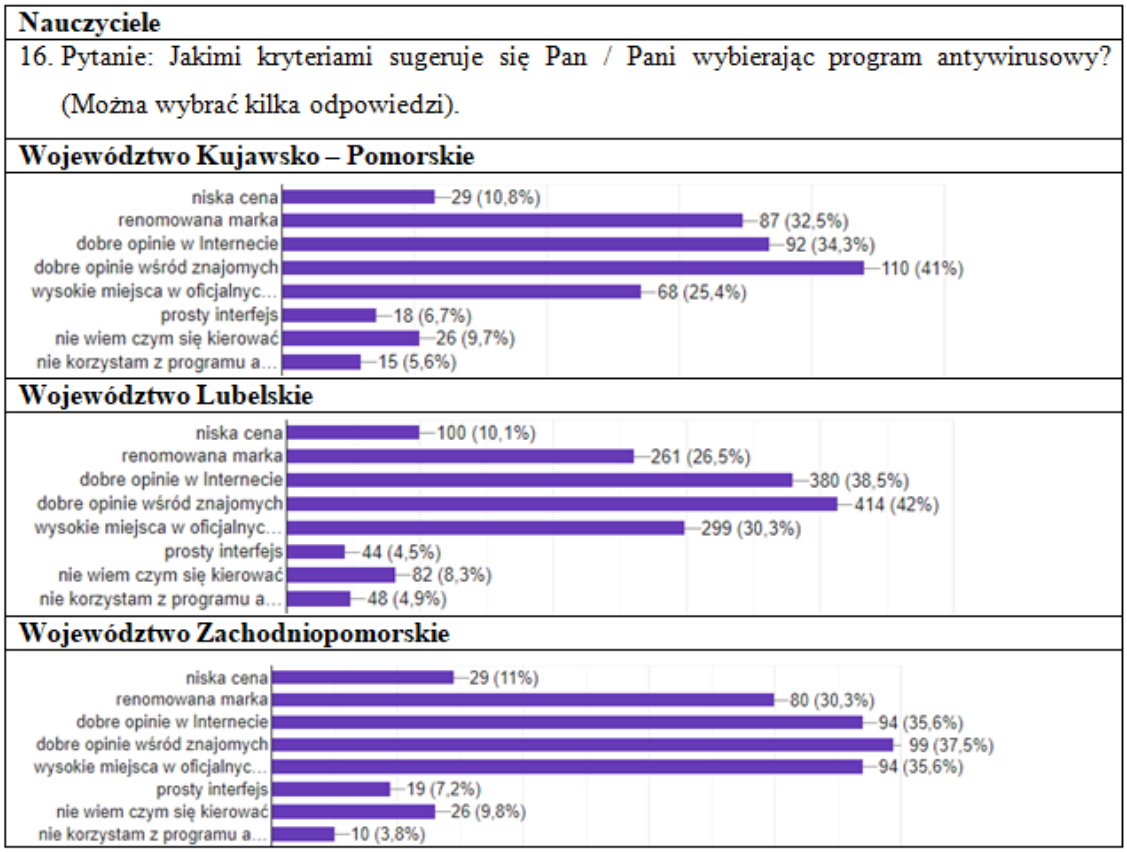
Wykres 6.14. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- uprawnienia aplikacji mobilnych (źródło: opracowanie własne)

W dalszej części badania ankietowani zostali zapytani o reakcję na otrzymanie powiadomienia o konieczności aktualizacji oprogramowania na swoim urządzeniu. We wszystkich trzech województwach wyniki były do siebie zbliżone. Blisko połowa respondentów aktualizuje oprogramowanie. Około 40 % badanych odkłada aktualizacje na później. Niewielka grupa respondentów nie decyduje się na zainstalowanie zaktualizowanego oprogramowania lub nie otrzymuje powiadomień o konieczności aktualizacji. Jak widać większość badanych zainstaluje aktualizację od razu lub w niedalekiej przyszłości. Jednak odsetek, który nie zdecyduje się na wykonanie takiego działania, prawdopodobnie nie ma świadomości z zalet regularnej aktualizacji systemu oraz jej wpływu na bezpieczeństwo oraz stabilność pracy urządzenia. Wyniki prezentuje poniższy wykres 6.15.



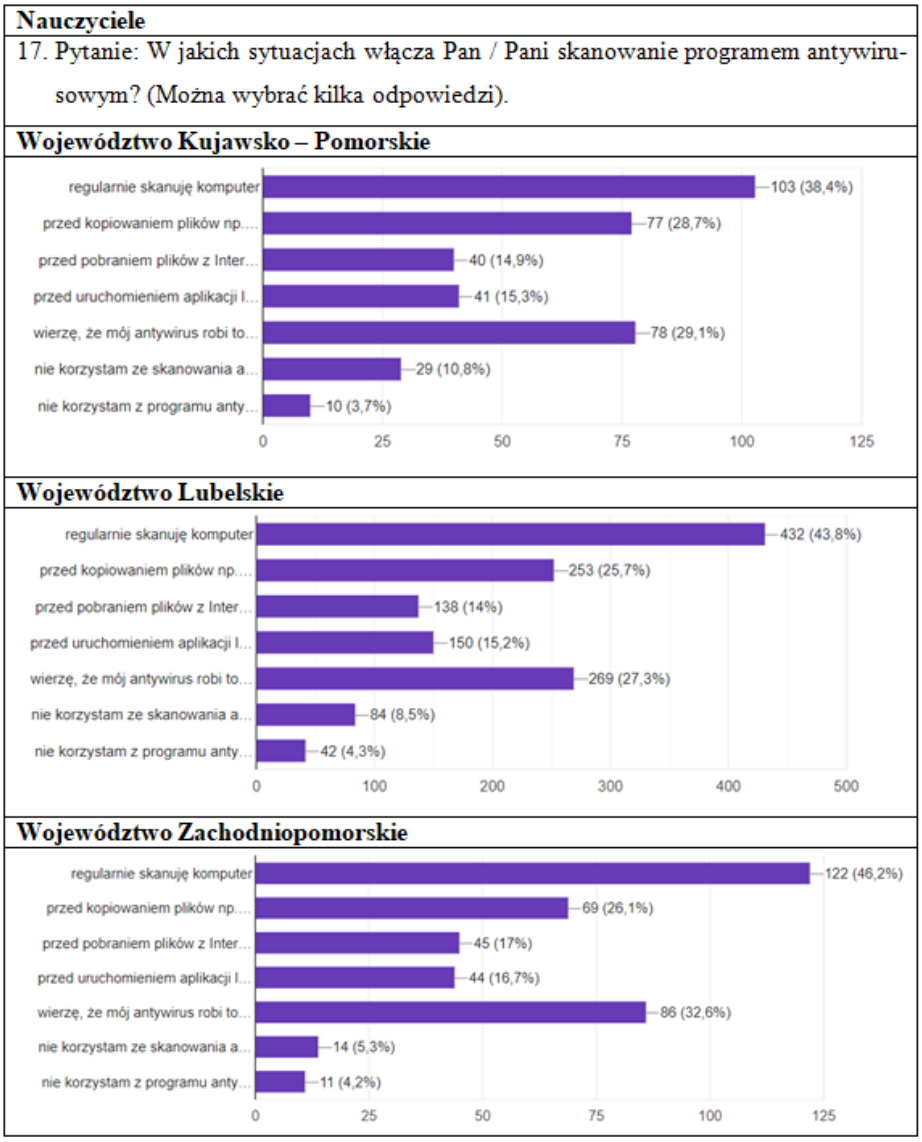
Wykres 6.15. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- powiadomienia o aktualizacji (źródło: opracowanie własne)

Obecnie wybór programu antywirusowego może okazać się bardzo skomplikowany. Na rynku istnieje mnóstwo ofert różnych producentów. Według nauczycieli ze wszystkich badanych województw największy wpływ na ich decyzje o wyborze konkretnego rozwiązania ma dobra opinia wśród znajomych. Wpływ na decyzje nauczycieli jako następne czynniki, mają dobre opinie w Internecie oraz wysokie miejsce w oficjalnych klasyfikacjach. Warto zauważyć, że dla nauczycieli z woj. Kujawsko – Pomorskiego renomowana marka jest częściej dobieranym kryterium niż wspomniane wyżej oficjalne klasyfikacje. W dalszej kolejności nauczyciele biorą pod uwagę cenę oraz złożoność interfejsu. W każdym z województw występuje grupa, która nie wie jakie kryteria powinna wziąć pod uwagę oraz również taka część, która w ogóle nie stosuje oprogramowania antywirusowego. W woj. Zachodniopomorskim niewiedzę wykazuje, aż 9,8%, podobnie w woj. Kujawsko – Pomorskim 9,7%.



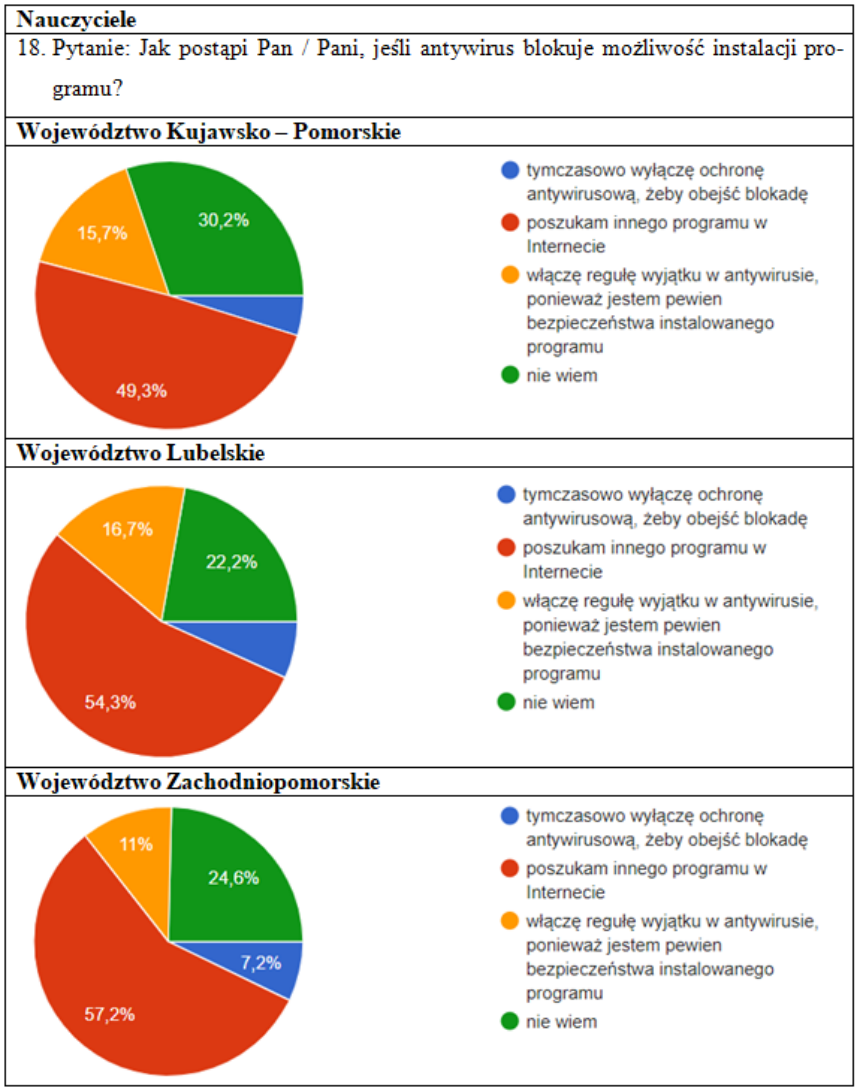
Wykres 6.16. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw-kryteria w wyborze programu antywirusowego (źródło: opracowanie własne)

Po sprawdzeniu kryteriów którymi kierują się nauczyciele podczas doboru oprogramowania antywirusowego zbadana została częstotliwość wykonywania skanowania antywirusowego posiadanych urządzeń. Większość badanych deklaruje regularne skanowanie komputera. Znaczna grupa zdaje się na automatyczne działanie „antywirusa" (najwięcej w woj. Zachodniopomorskim 37,6%). Jako kolejne ankietowani wskazali, że wykorzystują możliwość skanowania podczas kopiowania plików z nośników zewnętrznych. Największy udział osób niekorzystających ze skanowania występuje w woj. Kujawsko – Pomorskim (10,8%).



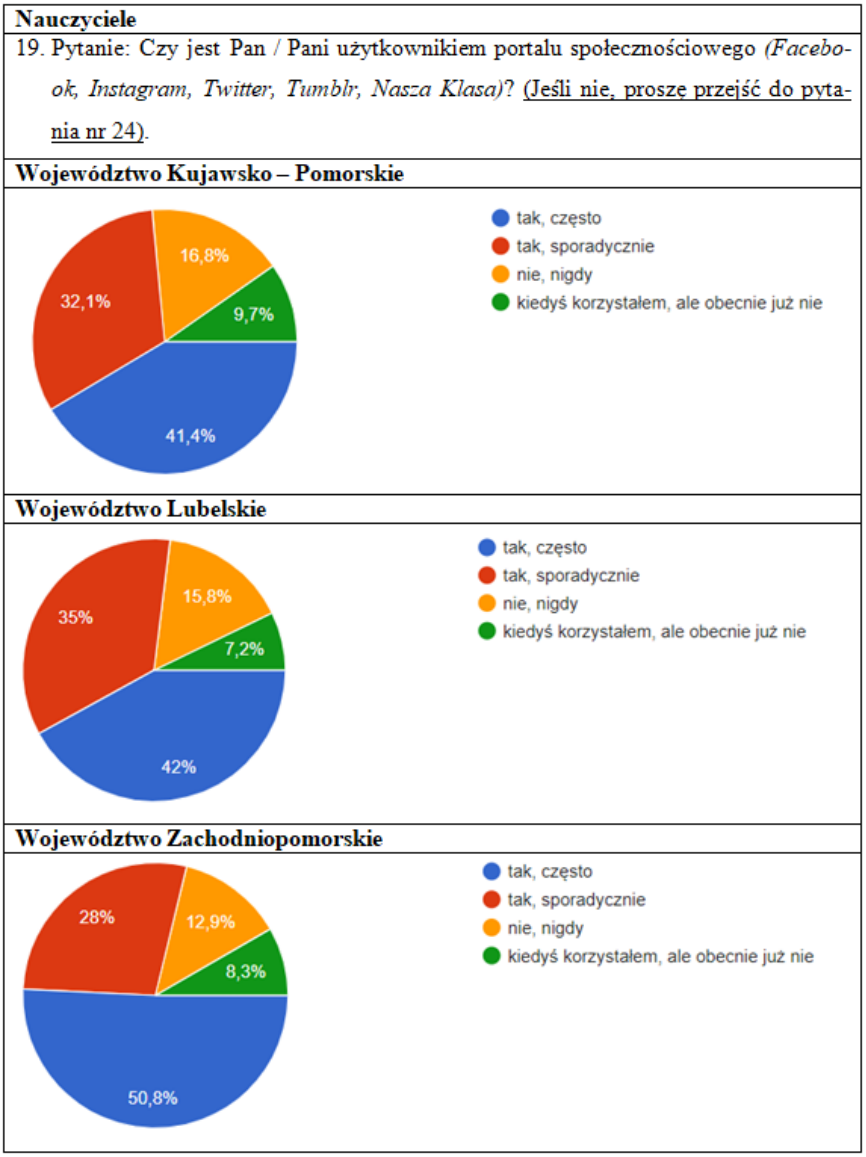
Wykres 6.17. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- skanowanie antywirusem (źródło: opracowanie własne)

Pytanie numer 18 badało postępowanie nauczycieli w przypadku blokady możliwości instalacji nowego programu przez oprogramowanie antywirusowe. Jak widać na zamieszczonym poniżej wykresie (6.18.) ponad połowa badanych postara się znaleźć inny program posiadający te same funkcje. Około 15% nauczycieli w woj. Kujawsko – pomorskim i lubelskim oraz 11% w woj. Zachodniopomorskim zdecyduje się na ryzykowny krok jakim jest dodanie wyjątku do oprogramowania antywirusowego w przekonaniu, że instalowany program nie jest zagrożeniem dla ich urządzenia. Największe ryzyko podejmie grupa, która zdecyduję się na całkowite wyłączenie ochrony antywirusowej. Jest ona najmniej liczna. Drugą co do liczebności grupę stanowią osoby, które nie potrafią postąpić w takiej sytuacji. Opisywane rezultaty wskazują na stosunkowo dużą świadomość badanych na temat tego typu zagrożeń. Jednak niepokojący jest fakt występowania tak znacznej grupy osób, niemających wiedzy w tym zakresie.



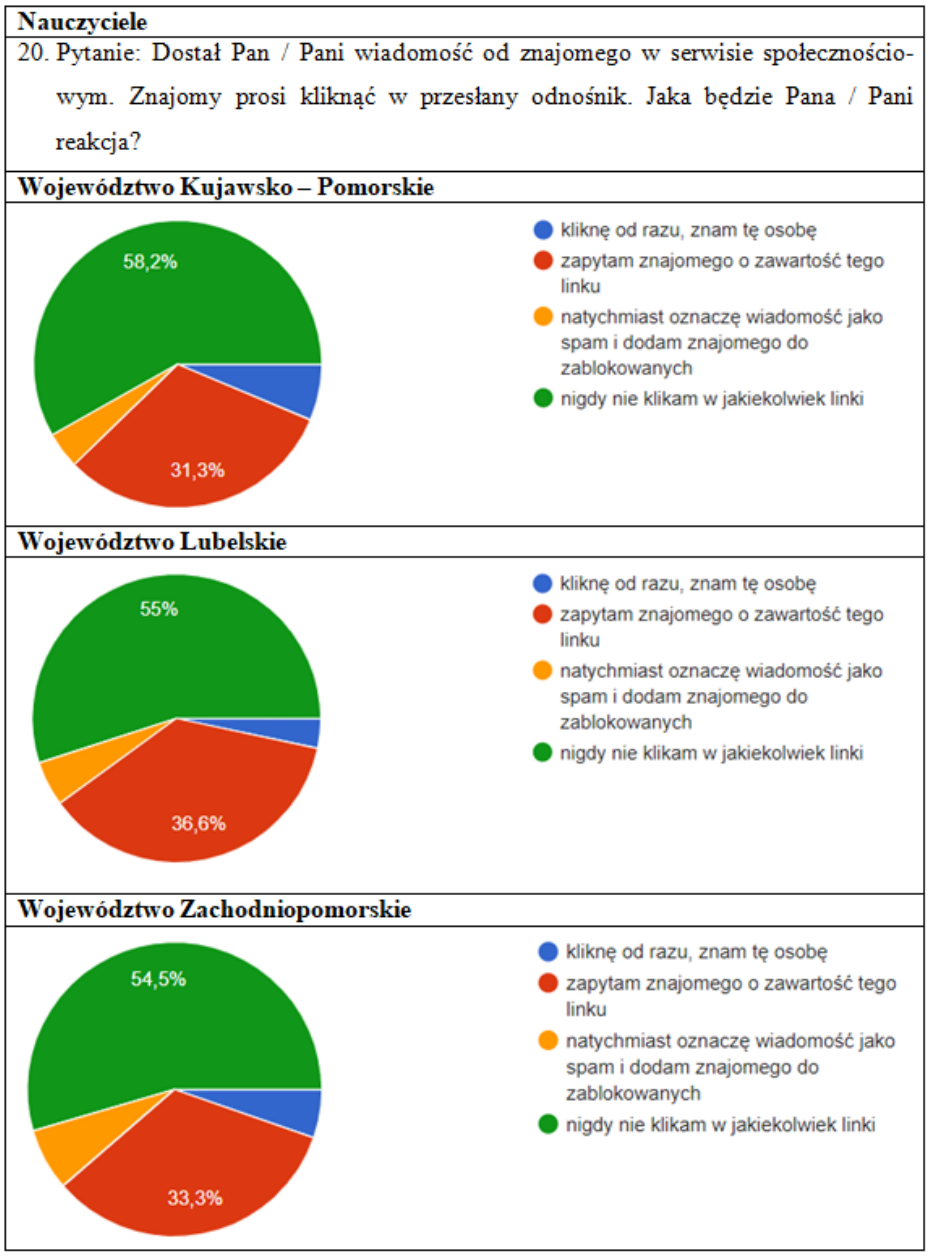
Wykres 6.18. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- blokada instalacji programu (źródło: opracowanie własne)

W dalszej części badania respondenci mieli wskazać częstotliwość korzystania z mediów społecznościowych. Większość z nich twierdzi, że często wykorzystuje popularne portale społecznościowe. W woj. Zachodniopomorskim grupa ta stanowi, aż 50,8%, w pozostałych województwach jest to około 41%. Kolejną pod względem wielkości grupę stanowią osoby deklarujące sporadyczne korzystanie z takich usług w Internecie. Aż 16,8% nauczycieli w woj. Kujawsko – Pomorskim nigdy nie korzystało z mediów społecznościowych. Podobna ilość ankietowanych odpowiedziała tak samo w woj. Lubelskim (15,8%) Natomiast w woj. Zachodniopomorskim tą grupę stanowiło 12,9% przebadanych nauczycieli. Najmniej liczny zbiór stanowią osoby, które zdecydowały się na zaprzestanie korzystania z mediów społecznościowych. Rozkład wyników we wszystkich trzech województwach był do siebie bardzo zbliżony.



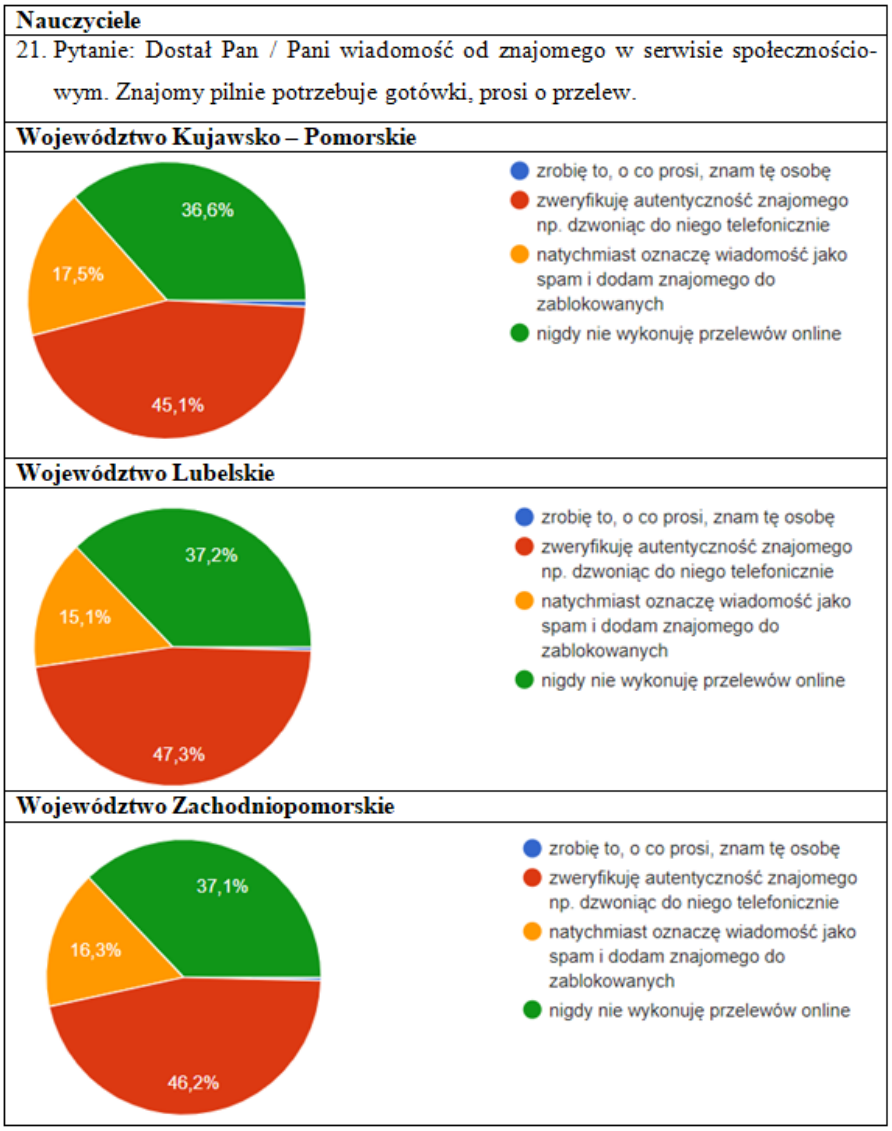
Wykres 6.19. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- korzystanie z tzw. *social media* (źródło: opracowanie własne)

Pytanie numer 20 odnosi się do reakcji na otrzymaną od znajomego wiadomość, która zawiera nieznany badanym link. We wszystkich trzech województwach rozkład wyników był bardzo podobny, ponad połowa nauczycieli stwierdziła, że nigdy nie klika w jakiekolwiek linki. Ponad 30% badanych zachowa ostrożność i zapyta znajomego o zawartość linku. Blisko 10 % nauczycieli zdecyduje się na przejście do podanej strony. Pozostała część ankietowanych doda znajomego do listy zablokowanych użytkowników, a wiadomość przeniesie od folderu ze spamem. Jak widać ponad 80% adresatów wiadomości zawierającej podejrzany link zachowa ostrożność i nie zaryzykuje przekierowania pod ten adres internetowy.



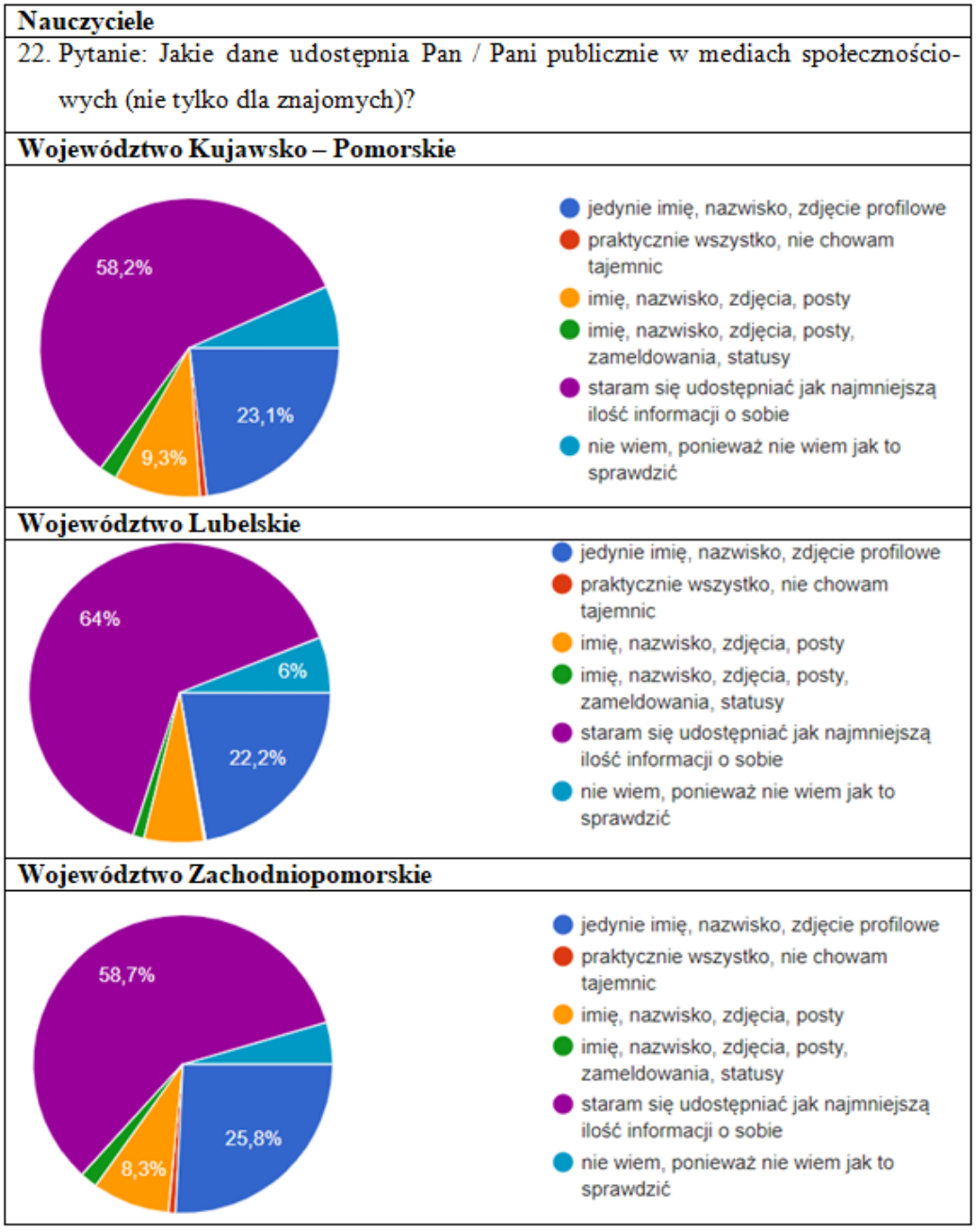
Wykres 6.20. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- otrzymanie wiadomości od znajomego, kliknięcie w link (źródło: opracowanie własne)

Pytanie numer 21 jest zbliżone do poprzedniego. Bada ono reakcję na prośbę o przekazanie pieniędzy przelewem. Największą grupę badanych stanowią nauczyciele, którzy podejmą próbę zweryfikowania takiej wiadomości. Wśród sondażowanych występuje również znaczna grupa (około 36%), która nigdy nie wykonuje przelewów internetowych. Trzecią grupę stanowią osoby, które natychmiastowo zablokują znajomego, a wiadomość przeniosą do folderu ze spamem. Poniżej 1% przebadanych nauczycieli zdecyduje się na przesłanie pieniędzy bez zweryfikowania autentyczności otrzymanej wiadomości. Zatem porównując pytania numer 20 i 21 możemy zauważyć, że jeżeli występuje kwestia finansów, nauczyciele ze wszystkich trzech województw zachowują dużo większą ostrożność i nie decydują się na zrealizowanie prośby zawartej w wiadomości.



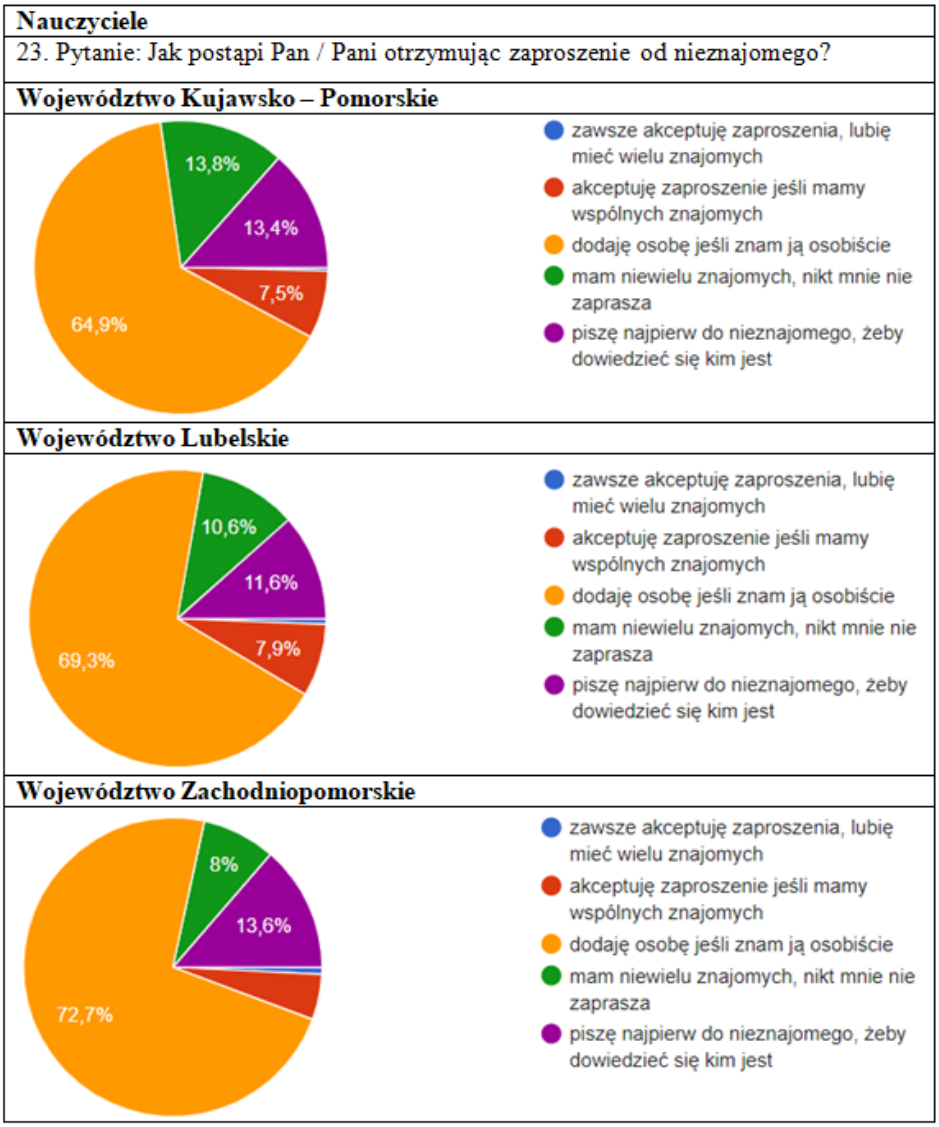
Wykres 6.21. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- otrzymanie wiadomości od znajomego, prośba o przelew (źródło: opracowanie własne)

Analizując poniższe wykresy (6.22) można ocenić, iż większość ankietowanych w swojej opinii stara się udostępniać jak najmniejszą ilość danych. Niewiele ponad 30% stanowi grupa badanych, która udostępnia jedynie imię nazwisko i zdjęcie profilowe lub inne zdjęcia i posty. Niewielka część badanych dodatkowo decyduje się na udostępnienie swojej lokalizacji. Niepokojący jest fakt występowania grupy nauczycieli, którzy pomimo korzystania z mediów społecznościowych nie wiedzą, jak sprawdzić udostępniane przez siebie dane lub upubliczniają wszystkie informacje.



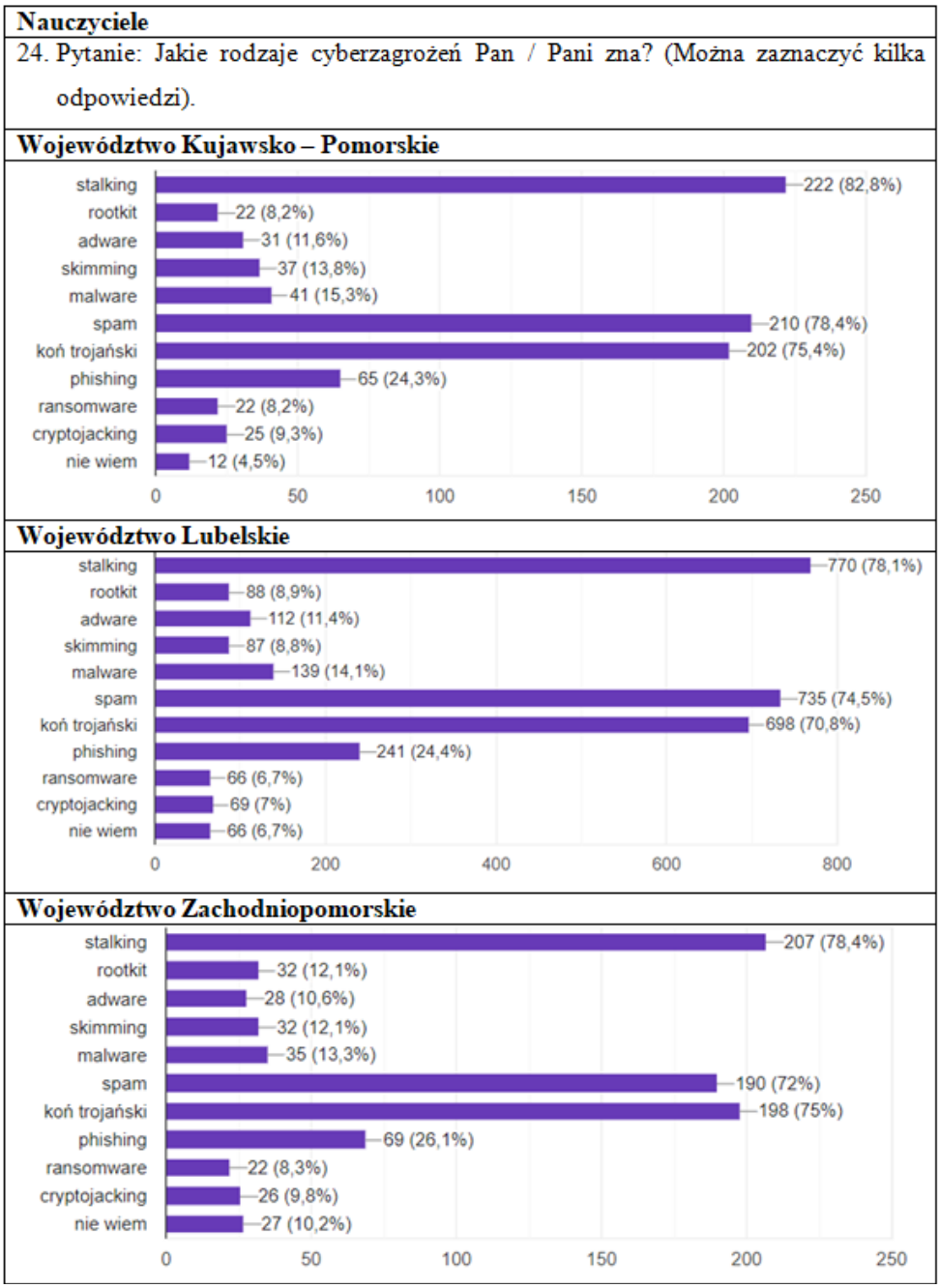
Wykres 6.22. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- udostępnianie informacji w tzw. *social media* (źródło: opracowanie własne)

Większość serwisów społecznościowych daje możliwość tworzenia grupy znajomych. W kolejnej części ankiety, nauczyciele zostali zapytani o to jak postąpią po otrzymaniu zaproszenia od nieznajomego. Od 64% do prawie 73% badanych doda tę osobę do listy znajomych tylko, jeżeli zna ją osobiście. Próbę weryfikacji użytkownika i wejścia z nim w kontakt podejmuje w zależności od województwa od 11,6% do 13,8% badanych. Dla około 7,5% badanych wystarczający jest fakt, że osoba ta posiada wspólnych znajomych. Wśród ankietowanych powstała również grupa niecieszące się taką popularnością i nieotrzymująca nowych zaproszeń do grona znajomych. Bez zastanowienia zaproszenia akceptuje nieznaczna część nauczycieli (poniżej 1%). Jak widać większość ankietowanych postępuje prawidłowo dodając osoby, które zna lub w przypadku wątpliwości weryfikuje tą znajomość.



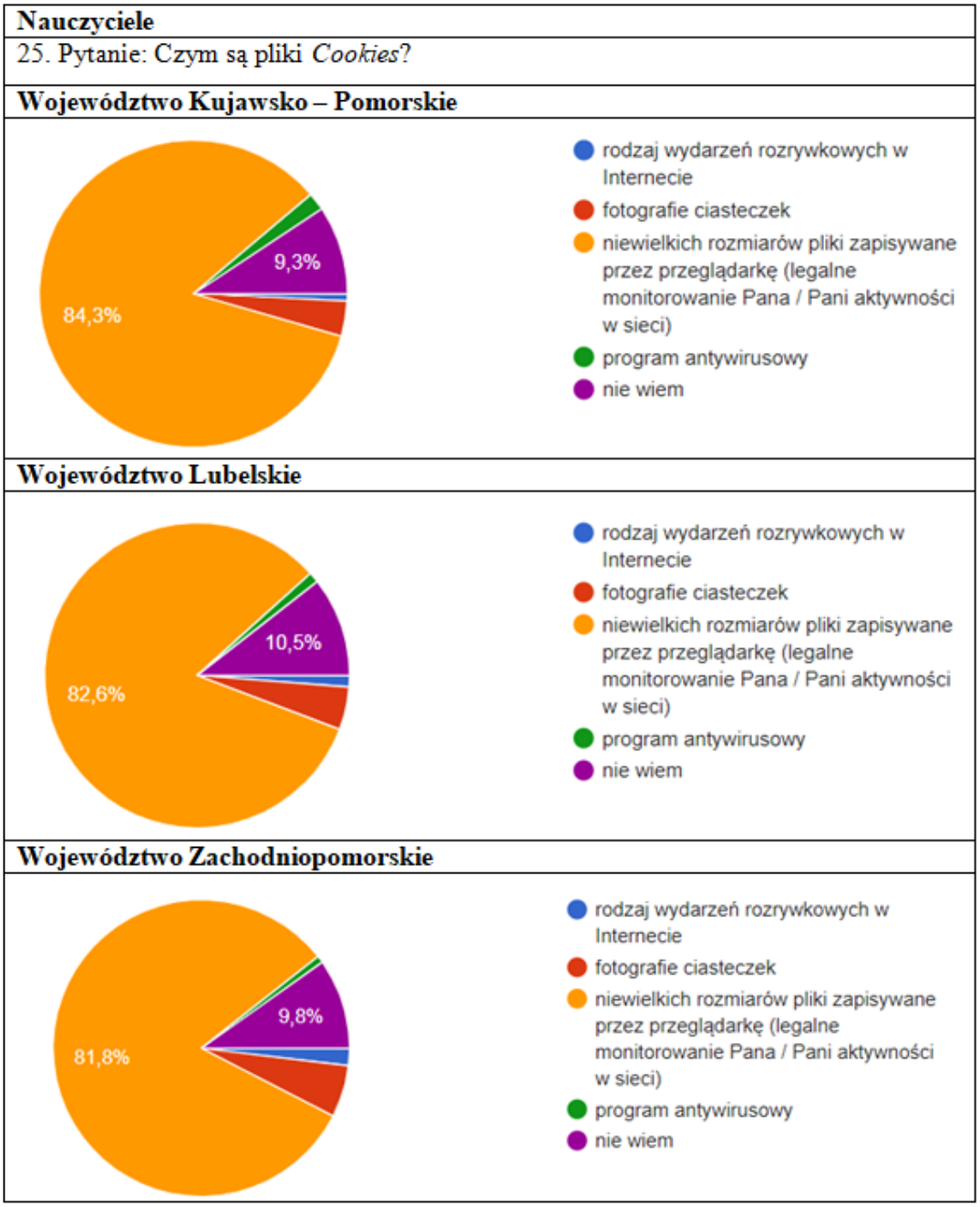
Wykres 6.23. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- otrzymanie zaproszenia od nieznajomego (źródło: opracowanie własne)

Korzystając z Internetu możemy napotkać wiele zagrożeń. Według badanych z trzech województw najbardziej znanymi cyberzagrożeniami są: stalking, spam oraz koń trojański. Zjawiska te uzyskały prawie po 80% głosów. Kolejnym najczęściej wskazywanym zagrożeniem jest phishing (około 25%). Wśród respondentów wyłoniła się grupa, która nie potrafiła wskazać zagrożeń występujących w sieci. Najwięcej, bo 66 osób w woj. Lubelskim. Takie wyniki mogą sugerować, że wiedza na temat zagrożeń jest stosunkowo niewielka i ogranicza się tylko do umiejętności zdefiniowania najbardziej popularnych zjawisk.



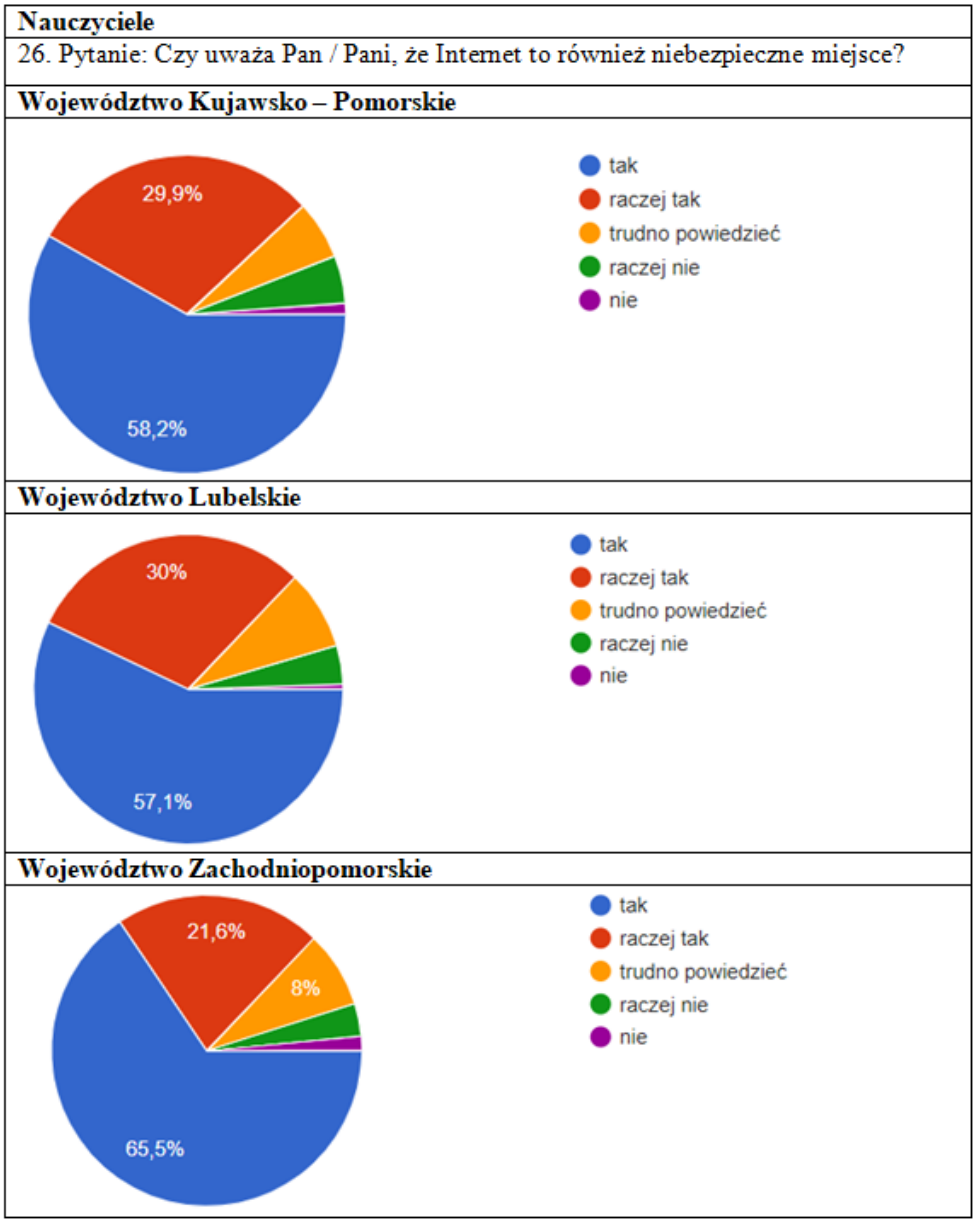
Wykres 6.24. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- znajomość cyberzagrożeń (źródło: opracowanie własne)

W przypadku znajomości pojęcia *Cookies*, można wskazać główny podział na dwie odpowiedzi. Większość, bo ponad 80% badanych wskazało prawidłową definicję „ciasteczek". Druga grupa około 10% z każdego województwa nie potrafiła określić czym są pliki *Cookies*. Pozostałe odpowiedzi nie uzyskały znaczącej liczby głosów. Pomimo wyświetlanych komunikatów o gromadzeniu danych w postaci *Cookies* odsetek osób błędnie je definiujących jest dość wysoki i wynosi blisko 20% w każdym z badanych województw.



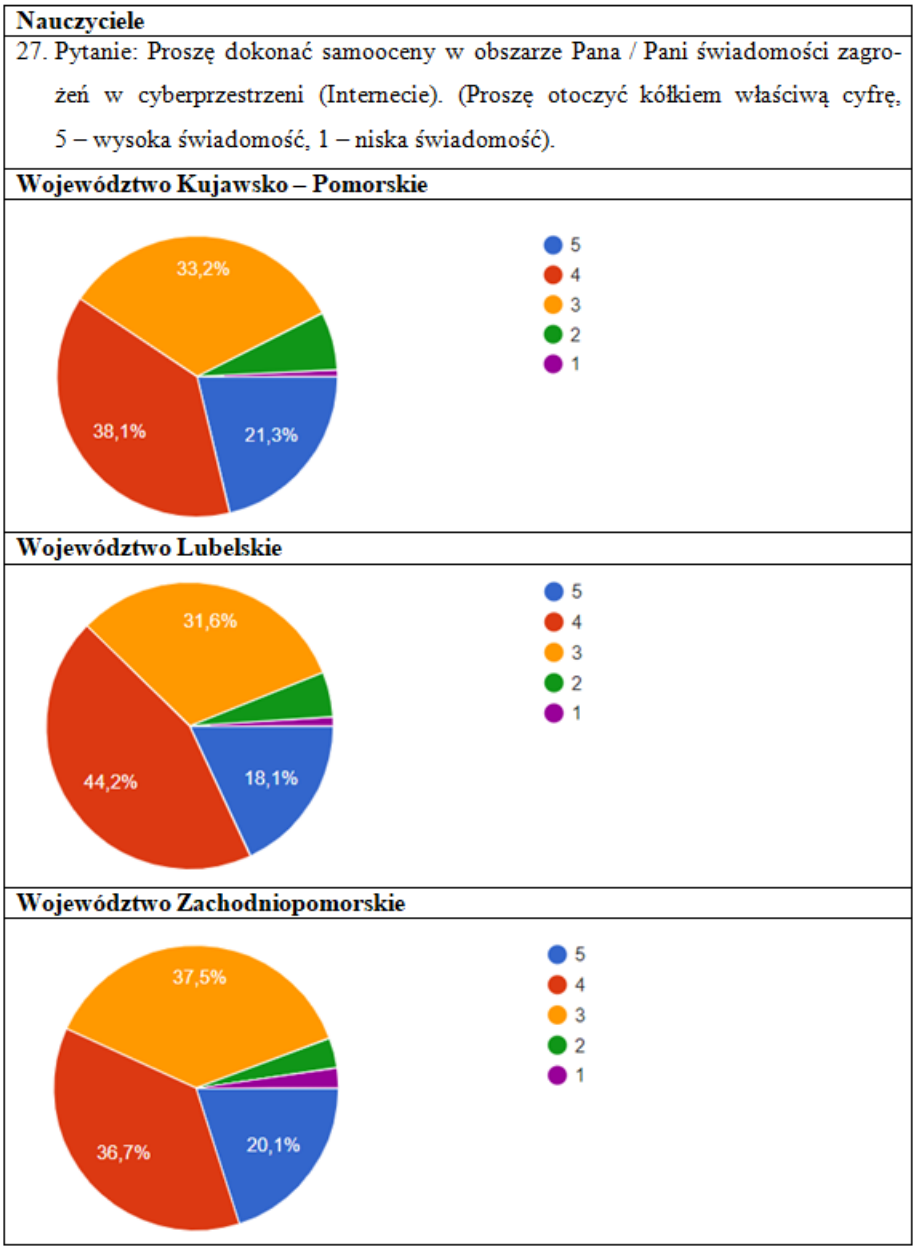
Wykres 6.25. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- znajomość definicji plików *Cookies* (źródło: opracowanie własne)

Jak ukazują poniższe wykresy (6.26.) większość badanych nauczycieli uważa Internet za niebezpieczne miejsce. W woj. Zachodniopomorskim taki pogląd podziela, aż 65,5% ankietowanych. W pozostałych województwach wynik jest prawie tak samo wysoki, w woj. Lubelskim 58,2% a w woj. Kujawsko – Pomorskim 57,1%. Pozostali nauczyciele mieli problem w określeniu swojego zdania lub skłaniali się ku odpowiedzi „raczej nie". Niewielka grupa badanych wskazała Internet jako miejsce bezpieczne. Zatem, konkludując, większość respondentów (prawie 90%) uważa Internet za miejsce niebezpieczne lub skłania się do takiej odpowiedzi.



Wykres 6.26. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- określenie Internetu jako niebezpiecznego miejsca (źródło: opracowanie własne)

Analizując poniższe wyniki można stwierdzić, że większość ankietowanych ocenia swoją świadomość na temat zagrożeń w cyberprzestrzeni jako średnią lub wyższą. Średnią świadomość (ocena 3 i 4) wykazuje ponad połowa badanych. Natomiast wysoką świadomość deklaruje jedna piąta badanych. Wyniki te wskazują, że większość nauczycieli świadomie porusza się w środowisku internetowym i wie, jak zadbać o swoje bezpieczeństwo. Jednak występowanie zbioru, który dość nisko ocenia swoją świadomość na temat zagrożeń w cyberprzestrzeni może sugerować potrzebę dalszej edukacji w tym zakresie.



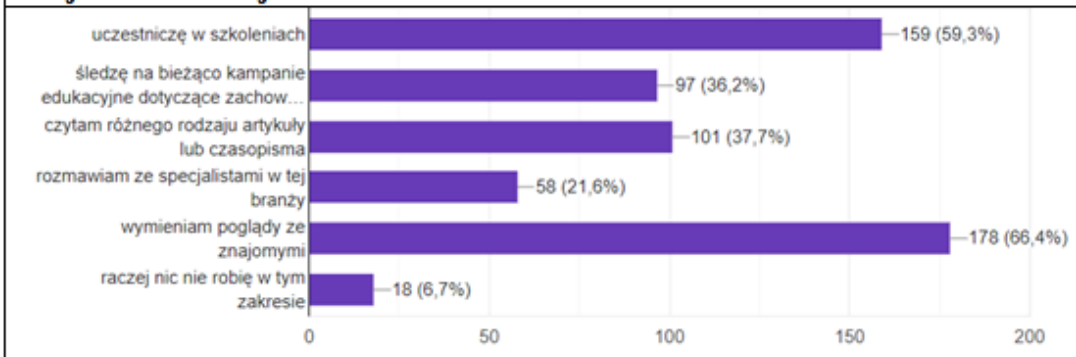
Wykres 6.27. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- samoocena świadomości zagrożeń (źródło: opracowanie własne)

W obecnych czasach szybkość zmian w sferze cyfrowej jest bardzo wysoka. Konieczny jest ciągły rozwój w tym zakresie, żeby nie pozostać w tyle i nie stać się podatnym na równie szybko rozwijające się zagrożenia. Nauczyciele zapytani o to w jaki sposób rozwijają swoje kompetencje cyfrowe odpowiadali następująco. W woj. Kujawsko – Pomorskim wymiana poglądów ze znajomymi (66,4%) została najczęściej wskazywaną metodą rozwoju kompetencji cyfrowych. Uczestnictwo w szkoleniach wykazuje 59,3% badanych. Prawie taka sama grupa nauczycieli czerpie wiedzę z kampanii edukacyjnych (36,2%) oraz czasopism i artykułów (37,7%). Pomoc specjalistów wybiera 21,6% badanych. W woj. Lubelskim jako najpopularniejszy sposób rozwoju kompetencji cyfrowych wskazane zostały szkolenia (68,2%) a jako druga wymiana poglądów ze znajomymi (59,1%). Podobnie jak w woj. Kujawsko – Pomorskim wystąpiły grupy badanych wykorzystujące do rozwoju artykuły i czasopisma (36,9%), kampanie edukacyjne (31,7%) oraz rozmowy ze specjalistami (19%). W woj. Zachodniopomorskim zbliżona ilość badanych wykazuje uczestnictwo w szkoleniach oraz wymianę poglądów ze swoimi znajomymi (około 60%). Następnie znaczną ilość głosów otrzymało korzystanie z czasopism i artykułów (48,5%) i podobnie jak w pozostałych województwach ankietowani wybierali kampanie edukacyjne (33,7%) oraz rady specjalistów (19%). W każdym z badanych województw wystąpiła grupa, która nie podejmuje próby zwiększenia swoich kompetencji cyfrowych. Zatem za najpopularniejsze metody rozwoju kompetencji cyfrowych należy ująć wymianę doświadczeń ze znajomymi oraz szkolenia z zakresu cyberbezpieczeństwa.

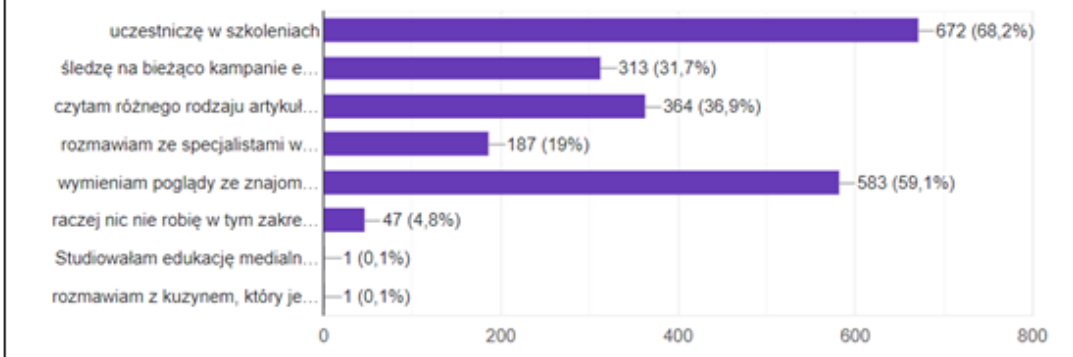
Nauczyciele

28. Pytanie: Jakie działania podejmuje Pan / Pani, żeby zwiększać swój poziom kompetencji cyfrowych? Kompetencje cyfrowe rozumiane są w uproszczeniu jako zbiór umiejętności pozwalających skutecznie i sprawnie korzystać z komputera oraz Internetu. (Można zaznaczyć kilka odpowiedzi).

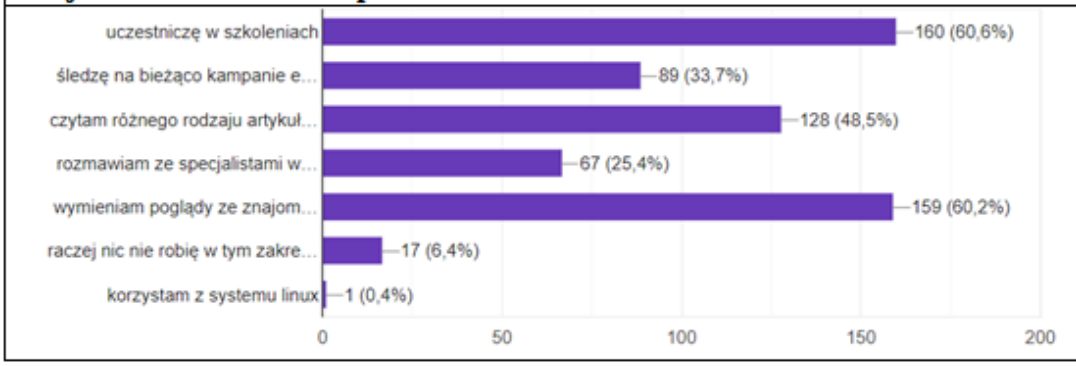
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

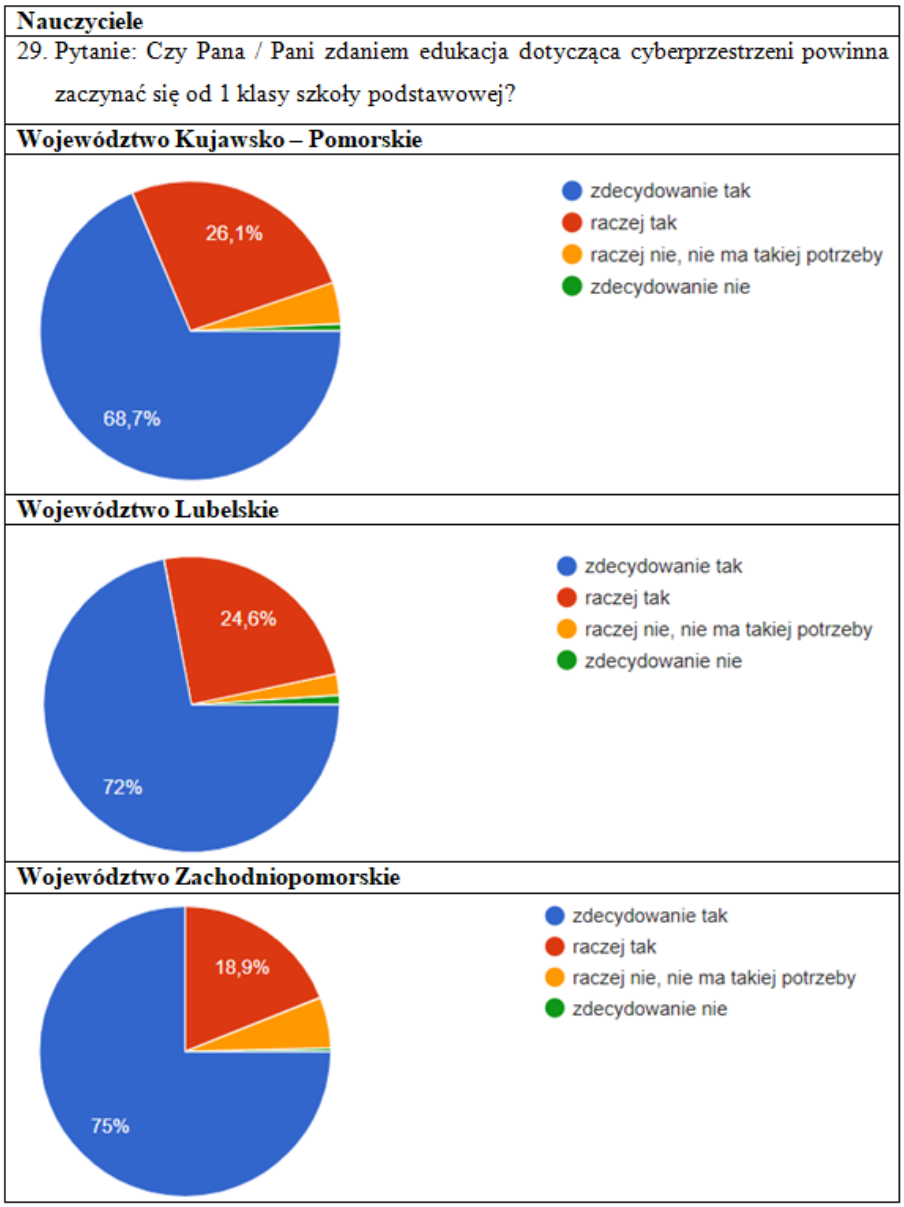


Województwo Zachodniopomorskie



Wykres 6.28. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- podejmowanie działań zwiększających poziom kompetencji cyfrowych (źródło: opracowanie własne)

Badani nauczyciele opowiedzieli się za rozpoczęciem nauki na temat cyberprzestrzeni już od 1. klasy szkoły podstawowej. Takiej odpowiedzi udzieliło aż 75% badanych z woj. Zachodniopomorskiego i kolejno z woj. Lubelskiego 72% oraz woj. Kujawsko – Pomorskiego 68,7%. Znaczna grupa badanych skłaniała się ku takiej odpowiedzi najwięcej w woj. Kujawsko – pomorskim (26,1%), najmniej w woj. Zachodniopomorskim (18,9%). Pozostała część ankietowanych nie odczuwała potrzeby wprowadzenia takich zagadnień do programu nauczania 1. klasy szkoły podstawowej. Zatem zdecydowana większość nauczycieli dostrzega konieczność nauki o zagrożeniach i bezpieczeństwie w sieci już od najmłodszych lat.



Wykres 6.29. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wskazanie istoty edukacji od wczesnych lat ucznia (źródło: opracowanie własne)

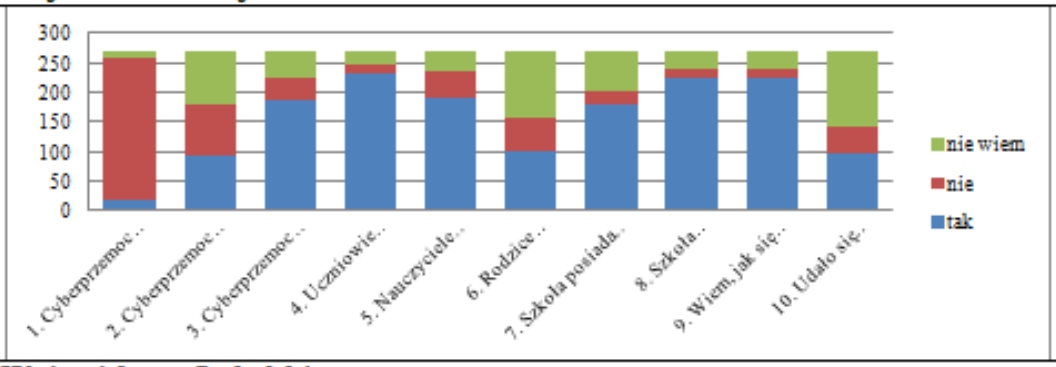
Pytanie numer 30 dotyczyło zjawiska cyberprzemocy. Podpunkty w nim zawarte można podzielić na trzy grupy. Grupa pierwsza (1-3) dotyczy występowania tego zjawiska. Grupa druga (4-6) odnosi się do szkolenia w zakresie cyberprzemocy. Natomiast grupa trzecia (7-10) obejmuje procedury oraz ich skuteczność. Analizując poniższe wykresy należy stwierdzić, że wyniki w trzech badanych województwach są do siebie zbliżone. Odnosząc się do pierwszej grupy podpunktów, większość nauczycieli nie była dotknięta bezpośrednio cyberprzemocą jednak potrafi wskazać innego nauczyciela bądź ucznia, który doznał takiego ataku. Jednak odsetek uczniów dotkniętych tym zjawiskiem przewyższa o ponad połowę zaatakowanych nauczycieli. Analizując drugą grupę dotyczącą szkoleń warto dostrzec, że nauczyciele oraz uczniowie w większości odbywają szkolenia z zakresy cyberprzemocy. Według badanych gorzej ma się ta kwestia w przypadku rodziców. Wykazują oni jednak znaczą niewiedzę. W odniesieniu do procedur i ich skuteczności można zaobserwować, że większość szkół posiada procedury postępowania w przypadku wystąpienia zjawiska cyberprzemocy oraz nauczyciele wiedzą jak mają postąpić w takiej sytuacji. Szkoły w których pracują badani w większości podjęły współpracę z innymi podmiotami zajmującymi się obszarem cyberprzemocy. Jednak pomimo wiedzy nauczycieli oraz posiadanych procedur sprawcę cyberprzemocy udało się ustalić tylko w około jednej trzeciej przypadków. Liczba ta może być jednak wyższa lub niższa, ponieważ ankietowani również w tym przypadku wykazali znaczą niewiedzę.

Nauczyciele

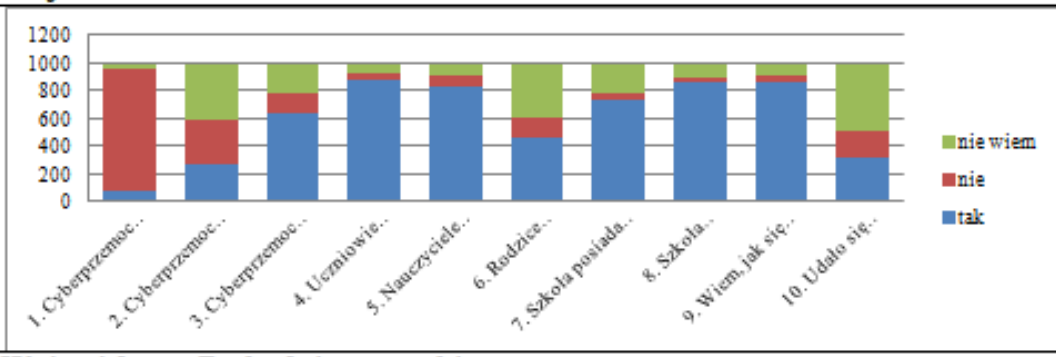
30. Pytanie: Czy spotkał się Pan / Pani z problemem cyberprzemocy (nękanie, dręczenie, prześladowanie w Internecie)? (Proszę odnieść się do <u>każdego</u> z podpunktów).

1. Cyberprzemoc dotknęła mnie bezpośrednio
2. Cyberprzemoc dotknęła innych nauczycieli
3. Cyberprzemoc dotknęła uczniów
4. Uczniowie odbywają lekcje związane z przeciwdziałaniem cyberprzemocy
5. Nauczyciele odbywają szkolenia związane z przeciwdziałaniem cyberprzemocy
6. Rodzice odbywają szkolenia związane z przeciwdziałaniem cyberprzemocy
7. Szkoła posiada procedury działania w sytuacji cyberprzemocy
8. Szkoła współpracuje z różnymi podmiotami w zakresie cyberprzemocy np. z policją
9. Wiem, jak się zachować kiedy występuje zjawisko cyberprzemocy
10. Udało się ustalić sprawcę cyberprzemocy

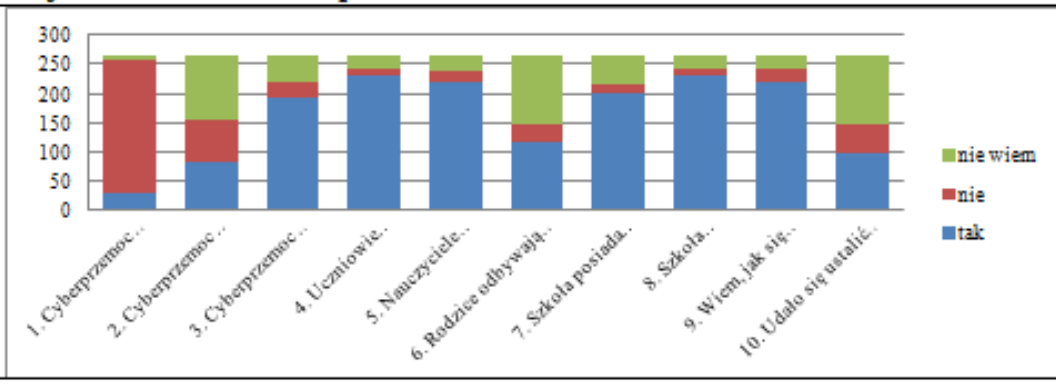
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

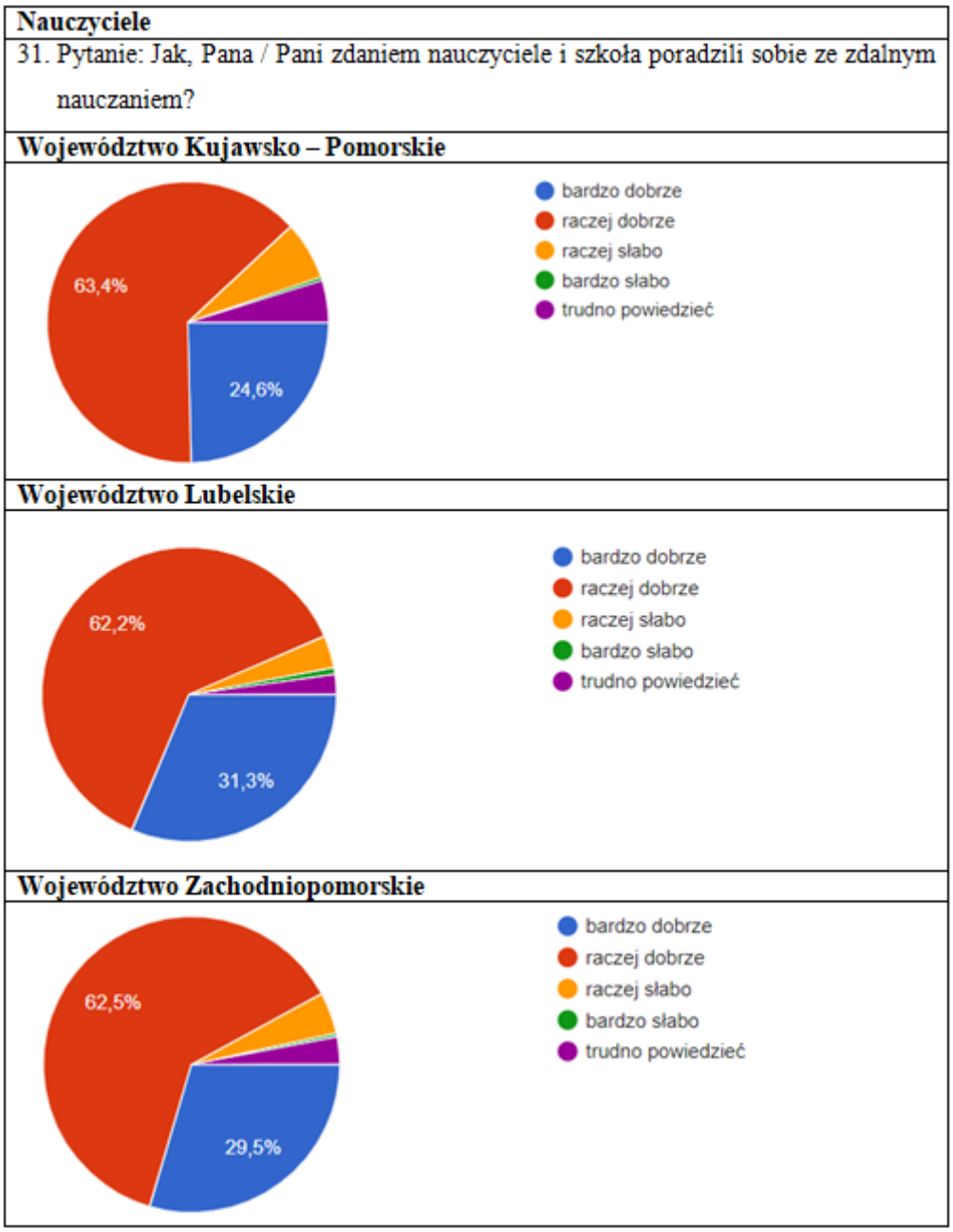


Województwo Zachodniopomorskie



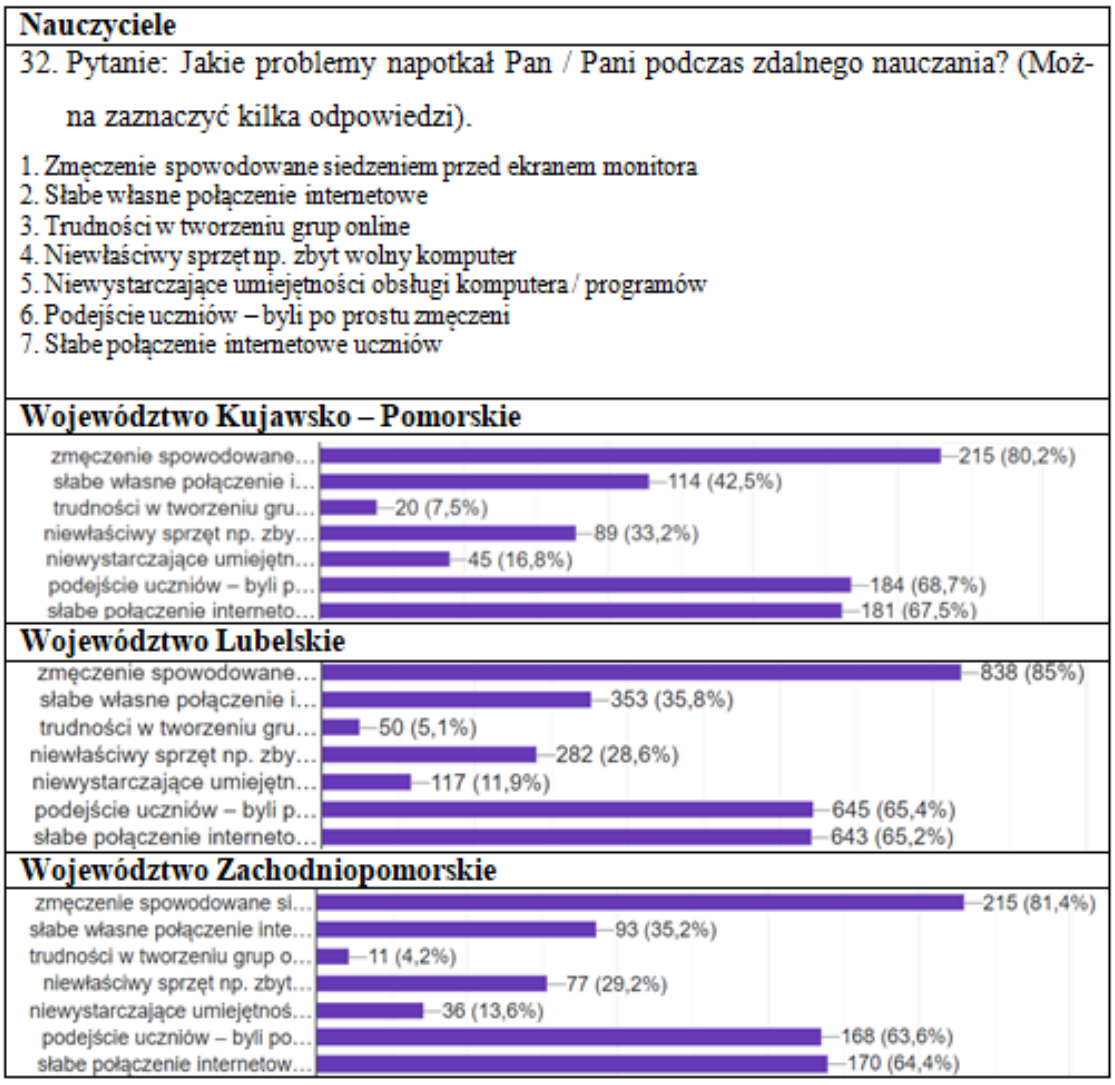
Wykres 6.30. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw-zetknięcie się z problemem cyberprzemocy (źródło: opracowanie własne)

W opinii nauczycieli okres zdalnego nauczania został oceniony pozytywnie (około 90% odpowiedzi). Taki rozkład odpowiedzi sugeruje, że większość badanych miała dobre doświadczenia związane z nauką zdalną. Może również wskazywać na umiejętność szybkiego dostosowania się nauczycieli do nowego sposobu nauczania. Wystąpienie grupy oceniającej zdalne nauczenie negatywnie najprawdopodobniej powiązane jest z różnymi trudnościami jakie napotkali oni podczas prowadzenia takich zajęć.



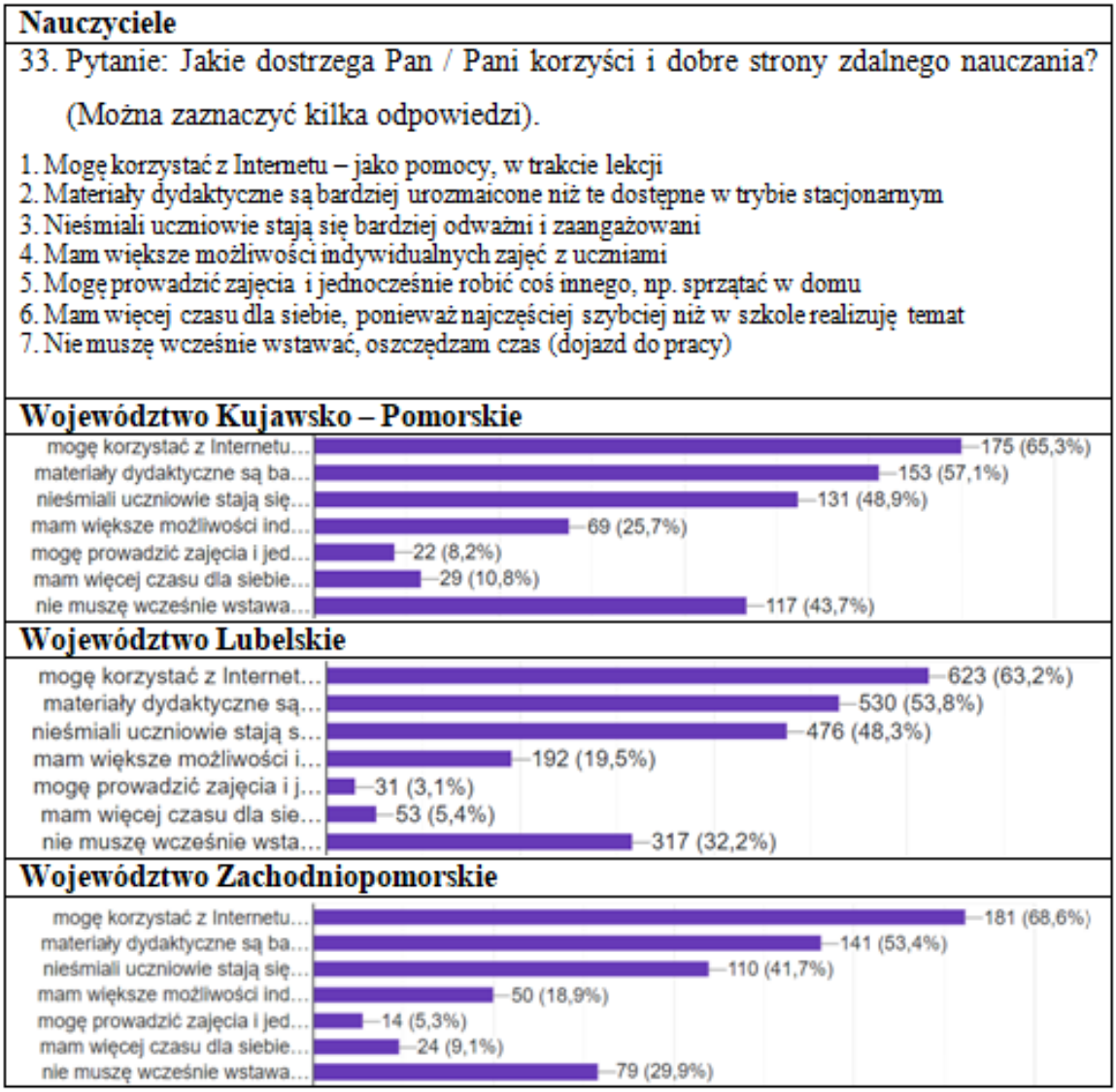
Wykres 6.31. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- ocena zdalnego nauczania (źródło: opracowanie własne)

Według nauczycieli, do trzech najczęściej występujących problemów podczas zdalnego nauczania zaliczono: zmęczenie spowodowane siedzeniem przed ekranem, podejście uczniów (zmęczenie) oraz problem natury technicznej jakim jest jakość połączenia internetowego uczniów. Najmniej problemu sprawiało tworzenie grup szkoleniowych. Znaczna ilość ankietowanych wskazała jako wyzwanie jakość własnego połączenia internetowego. Pośród badanych wystąpiła również grupa, która stwierdziła braki w umiejętności obsługi komputera i programów. Wyniki prezentuje poniższy wykres 6.32.



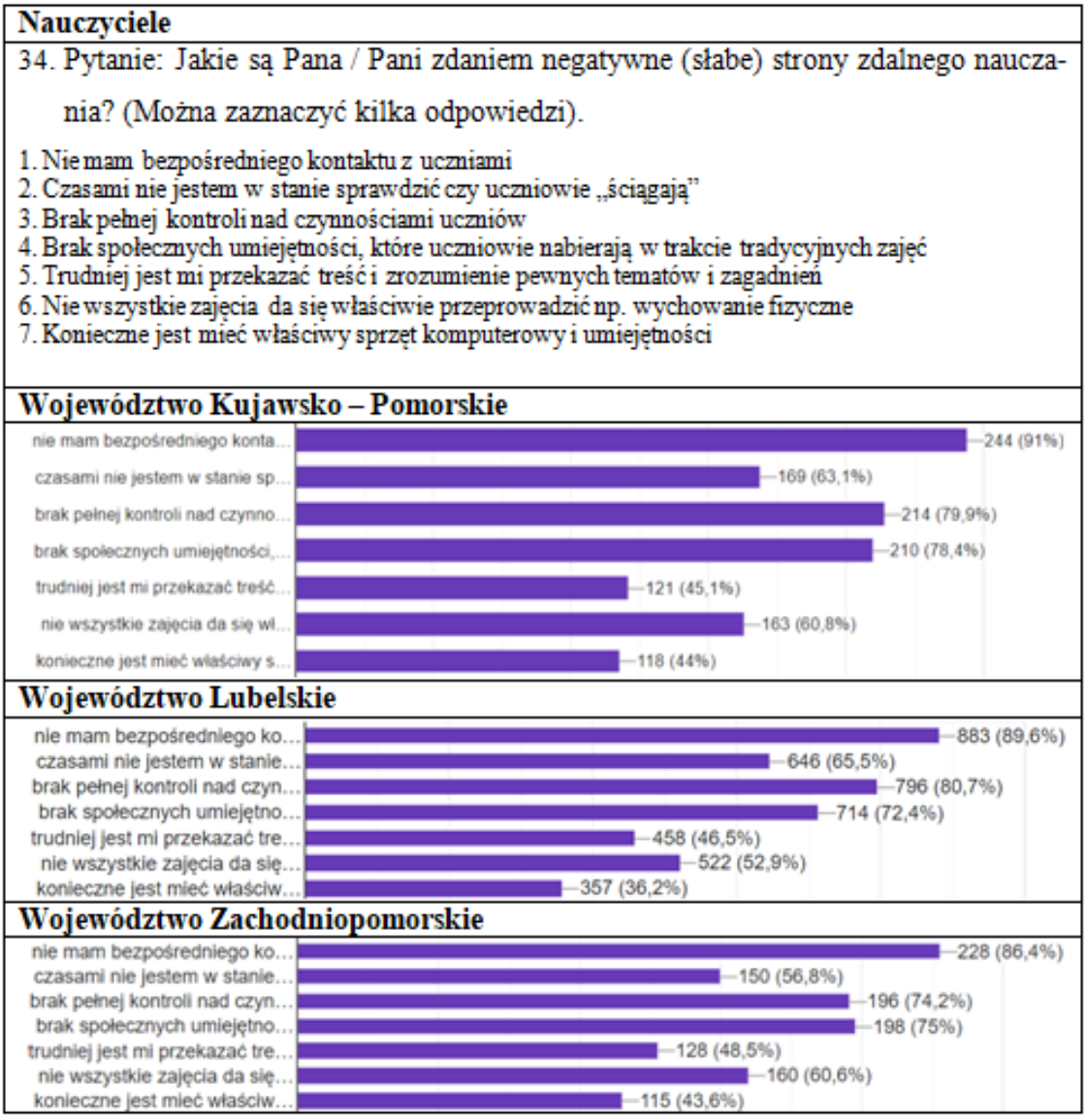
Wykres 6.32. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- problemy w trakcie zdalnego nauczania (źródło: opracowanie własne)

Zapytani o korzyści płynące ze zdalnego nauczania, badani nauczyciele za największą zgodnie wskazali- możliwość korzystania z Internetu jako pomocy w tracie prowadzenia zajęć. Dalej zostały zaznaczone materiały dydaktyczne, które przy wykorzystaniu nauczania zdalnego mogą być bardziej urozmaicone. Zauważono również większe zaangażowanie uczniów, którzy przy nauczaniu stacjonarnym byli nieśmiali oraz możliwość indywidualnego podejścia i prowadzenia indywidualnych zajęć z uczniami. Jeżeli mowa o korzyściach dotyczących nauczycieli, znaczna grupa opowiedziała się za oszczędnością własnego czasu oraz możliwością wykonywania innych czynności podczas prowadzenia zajęć.



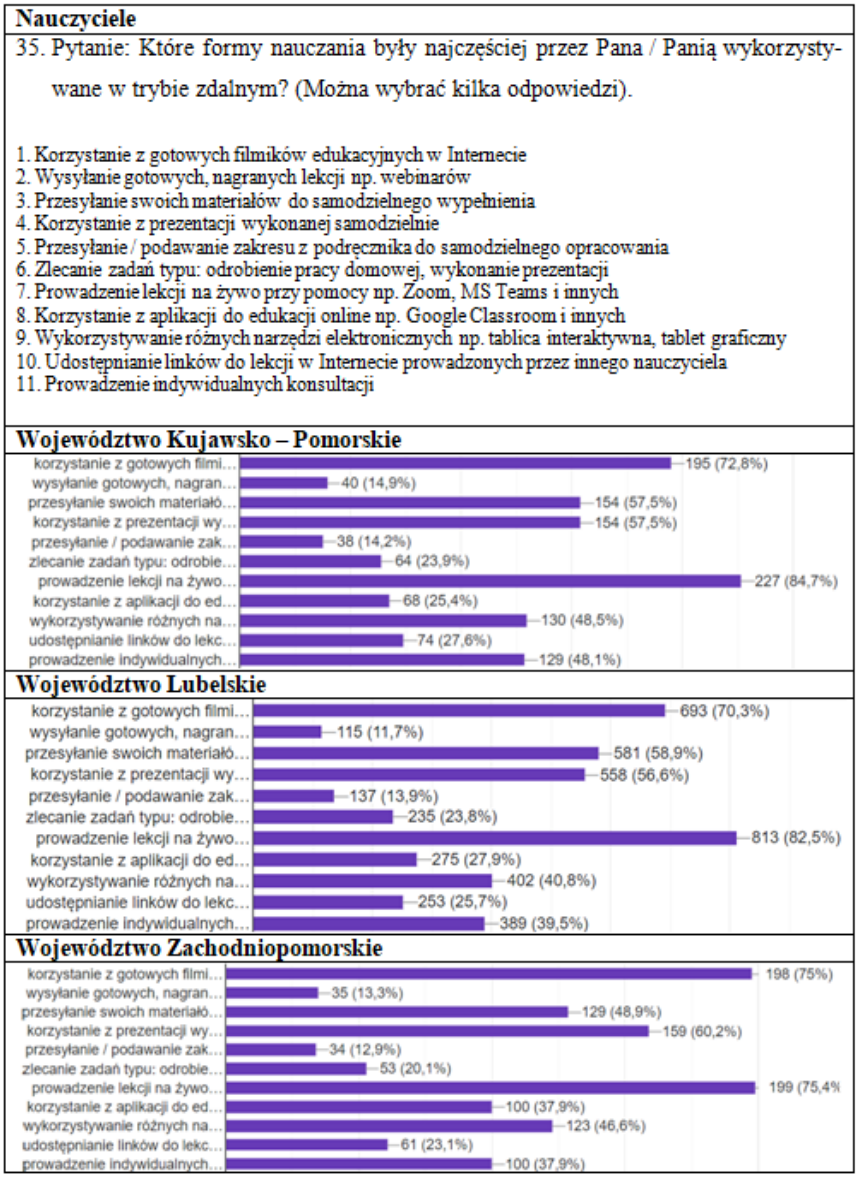
Wykres 6.33. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- korzyści w ramach zdalnego nauczania (źródło: opracowanie własne)

W odpowiedzi na pytanie nr 34 wśród negatywnych stron zdalnego nauczania za największą wadę uznano brak bezpośredniego kontaktu z uczniami. Kolejno, prawie na równi nauczyciele wymieniają brak kontroli nad tym co robią uczniowie w czasie zajęć oraz brak umiejętności społecznych, które uczniowie zdobywają podczas tradycyjnych zajęć stacjonarnych. Najrzadziej występującą wadą jest konieczność posiadania odpowiedniego sprzętu oraz umiejętności do prowadzenia zajęć zdalnych. Warto zaznaczyć, iż wspomniana wcześniej wada jest najrzadziej występującą, co wskazywało na nią aż 44% nauczycieli w woj. Kujawsko – Pomorskim, 43,6% w woj. Zachodniopomorskim oraz 36,2 % w woj. Lubelskim. Jak widać ilość głosów oddana na negatywne strony zdalnego nauczania jest wyższa niż w przypadku zalet.



Wykres 6.34. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- negatywne strony zdalnego nauczania (źródło: opracowanie własne)

Odpowiednie przygotowanie lekcji zdalnego nauczania wcale nie wymaga mniej wysiłku niż przygotowanie klasycznych stacjonarnych zajęć. Nauczyciele zapytani o formy nauczania stosowane podczas zajęć zdalnych w woj. Kujawsko – Pomorskim oraz Lubelskim wykazali, że prowadzili lekcje na żywo. Natomiast woj. Zachodniopomorskim wśród najczęściej stosowanych form na równi zostały wskazane lekcje na żywo oraz wykorzystanie gotowych filmów edukacyjnych. Ponad połowa badanych odpowiedziała, że stosuje wykonane osobiście prezentacje oraz swoje materiały przesłane uczniom do wypełnienia (w woj. Zachodniopomorskim tej odpowiedzi udzieliło 48,9% badanych). Najmniejszą popularnością pośród badanych cieszyło się wysyłanie gotowych nagranych wcześniej lekcji oraz przesyłanie określonego zakresu do samodzielnego opracowania.



Wykres 6.35. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- formy zdalnego nauczania (źródło: opracowanie własne)

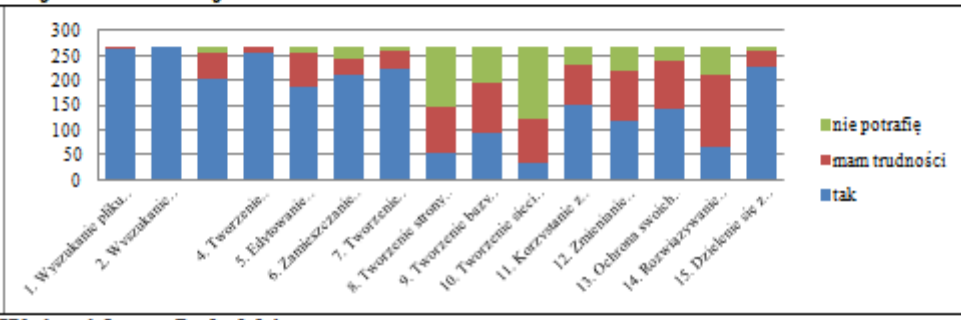
Pytanie numer 36 dotyczyło samooceny umiejętności wykonywania określonych zadań na komputerze. Analizując poniższe wykresy (6.36.) możemy zauważyć, że najmniej problemu badanym sprawia wyszukiwanie plików lub informacji. Z pewnymi trudnościami nauczyciele potrafią m.in. instalować aplikację, tworzyć dokumenty czy też udostępniać dane innym użytkownikom. Jeszcze poważniejsze wyzwanie nauczyciele mają przy zmianie bardziej złożonych ustawień komputera (antywirus, rozwiązywanie problemów technicznych) oraz obsłudze np. arkusza kalkulacyjnego. Natomiast największą niewiedzę ankietowanych można zaobserwować w obszarze dotyczącym bardziej złożonych zagadnień jakim jest np. tworzenie stron internetowych, sieci komputerowych lub baz danych. Wyniki we wszystkich województwach były zbliżone.

Nauczyciele

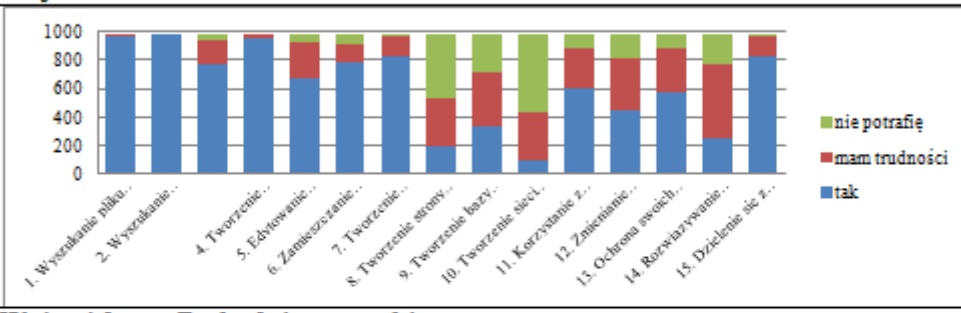
36. Pytanie: Jak ocenia Pan / Pani swoje umiejętności wykonywania poniższych zadań przy komputerze? (Proszę odnieść się do <u>każdego</u> z podpunktów).

1. Wyszukanie pliku na komputerze.
2. Wyszukanie informacji w Internecie
3. Zainstalowanie aplikacji / gry
4. Tworzenie dokumentów (np. wypracowań, sprawozdań)
5. Edytowanie fotografii cyfrowej / grafikicyberprzemocy
6. Zamieszczanie zdjęć, tekstów na portalu społecznościowym
7. Tworzenie prezentacji multimedialnej
8. Tworzenie strony internetowej
9. Tworzenie bazy danych
10. Tworzenie sieci komputerowej
11. Korzystanie z arkusza kalkulacyjnego
12. Zmienianie ustawień komputera (usprawnienie jego pracy)
13. Ochrona swoich danych np. poprzez zaporę, antywirusa
14. Rozwiązywanie problemów technicznych
15. Dzielenie się z innymi informacjami, danymi, plikami

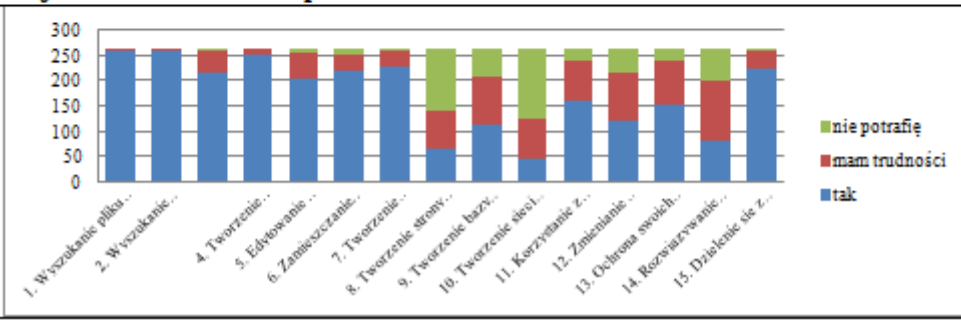
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

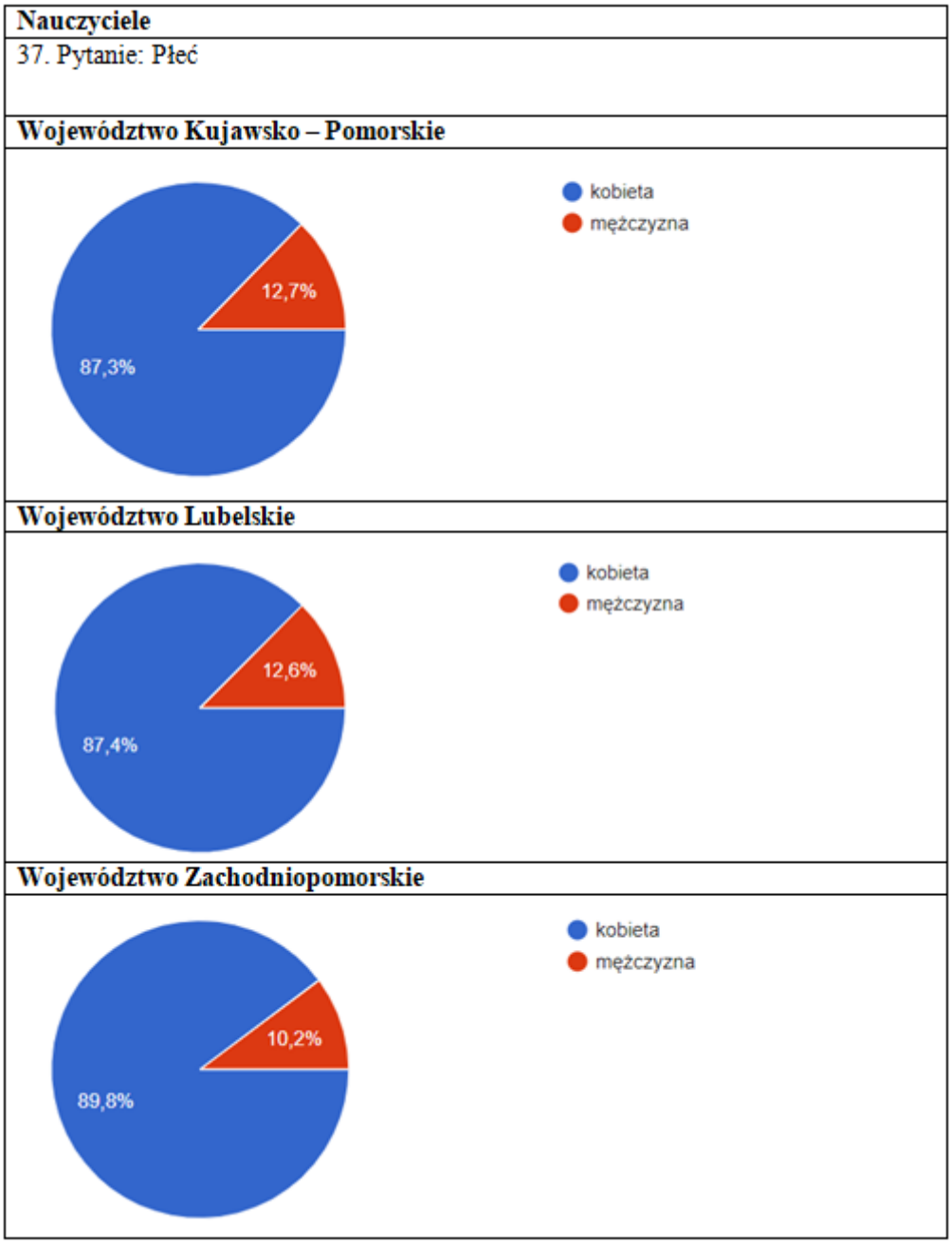


Województwo Zachodniopomorskie



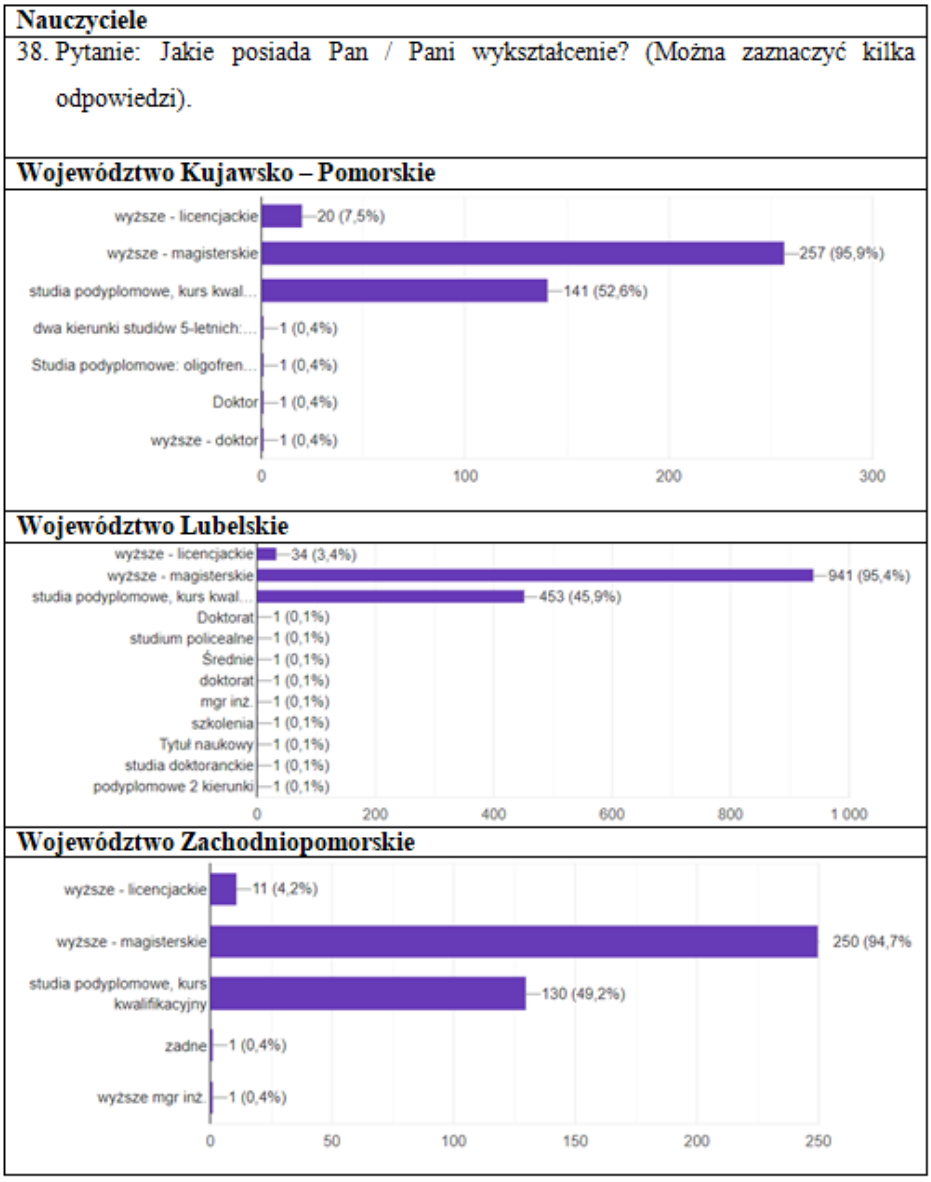
Wykres 6.36. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- ocena własnych umiejętności przy komputerze (źródło: opracowanie własne)

W pytaniu numer 37 została określona płeć badanych. Jak widać na poniższych wykresach, w woj. Kujawsko – Pomorskim w badaniu udział wzięło 87,3% kobiet oraz 12,7% mężczyzn. W woj. Lubelskim procentowy rozkład był bardzo zbliżony. Kobiety stanowiły 87,3% badanych a mężczyźni 12,6%. Natomiast w woj. Zachodniopomorskim grupa mężczyzn stanowiła 10,2% a kobiet 89,8%.



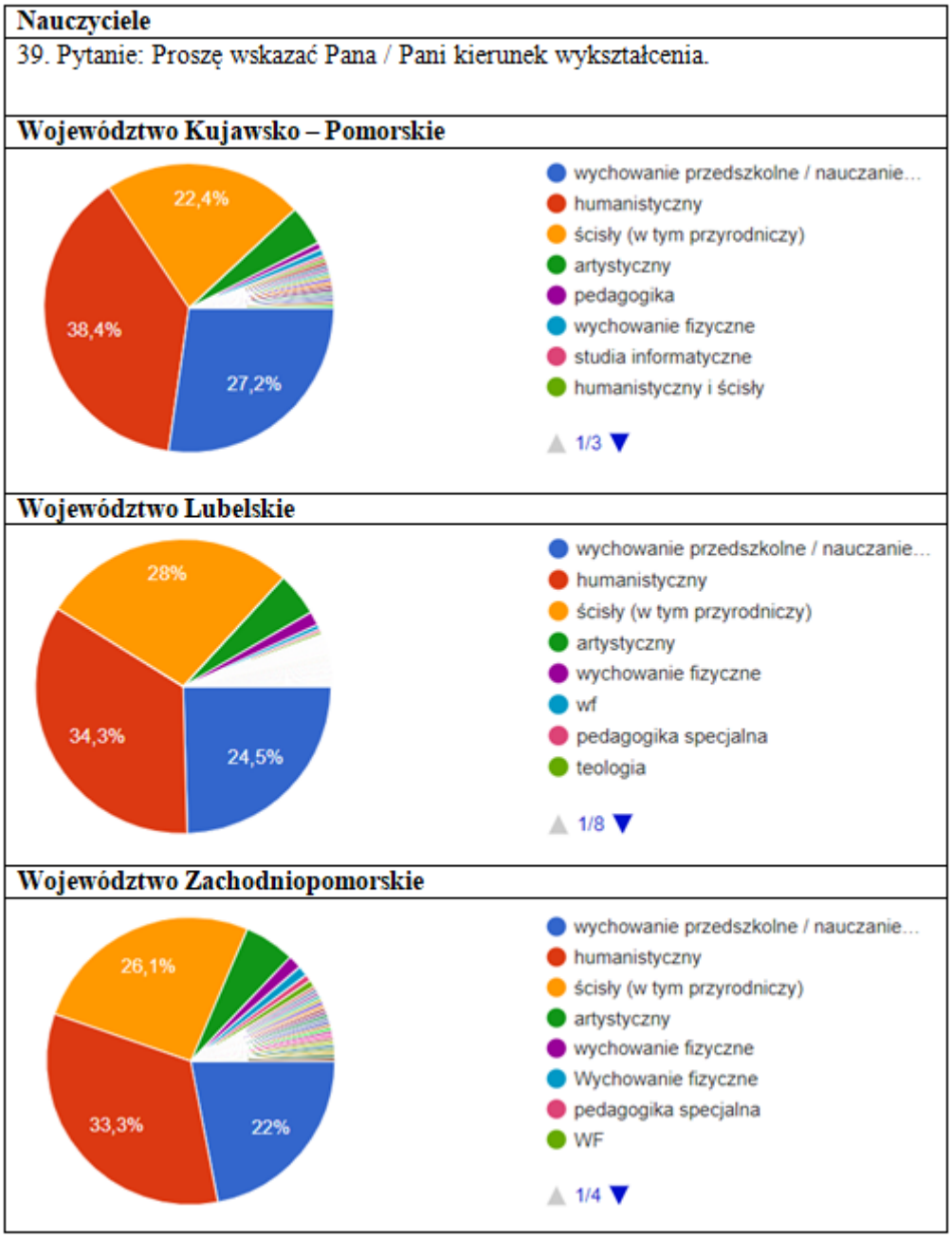
Wykres 6.37. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wskazanie płci badanego (źródło: opracowanie własne)

Kolejne pytanie dotyczyło wykształcenia badanych. W każdym z trzech województw wyłoniły się trzy zasadnicze grupy. Pierwsza z nich to osoby posiadające wykształcenie wyższe – magisterskie, druga to osoby, które ukończyły studia podyplomowe, a trzecia to osoby z wykształceniem wyższym - licencjackim. Przynależność do pierwszej grupy wykazało 95,9% nauczycieli z woj. Kujawsko – Pomorskiego, 95,4% z woj. Lubelskiego oraz 94,7% z woj. Zachodniopomorskiego. Ukończenie studiów podyplomowych sygnalizuje 52,6% ankietowanych z woj. Kujawsko – Pomorskiego, 45,9% z Lubelskiego oraz 49,2 z woj. Zachodniopomorskiego. Natomiast posiadanie wykształcenia wyższego – licencjackiego zaobserwować możemy u 7,5% badanych z woj. Kujawsko – Pomorskiego, 3,4% z woj. Lubelskiego i 4,2% z Zachodniopomorskiego.



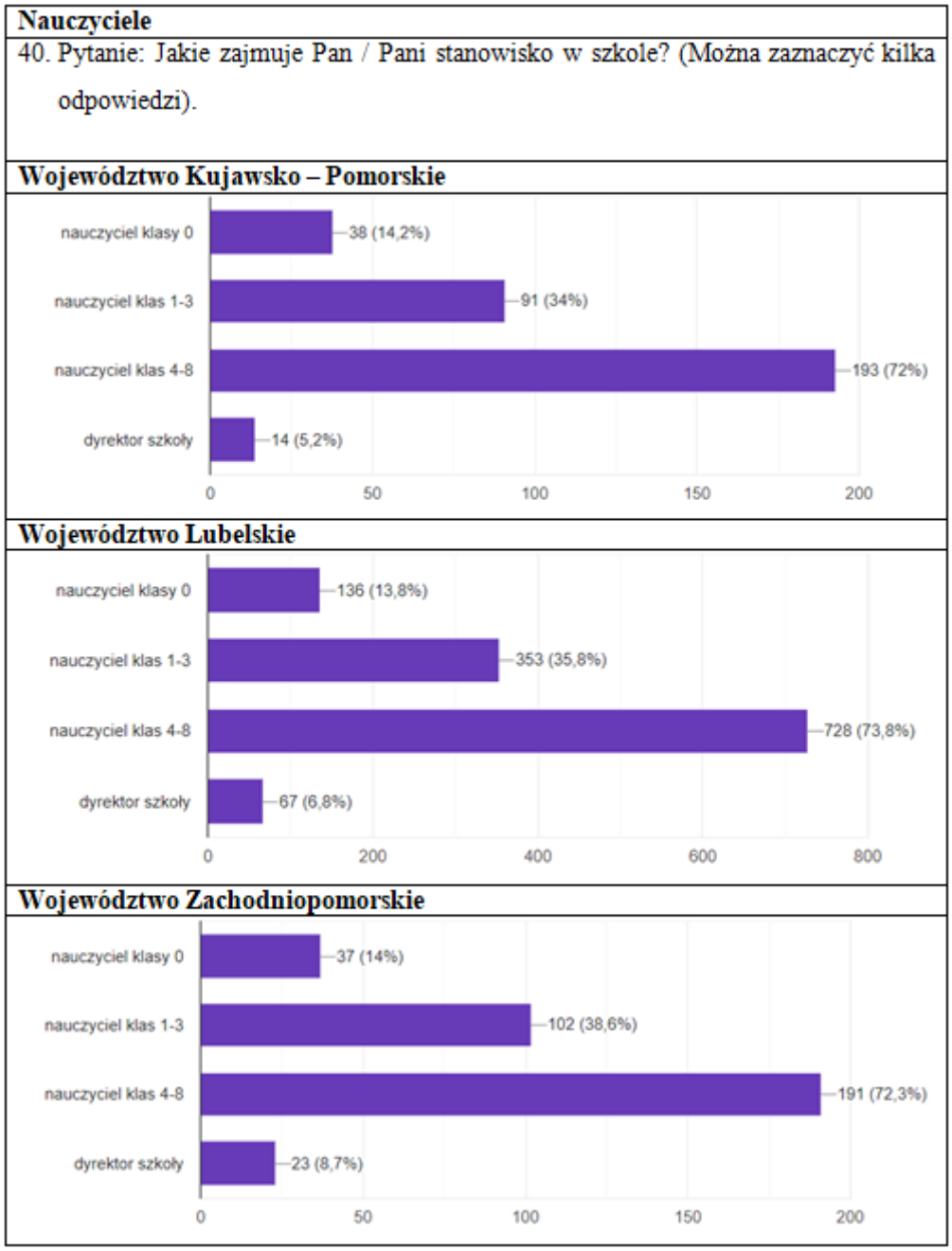
Wykres 6.38. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wskazanie wykształcenia (źródło: opracowanie własne)

W następnym pytaniu ankietowani zostali zapytani o kierunek ich wykształcenia. W każdym z badanych województw możemy zaobserwować trzy główne grupy, humanistyczną, ścisłą oraz wychowania przedszkolnego. Najbardziej liczną stanowią osoby z wykształceniem humanistycznym (między 33% a 38,4%). Wykształcenie ścisłe deklaruje pomiędzy 22% a 28% nauczycieli. Natomiast jako wychowawca przedszkolny określa się od 22% do 27,2% ankietowanych. Pojawiły się również inne mniejsze grupy wykształcone m.in. w kierunku wychowania fizycznego, artystycznym, pedagogicznym i informatycznym.



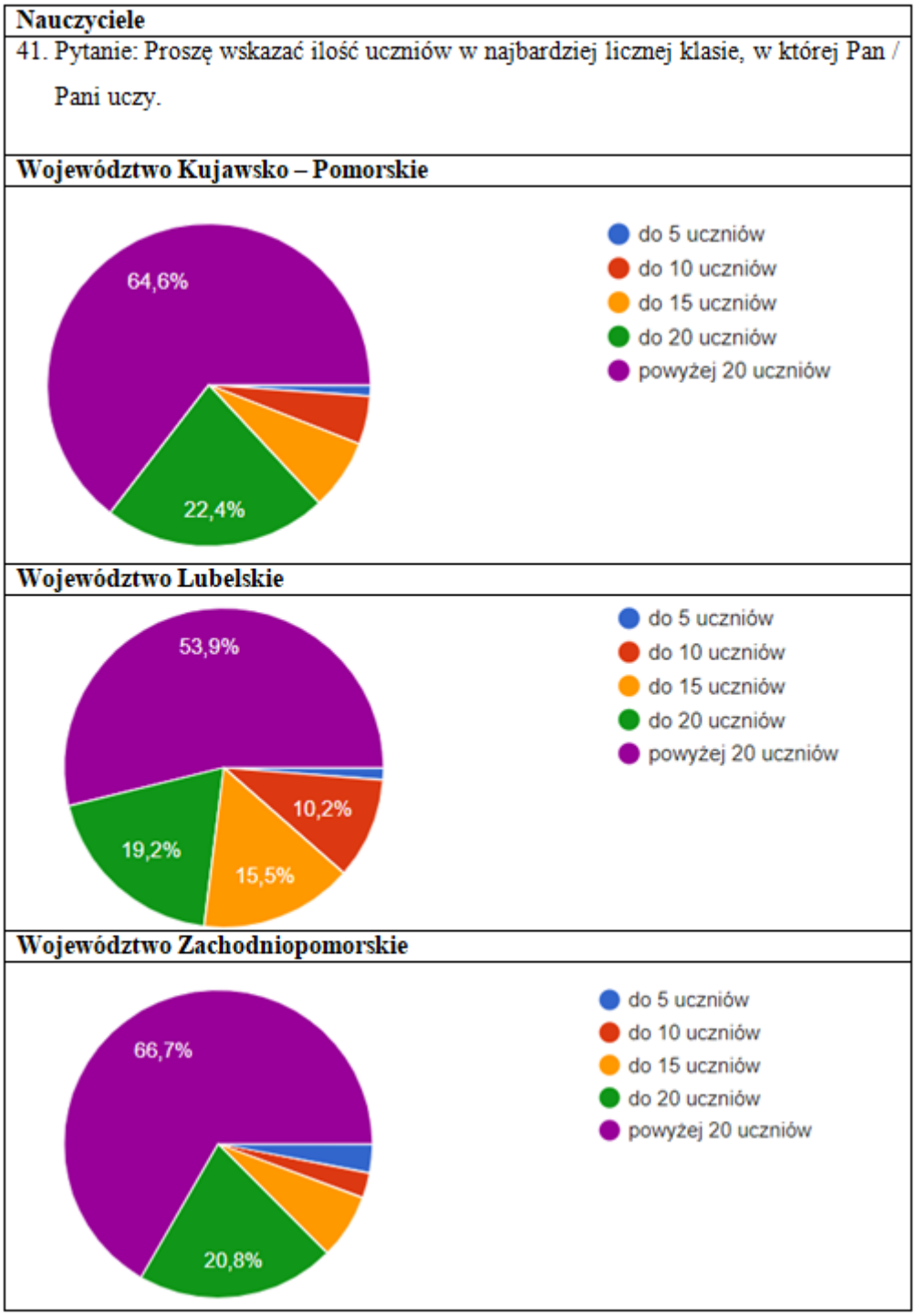
Wykres 6.39. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wskazanie kierunku wykształcenia (źródło: opracowanie własne)

Jak można zaobserwować na poniższych wykresach najbardziej liczną grupę pośród badanych w każdym z województw stanowią nauczyciele klas 4-8 (około 72%). Nauczyciele klas 1-3 tworzą od 34% (woj. Kujawsko – Pomorskie) do 38,6% (woj. Zachodniopomorskie) próby badawczej. Udział nauczycieli „zerówek" oscyluje w okolicach 14%. Zaś największy procentowy udział dyrektorów występuje w woj. Zachodniopomorskim (8,7%), a najmniejszy w Kujawsko – Pomorskim (5,2%).



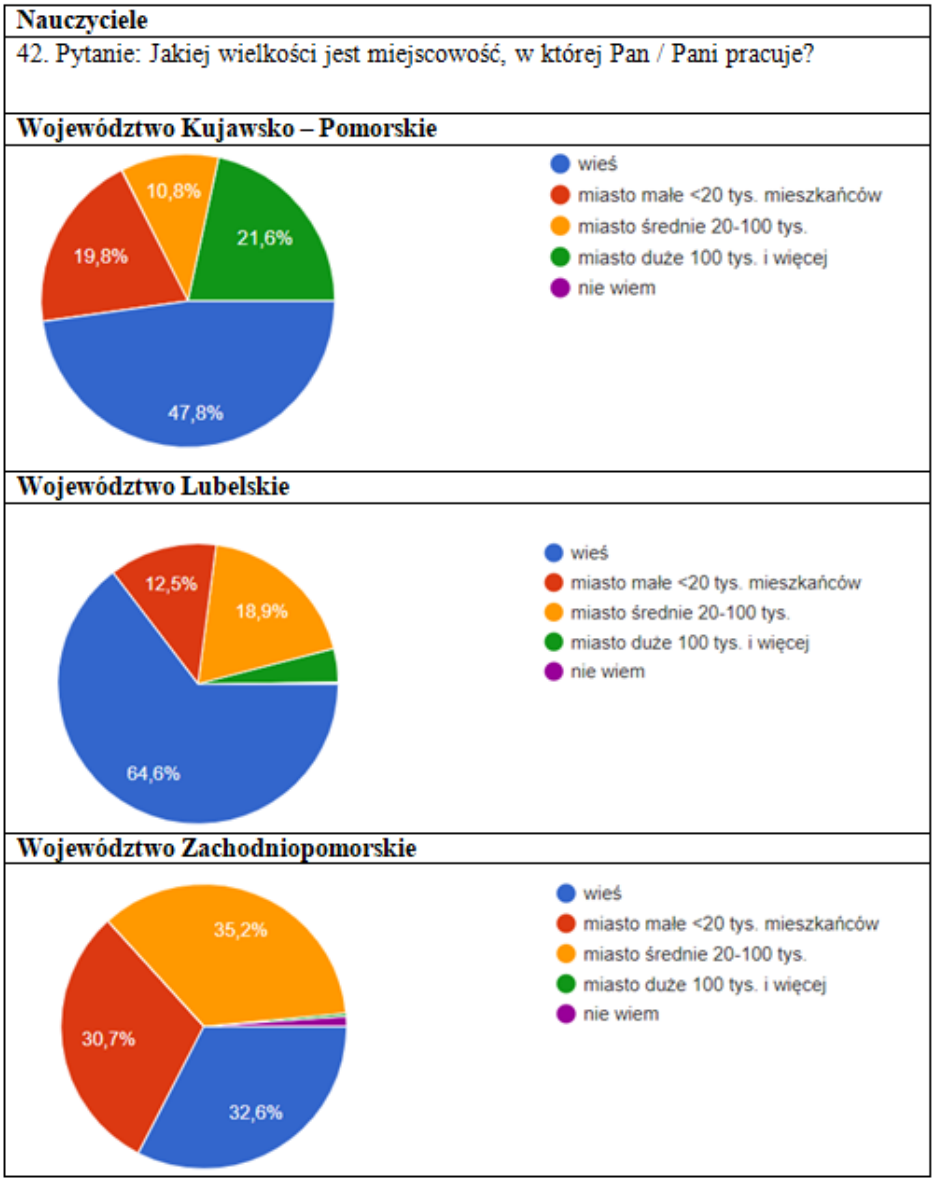
Wykres 6.40. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- zajmowane stanowisko służbowe (źródło: opracowanie własne)

Wskazując największą liczebność klasy, ponad połowa nauczycieli w każdym z województw odpowiedziała, że prowadzi zajęcia w klasach liczących ponad dwudziestu uczniów. W woj. Zachodniopomorskim takiej odpowiedzi udzieliło aż 66,7% badanych. Około 20% pedagogów kształci w klasach do 20 osób.



Wykres 6.41. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- najbardziej liczna klasa (źródło: opracowanie własne)

Ostatnie pytanie dotyczące respondentów odnosiło się do ich miejsca zamieszkania. Analizując wyniki z poszczególnych województw możemy zauważyć, że w woj. Kujawsko – Pomorskim wieś zamieszkuje 47,8% badanych, miasto powyżej 100 tyś mieszkańców – 21,6%, miasto średniej wielkości 10,8% oraz małe miasto 19,8%. Zbliżony rozkład wyników prezentuje woj. Lubelskie. Mieszkańcy wsi obejmują 64,4% ankietowanych, dużych miast – 4%, średnich 18,9% oraz małych 12.5%. W woj. Zachodniopomorskim uwypukla się podział na trzy części. Mieszkańcy wsi to 30,7% nauczycieli, średnich miast 35,2%, natomiast małych 30,7%. W tym województwie wystąpił również niewielki odsetek mieszkańców dużych miast oraz osób niepotrafiących określić swojego miejsca zamieszkania.



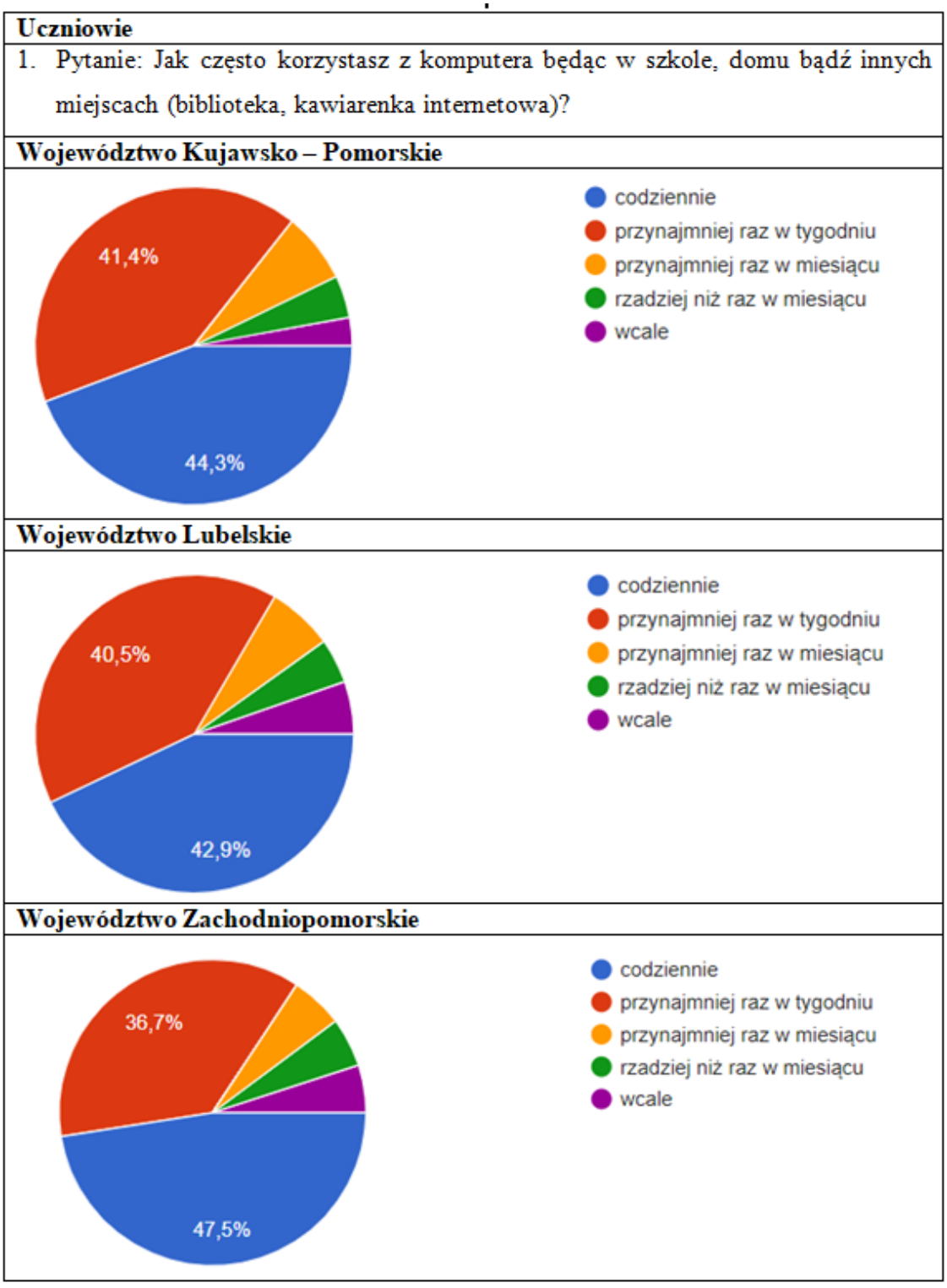
Wykres 6.42. Odpowiedzi ankietowanych nauczycieli z trzech wybranych województw- wielkość miejscowości (źródło: opracowanie własne)

Analiza wyników badań wśród nauczycieli:

- niespełna 1/3 respondentów pomimo rozwoju aplikacji zabezpieczających, nadal zapisuje własne hasła np. w zeszycie, tak więc metody tradycyjne wciąż są najbardziej popularne i obowiązujące;
- bezpieczny adres strony www jest w stanie wskazać nieco ponad 40 % badanych, toteż zdecydowanie za mało biorąc pod uwagę zmieniające się środowisko cyberprzestrzeni;
- kopie zapasowe plików wykonuje ok. 25% pedagogów, występują pewne różnice w zakresie regularności czy ilości i rodzajów kopiowanych danych;
- poprawność i autentyczność adresu www- 50%, co stanowi podstawę do twierdzenia, iż część z nich mogłaby stać się ofiarami potencjalnego ataku na bankowość internetową;
- prywatne dane na komputerze w ramach jedynie hasła podczas włączania komputera stosuje połowa uzupełniających ankietę, ponad 33 % używa specjalnego programu jako zabezpieczenie komputera, co może stanowić przesłankę do wzrostu świadomości użytkowników w tym zakresie;
- około 40 % badanych odkłada aktualizacje swoich urządzeń na później, nie posiadając wiedzy o zaletach regularnych aktualizacji i ich wpływu na stabilność oraz bezpieczeństwo pracy danego sprzętu;
- pozytywny aspekt stanowić mogą odpowiedzi na pytanie dotyczące reakcji na wiadomość od znajomego *(social media*), ponieważ ok. 80 % adresatów komunikatu zawierającego podejrzany link- będzie ostrożna i nie zaryzykuje przejścia pod nieznany adres internetowy;
- udostępnianie jak najmniejszej ilości informacji o sobie w mediach społecznościowych ok. 60%, niepokojącym jest jednak fakt występowania grupy pedagogów, którzy pomimo korzystania z mediów społecznościowych nie są w stanie sprawdzić jakie są udostępniane przez nich dane lub też po prostu upubliczniają wszystkie informacje;
- najbardziej rozpoznawalne cyberzagrożenia: stalking, spam oraz koń trojański, zastanawia jednak niewystarczająca świadomość czym jest zagrożenie phishingowe;
- Internet- za niebezpieczne miejsce uważa większość badanych (prawie 90% sumując odpowiedzi jak najbardziej twierdzące i skłaniające się do nich);

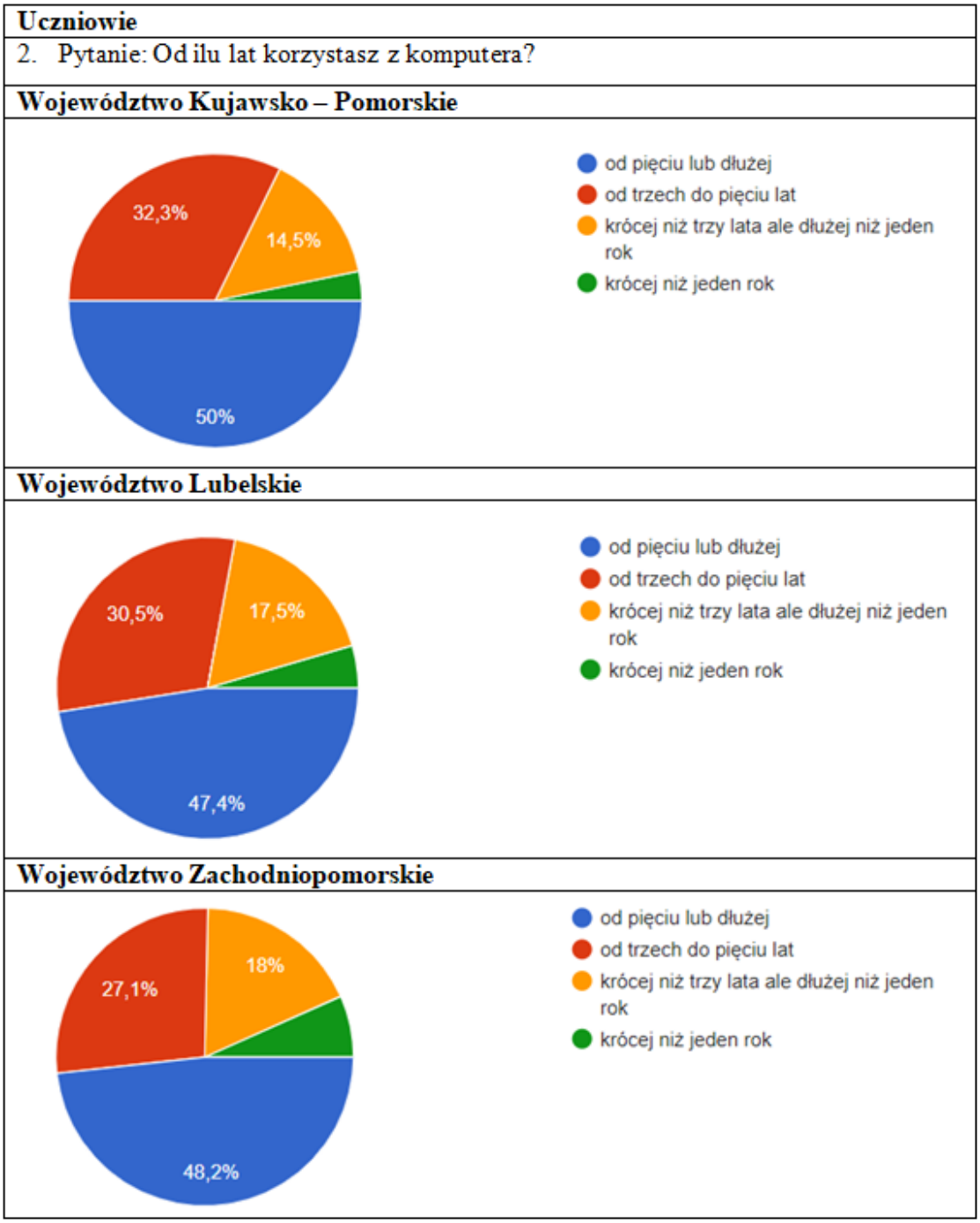
- najczęstsze problemy podczas zdalnego nauczania: zmęczenie spowodowane koniecznością pracy przed ekranem monitora; podejście uczniów – byli po prostu zmęczeni; słabe połączenie internetowe uczniów;
- do najważniejszych zalet cyfrowej edukacji zaliczono możliwość korzystania z sieci podczas zajęć, większe zaangażowanie nieśmiałych uczniów czy oszczędność czasu związaną m.in. z przemieszczeniem do miejsca pracy;
- najmniejszą popularnością pośród badanych cieszyło się wysyłanie gotowych nagranych wcześniej lekcji oraz przesyłanie określonego zakresu do samodzielnego opracowania;
- najmniej problemów sprawia nauczycielom wyszukanie informacji bądź pliku w Internecie; poważniejsze wyzwanie stanowi rozwiązywanie problemów technicznych czy obsługa arkusza kalkulacyjnego, zaś największe- tworzenie baz danych czy stron internetowych, co zdaniem autora jest naturalnym zjawiskiem biorąc pod uwagę najczęściej nietechniczne wykształcenie pedagogów;
- zdecydowana większość badanych- wykształcenie wyższe magisterskie (95%).

Z komputera korzysta codziennie ponad 40% badanych uczniów, najwięcej, ponieważ 47,5% w województwie Zachodniopomorskim. Wyniki w województwach są zbliżone.



Wykres 6.43. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- częstotliwość korzystania z komputera (źródło: opracowanie własne)

Najdłużej z komputera korzystają uczniowie woj. Kujawsko-Pomorskiego (połowa badanych), jest to pięć lat lub dłużej, ponadto odpowiedź trzech do pięciu lat została wskazana przez 32 %, co również powoduje, iż woj. Kujawsko-Pomorskie zajmuje pierwsze miejsce. Podsumowując, najdłużej korzystającymi z komputera użytkownikami są uczniowie woj. Kujawsko-Pomorskiego. Najwięcej młodych użytkowników (krócej niż jeden rok) dotyczy woj. Zachodniopomorskiego.



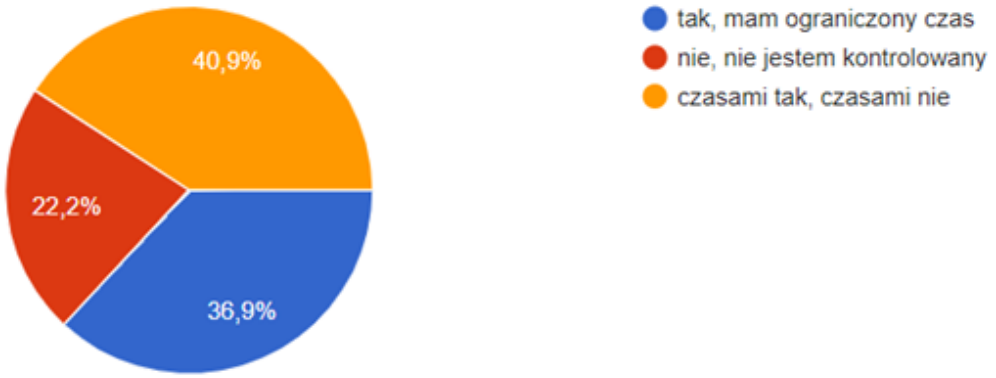
Wykres 6.44. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- długość korzystania z komputera (źródło: opracowanie własne)

Ponownie, woj. Kujawsko-Pomorskie na pierwszej lokacie w kwestii kontroli rodzicielskiej nad czasem spędzanym przez ich dzieci przed komputerem (wykres 6.45.) Blisko 37% badanych jest kontrolowana i ma ograniczony czas (woj. Kujawsko-Pomorskie). Najmniej korzystnie sytuacja wygląda w woj. Zachodniopomorskim, ponieważ blisko ¼ badanych uczniów nie jest w jakikolwiek sposób ograniczany czas przebywania przed komputerem przez rodziców (opiekunów). Te wartości są podstawą do stwierdzenia, iż rodzice (opiekuni) powinni poczuć się bardziej odpowiedzialni i sprawować większą kontrolę nad ilością czasu spędzanego przy komputerze przez dzieci.

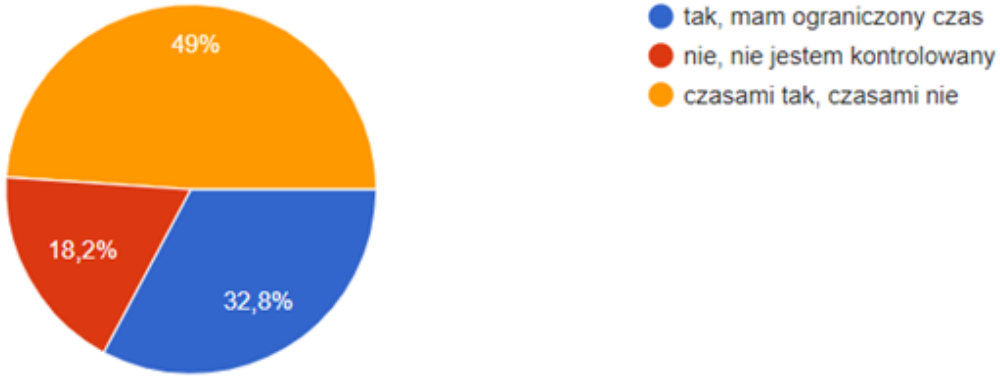
Uczniowie

3. Pytanie: Czy rodzice / opiekuni mają nadzór nad ilością Twojego czasu spędzanego przed komputerem?

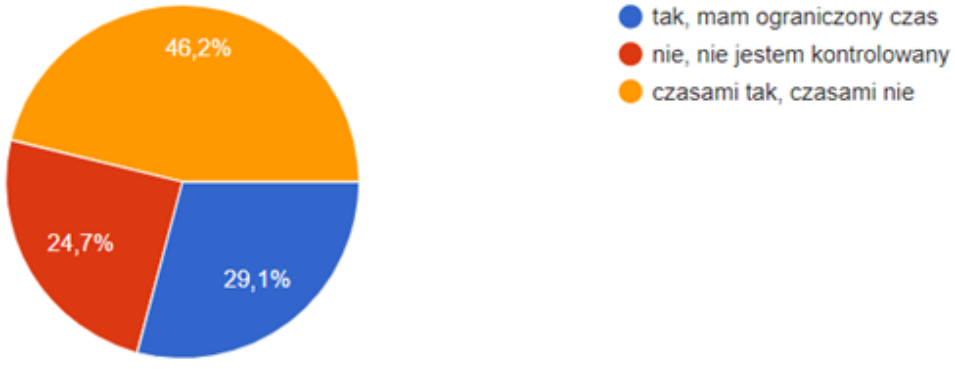
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

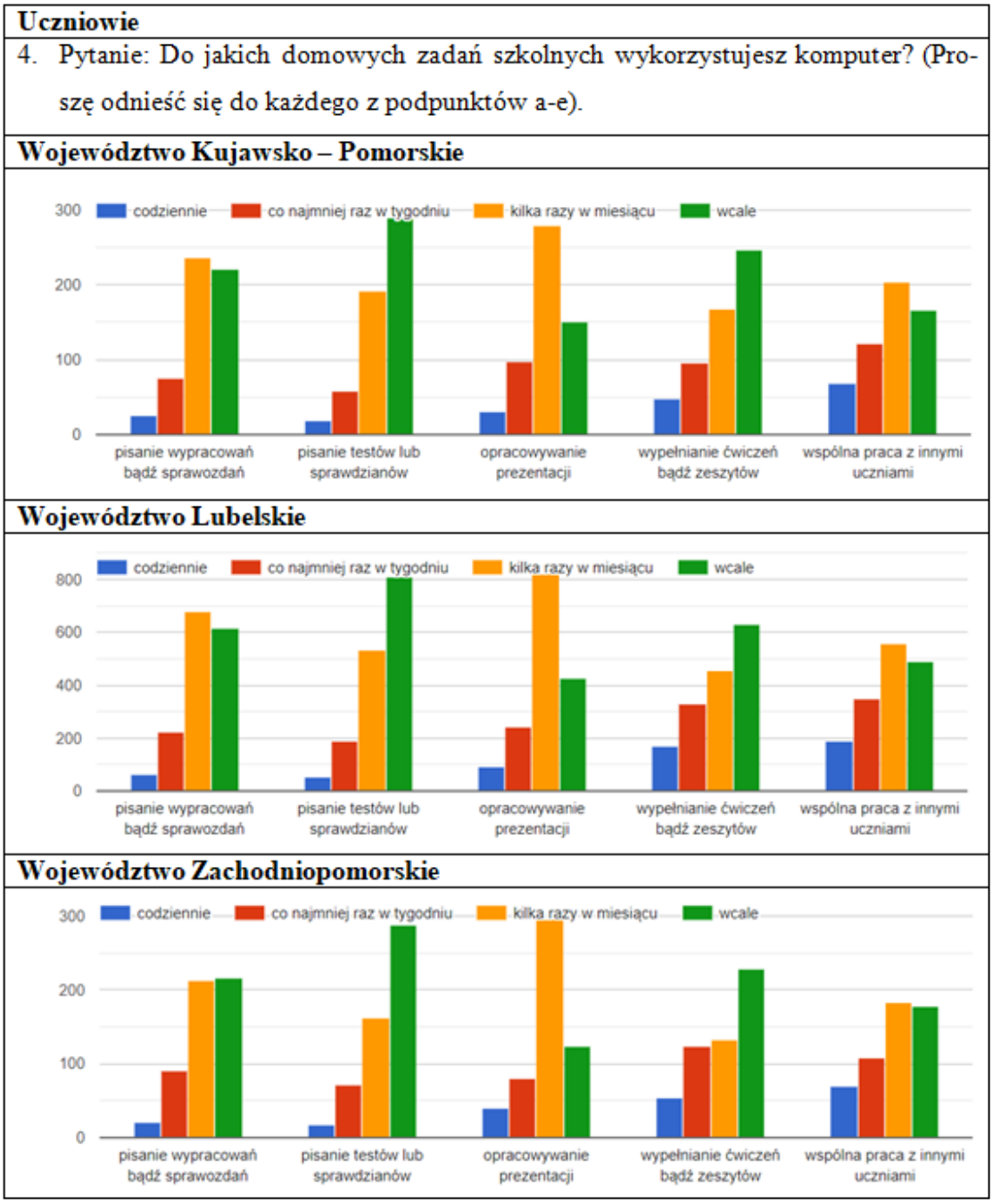


Województwo Zachodniopomorskie



Wykres 6.45. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- nadzór nad czasem przy komputerze (źródło: opracowanie własne)

Z wykresu 6.46. wynika, iż komputer najczęściej (codziennie) wykorzystywany jest do wspólnej pracy z innymi uczniami. Uczniowie co najmniej raz w tygodniu wypełniają ćwiczenia bądź zeszyty. Opracowywanie prezentacji odbywa się kilka razy w miesiącu. Wyniki we wszystkich województwach są zbieżne.



Wykres 6.46. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- wykorzystanie komputera (źródło: opracowanie własne)

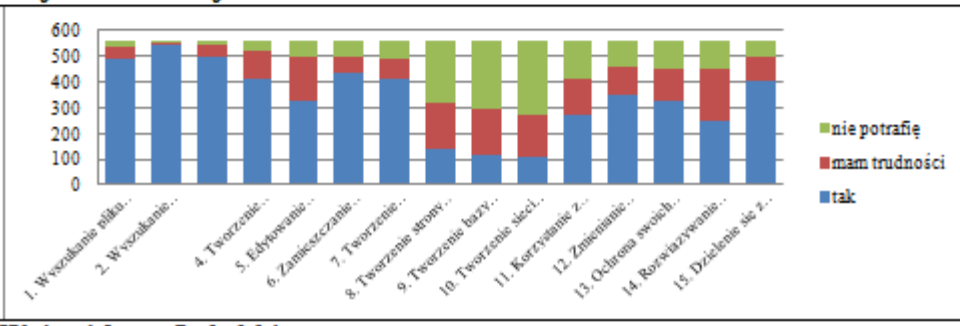
Zdecydowana większość uczniów potrafi: wyszukać plik na komputerze; wyszukać informacje w Internecie; zainstalować gry; aplikacje; tworzyć dokumenty (np. wypracowania, sprawozdania); zamieszczać zdjęcia; teksty na portalach społecznościowych oraz dzielić się z innymi informacjami i plikami. Trudności pojawiają się podczas edytowania fotografii cyfrowej / grafiki; tworzenia prezentacji multimedialnej; zmieniania ustawień komputera (usprawnienie jego pracy); ochrony swoich danych np. poprzez zaporę, antywirusa; korzystania z arkusza kalkulacyjnego. Największe wyzwanie stanowi dla uczniów: rozwiązywanie problemów technicznych; tworzenie strony internetowej; tworzenie bazy danych; tworzenie sieci komputerowej.

Uczniowie

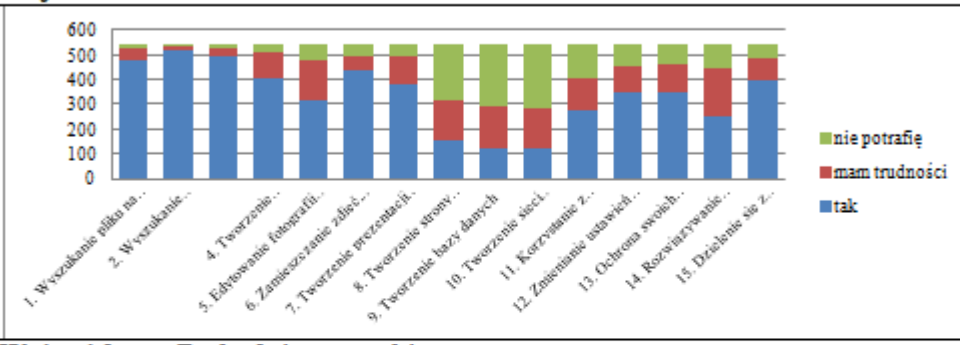
5. Pytanie: Jak oceniasz swoje umiejętności wykonywania poniższych zadań przy komputerze? (Proszę odnieść się do <u>każdego</u> z podpunktów).

1. Wyszukanie pliku na komputerze
2. Wyszukanie informacji w Internecie
3. Zainstalowanie aplikacji / gry
4. Tworzenie dokumentów (np. wypracowań, sprawozdań)
5. Edytowanie fotografii cyfrowej / grafiki
6. Zamieszczanie zdjęć, tekstów na portalu społecznościowym
7. Tworzenie prezentacji multimedialnej
8. Tworzenie strony internetowej
9. Tworzenie bazy danych
10. Tworzenie sieci komputerowej
11. Korzystanie z arkusza kalkulacyjnego
12. Zmienianie ustawień komputera (usprawnienie jego pracy)
13. Ochrona swoich danych np. poprzez zaporę, antywirusa
14. Rozwiązywanie problemów technicznych
15. Dzielenie się z innymi informacjami, danymi, plikami

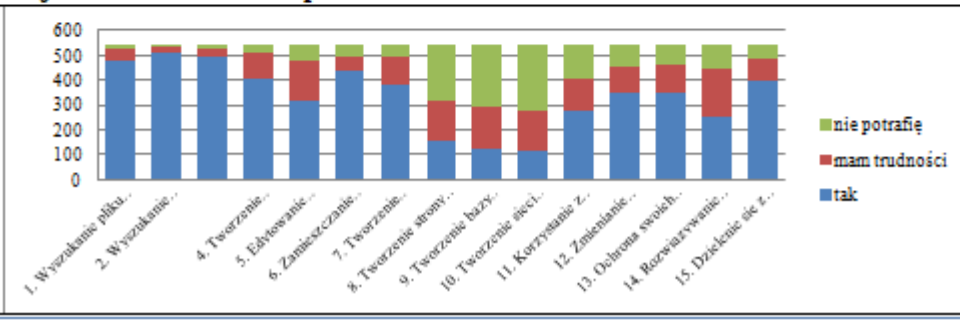
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

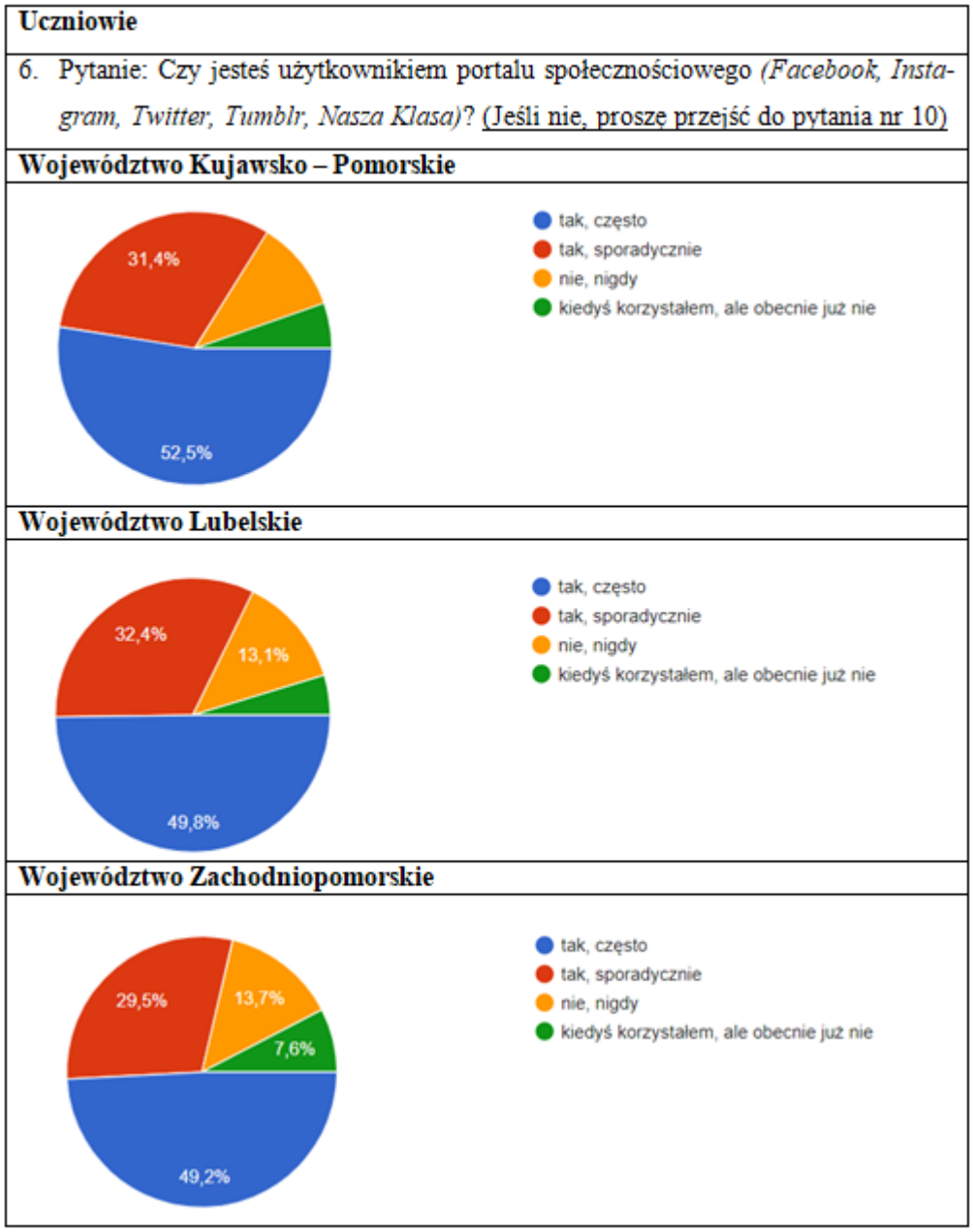


Województwo Zachodniopomorskie



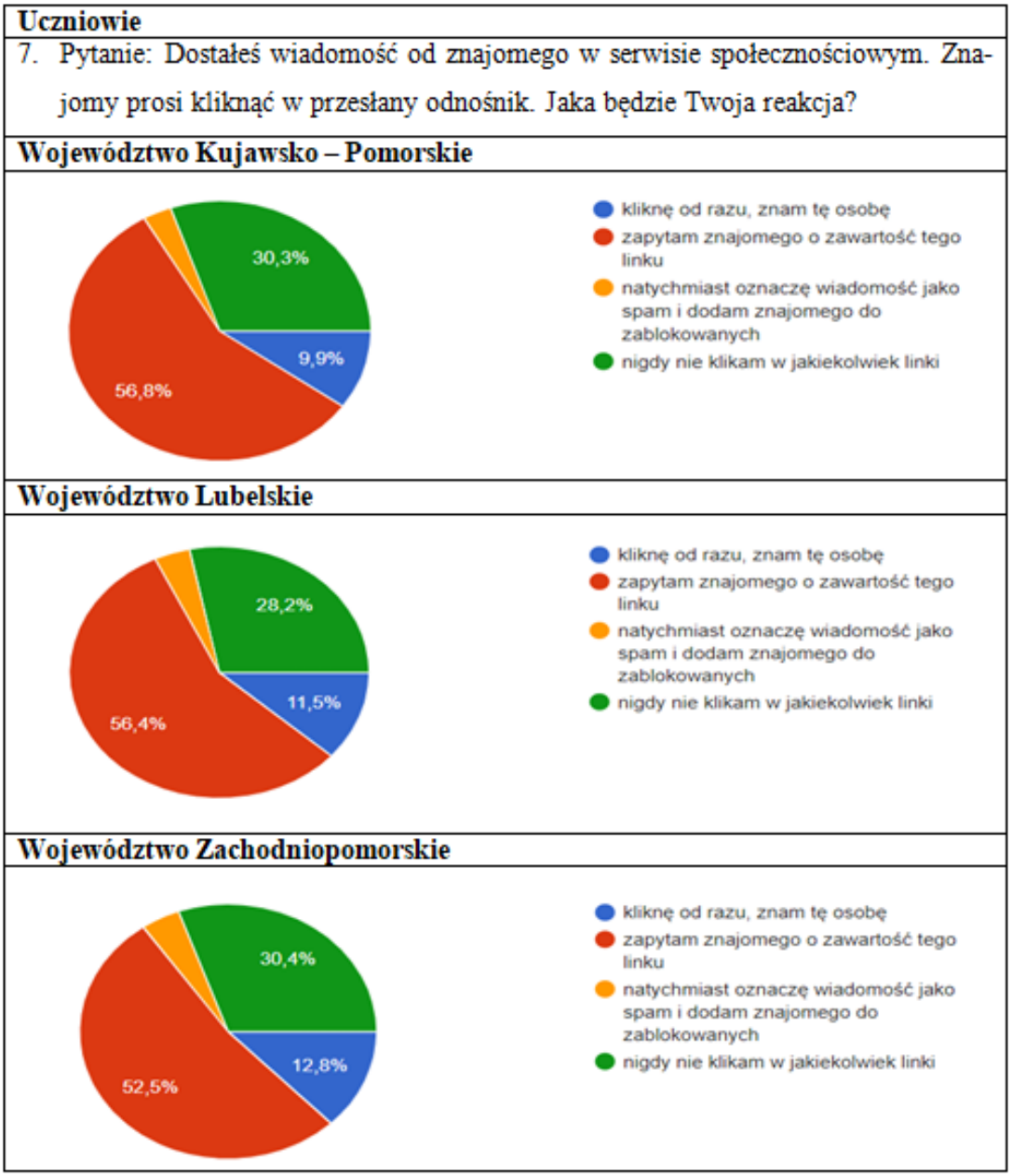
Wykres 6.47. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- umiejętności pracy przy komputerze (źródło: opracowanie własne)

Około 80% badanych jest użytkownikiem portalu społecznościowego (najwięcej woj. Kujawsko-Pomorskie). Połowa badanych często korzysta z *social media*. Kilkanaście procent badanych nigdy nie korzystało z żadnego z portali społecznościowych. Dowodzi to, iż obecnie znacząca część uczniów posługuje się serwisami społecznościowymi i jest tam często aktywna. Informacje prezentuje wykres 6.48.



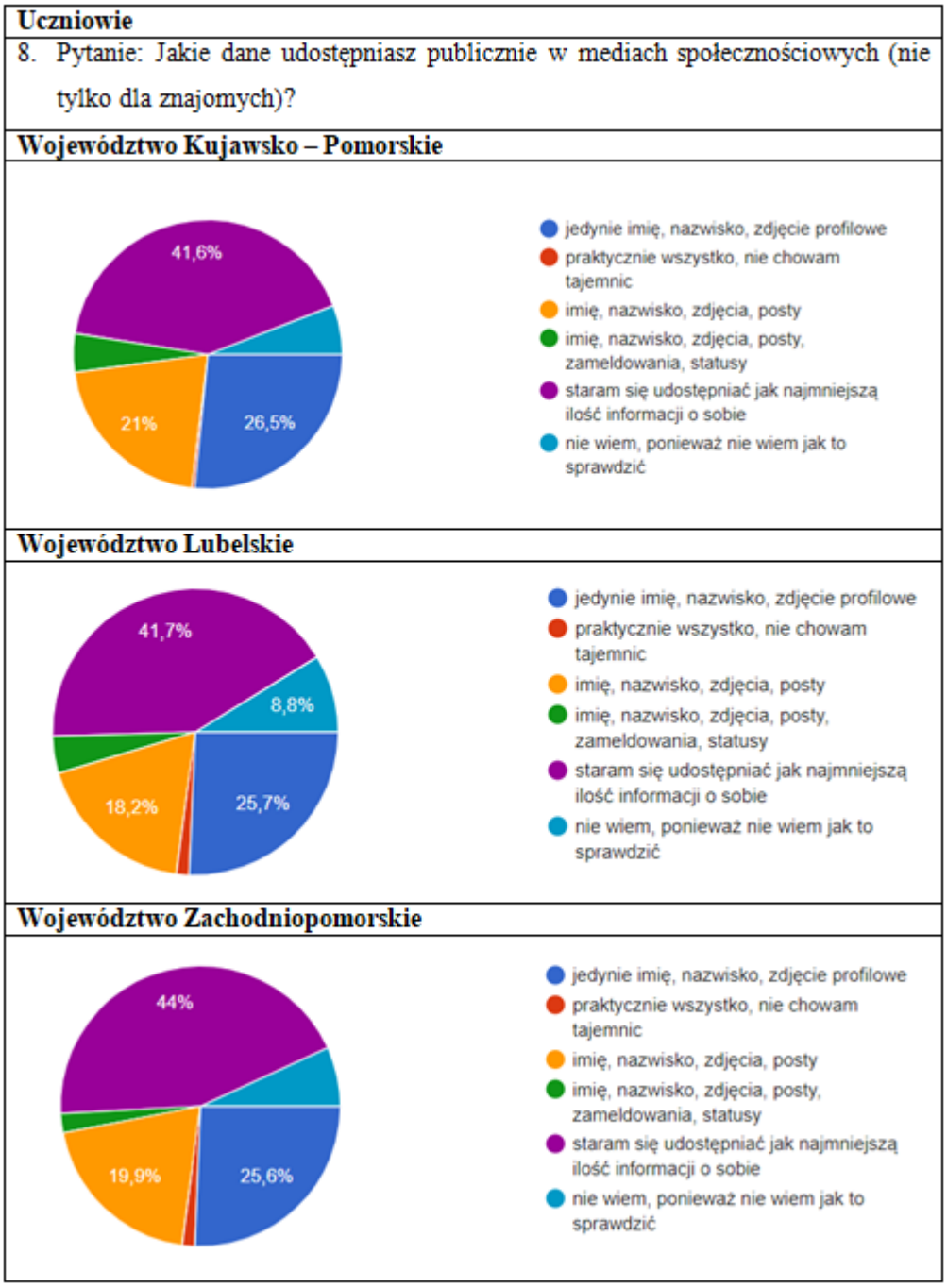
Wykres 6.48. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- korzystanie z portali społecznościowych (źródło: opracowanie własne)

Nieco ponad połowa ankietowanych otrzymując wiadomość od znajomego w serwisie społecznościowym z linkiem, odpowiedziała, iż zapyta znajomego co kryje się pod wskazanym linkiem. Niepokojącym jest fakt, iż około 10% uczniów kliknęłaby bezpośrednio w link sugerując się tym, iż znają daną osobę (najwięcej w woj. Zachodniopomorskim – prawie 13%). 1/3 badanych nie klika w jakiekolwiek linki.



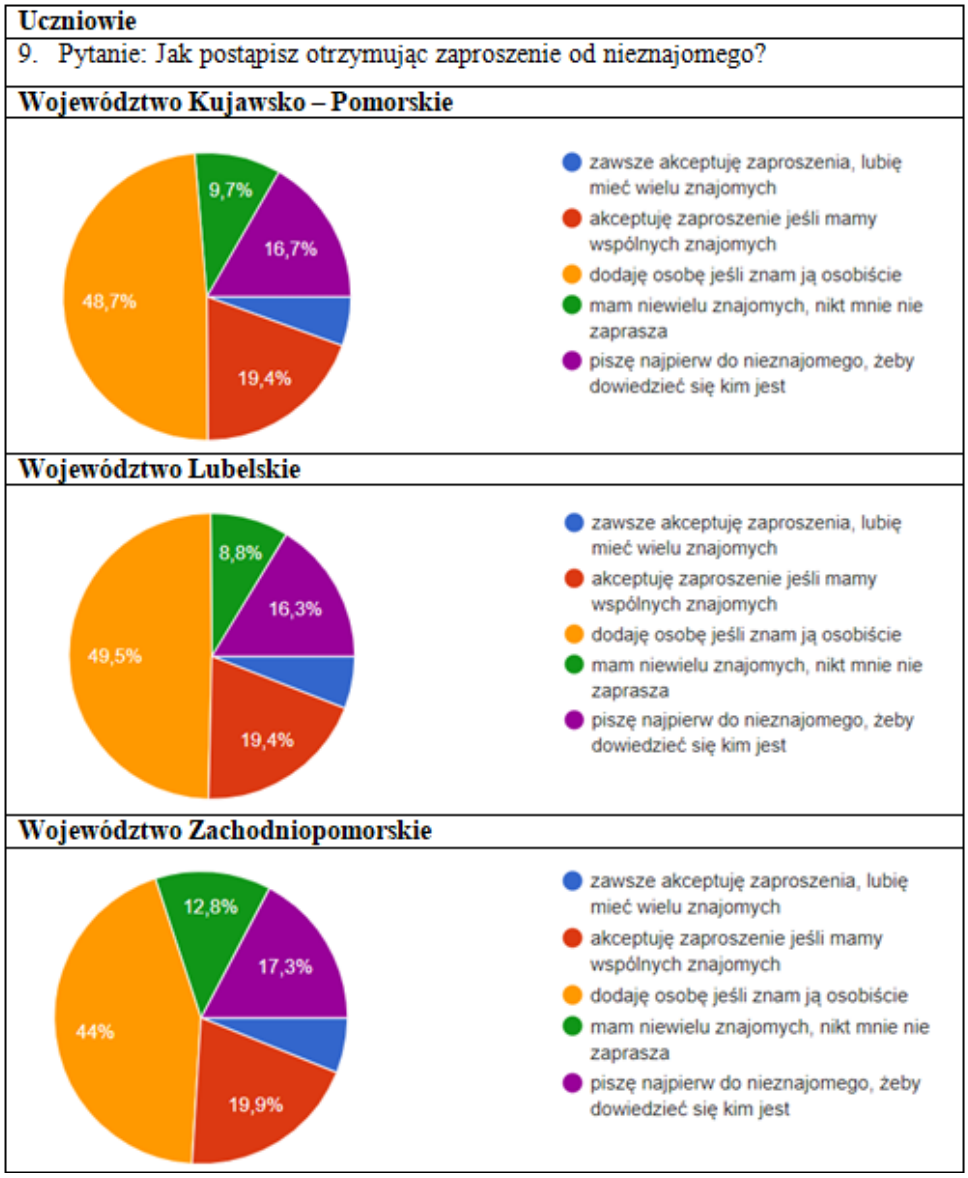
Wykres 6.49. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- badanie reakcji na wiadomość od znajomego (źródło: opracowanie własne)

Jak najmniejszą ilość informacji o sobie publicznie udostępnia ponad 40% uczniów (najbardziej świadomi użytkownicy- woj. Zachodniopomorskie). ¼ badanych udostępnia jedynie swoje imię, nazwisko i zdjęcie profilowe. Około 10% wszystkich ankietowanych nie potrafi samodzielnie sprawdzić co udostępnia i w jakim zakresie. Niestety we wszystkich województwach wystąpił znikomy procent respondentów udostępniających praktycznie wszystko. Dane przedstawiono na poniższym wykresie 6.50.



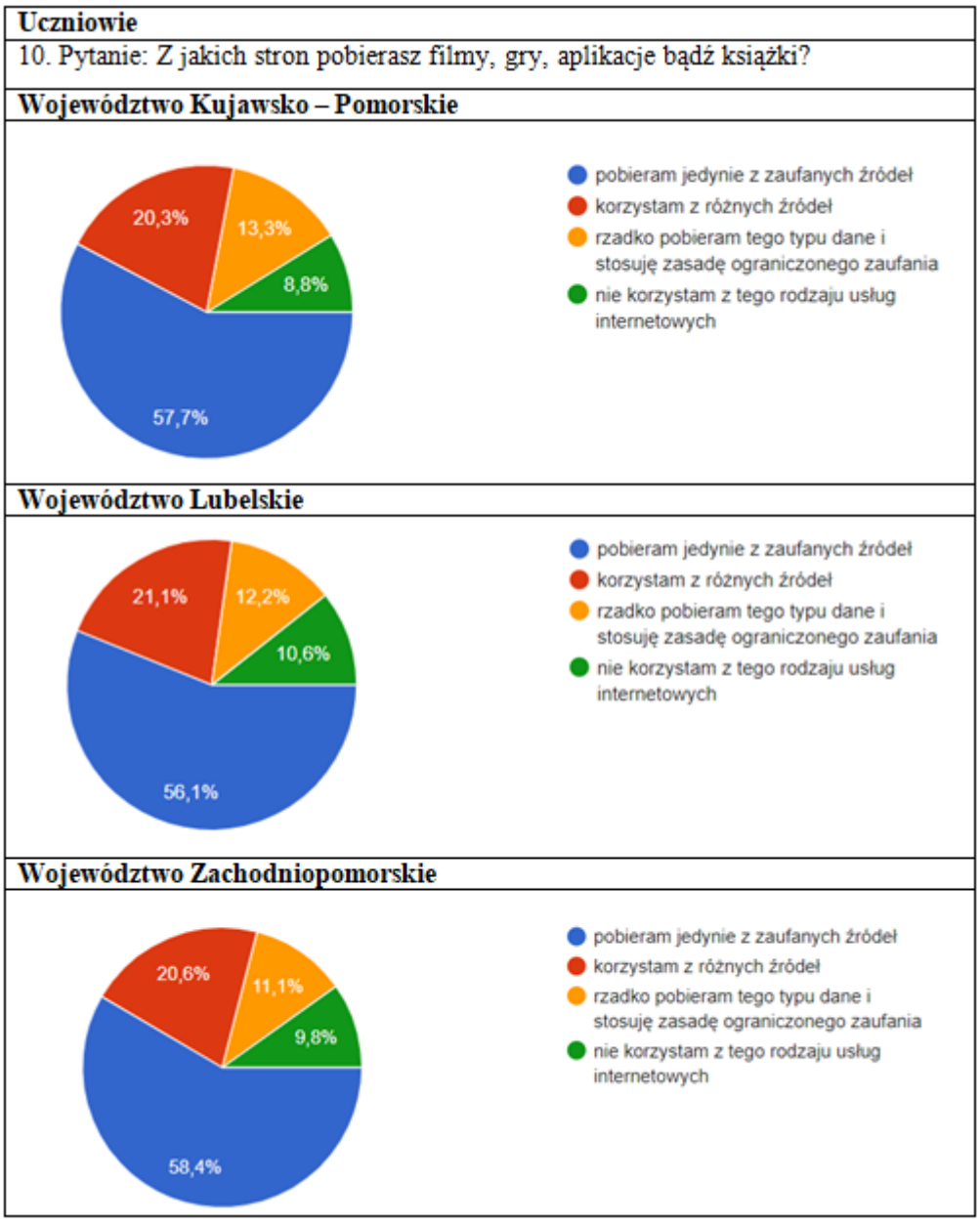
Wykres 6.50. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- udostępnianie informacji w mediach społecznościowych (źródło: opracowanie własne)

Uczniowie zapytani o postępowanie w przypadku otrzymania zaproszenia od nieznajomego we wszystkich badanych województwach odpowiadali zgodnie. Prawie połowa z nich dodaje taką osobę do grona znajomych tylko jeżeli zna ją osobiście. Blisko jedna piąta ankietowanych przy zaakceptowaniu zaproszenia sugeruje się posiadaniem wspólnych znajomych. Próbę weryfikacji znajomości poprzez napisanie wiadomości do nieznajomego wybiera około 16% uczniów z każdego z województw. Pomiędzy 8,8% a 12,8% badanych twierdzi, że posiada niewielką ilość znajomych i takich zaproszeń nie otrzymuje. Pozostali uczniowie deklarują przyjęcie takiego zaproszenia i poszerzenie swojego grona znajomych. Jednak odsetek ten jest niewielki.



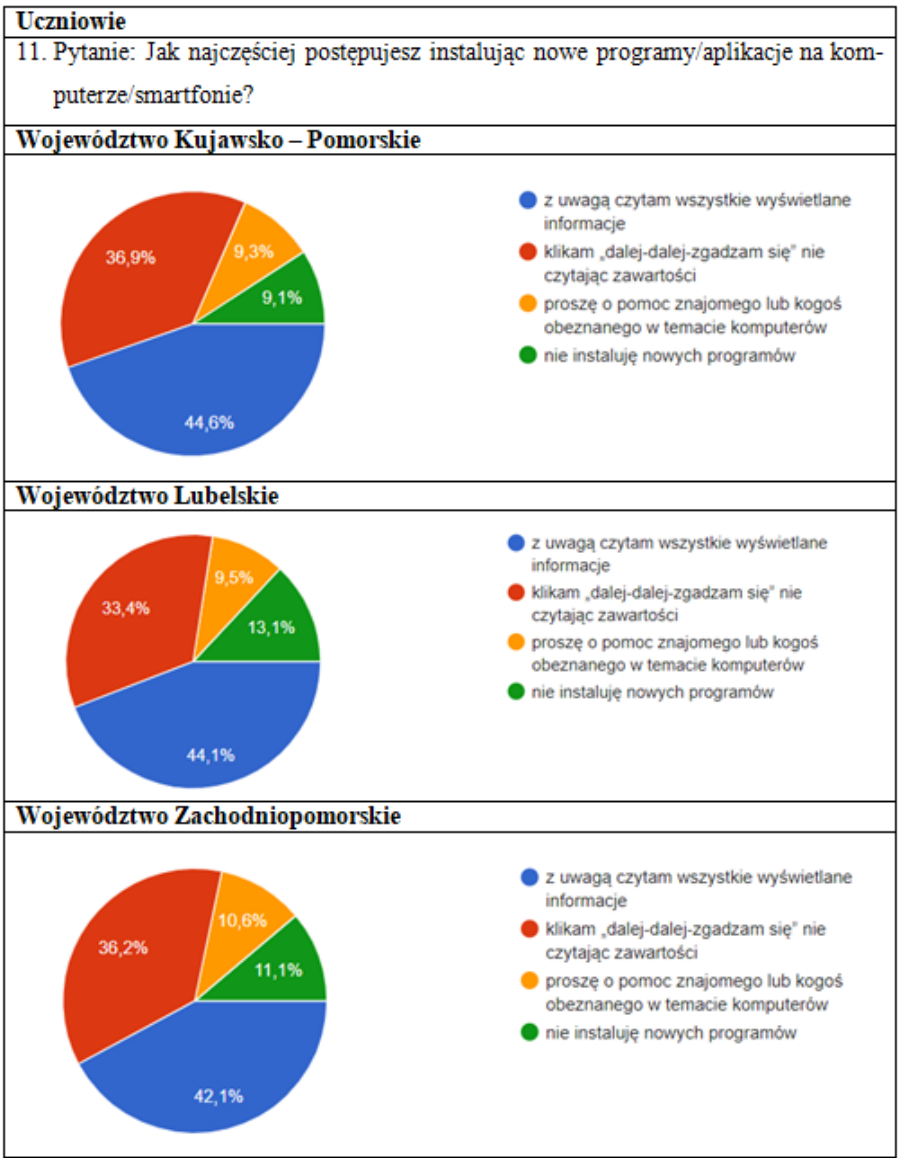
Wykres 6.51. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- postępowanie w sytuacji otrzymania zaproszenia od znajomego (źródło: opracowanie własne)

Kolejnym zadaniem uczniów było określenie źródła pobieranych przez nich danych (filmów, aplikacji, gier itp.). Blisko 60% uczniów w każdym województwie wskazało, że do pobierania tego typu plików wykorzystuje jedynie zaufane strony internetowe. Około 20% z badanych nie ma sprecyzowanych upodobań i wybiera różne źródła. Pozostała część ankietowanych albo rzadko pobiera tego rodzaju dane lub też nie pobiera ich w ogóle. Jak widać na poniższym wykresie (6.52.) wyniki w badanych województwach są do siebie bardzo zbliżone.



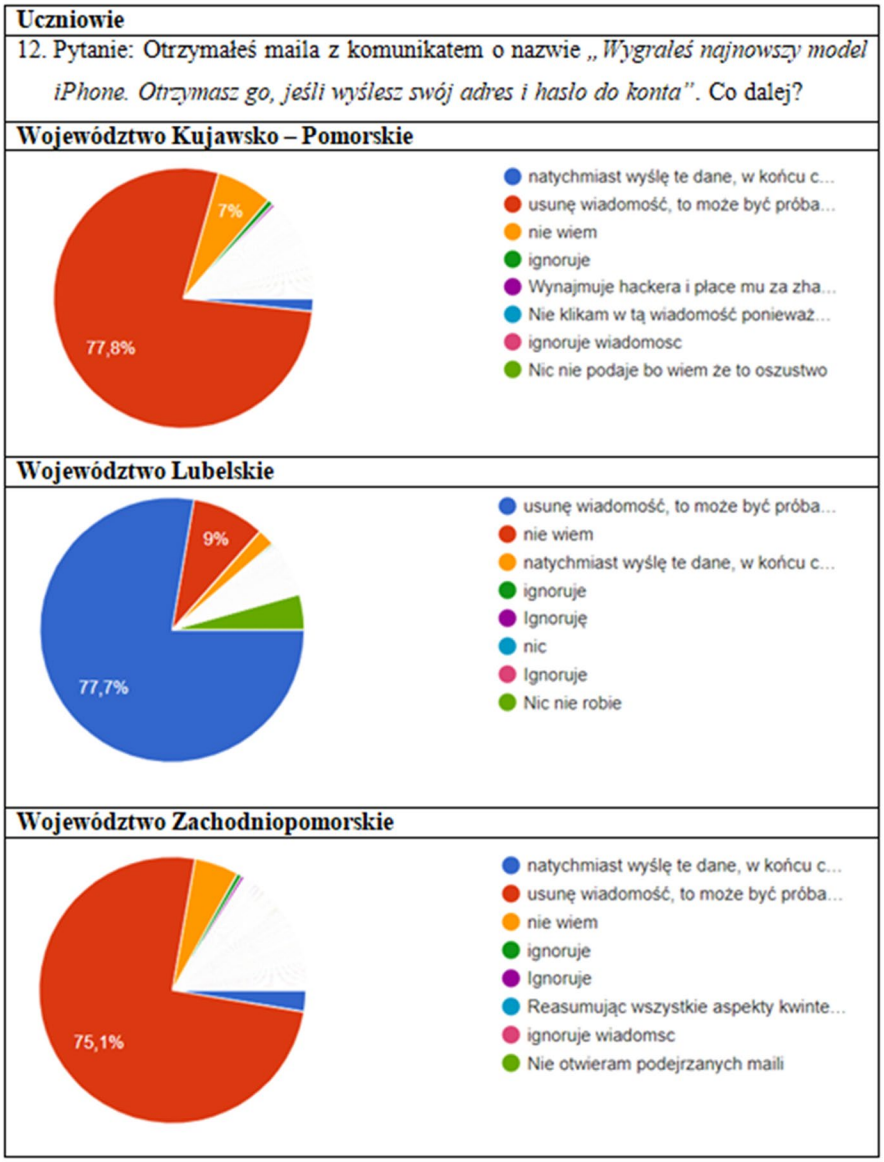
Wykres 6.52. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- pobieranie filmów, gier, etc. (źródło: opracowanie własne)

W kolejnym pytaniu zbadane zostało zachowanie uczniów podczas instalacji nowych programów i aplikacji. Blisko połowa z nich twierdzi, że czyta wszystkie przedstawione na ekranie informacje. Aż 36,9% badanych nie przywiązuje uwagi do wyświetlanych komunikatów i zgadza się na aktywność czego wymaga producent danego oprogramowania. W pozostałych województwach odsetek uczniów postępujących tak samo był zbliżony i wyniósł 36,2% w woj. Zachodniopomorskim oraz 33,4% w woj. Lubelskim. Wykorzystanie pomocy bardziej doświadczonych w tym temacie znajomych zadeklarowała około dziesięcioprocentowa grupa badanych w każdym z województw. Pozostali uczniowie tworzą grupę, która nie instaluje nowego oprogramowania na swoich urządzeniach (wykres 6.53).



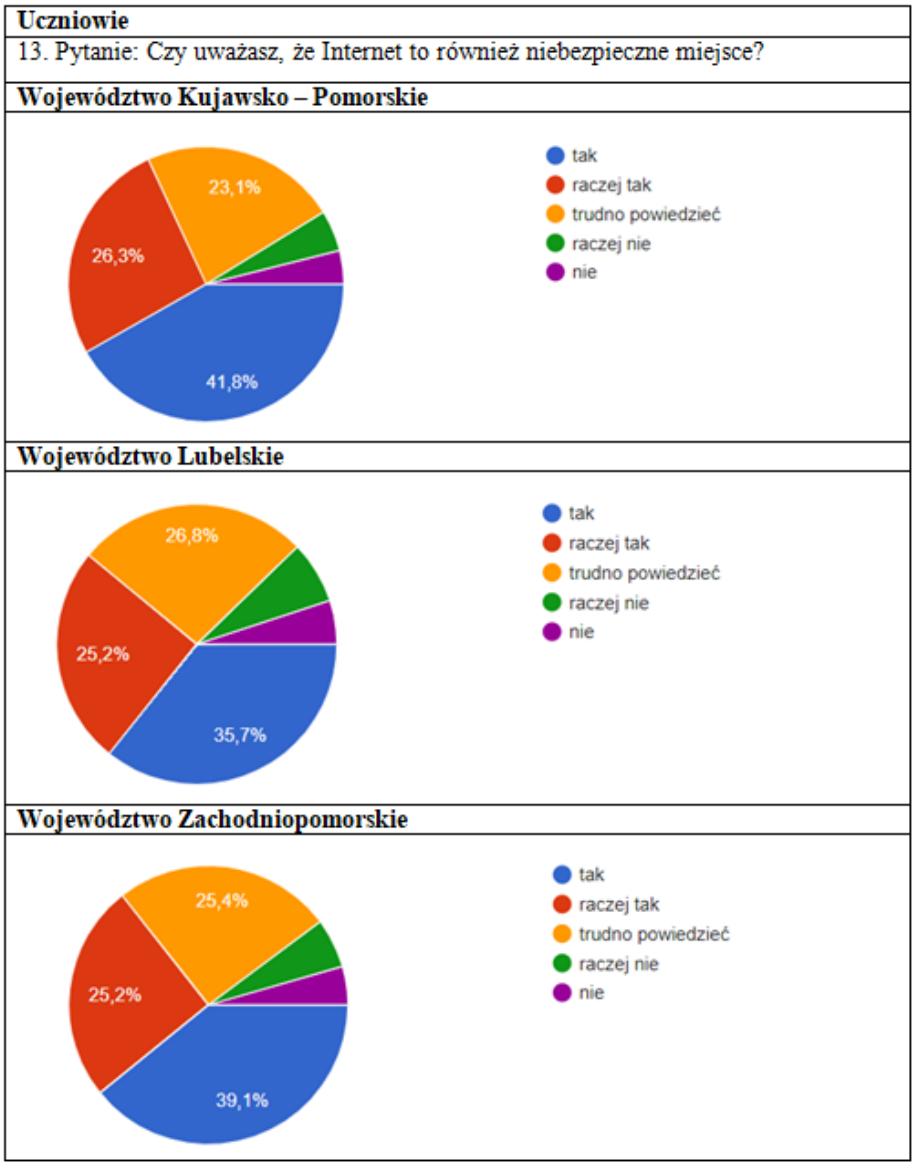
Wykres 6.53. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- postępowanie podczas instalacji nowych programów (źródło: opracowanie własne)

Zachowanie badanych po otrzymaniu maila informującego o wygranej zostało zbadane w pytaniu numer 12 (wykres 6.54.). W woj. Kujawsko – Pomorskim 77,8% badanych usunie taką wiadomość. Podobna ilość zrobi to samo w woj. Lubelskim. Nieco niższy wynik wystąpił w woj. Zachodniopomorskim, lecz jest on również bardzo wysoki (75,1%). Drugą co do liczebności grupę stanowią osoby, które nie wiedzą, jak postąpią. Jest to między 7%, a 9% badanych zależnie od województwa. Głosy otrzymywały również takie odpowiedzi jak „ignoruję", „wyślę dane" i wiele innych jednak ich odsetek był nieznaczący. Taki rozkład wyników może świadczyć o wysokiej świadomości badanych na temat potencjalnego zagrożenia kryjącego się w takiej wiadomości e-mail.



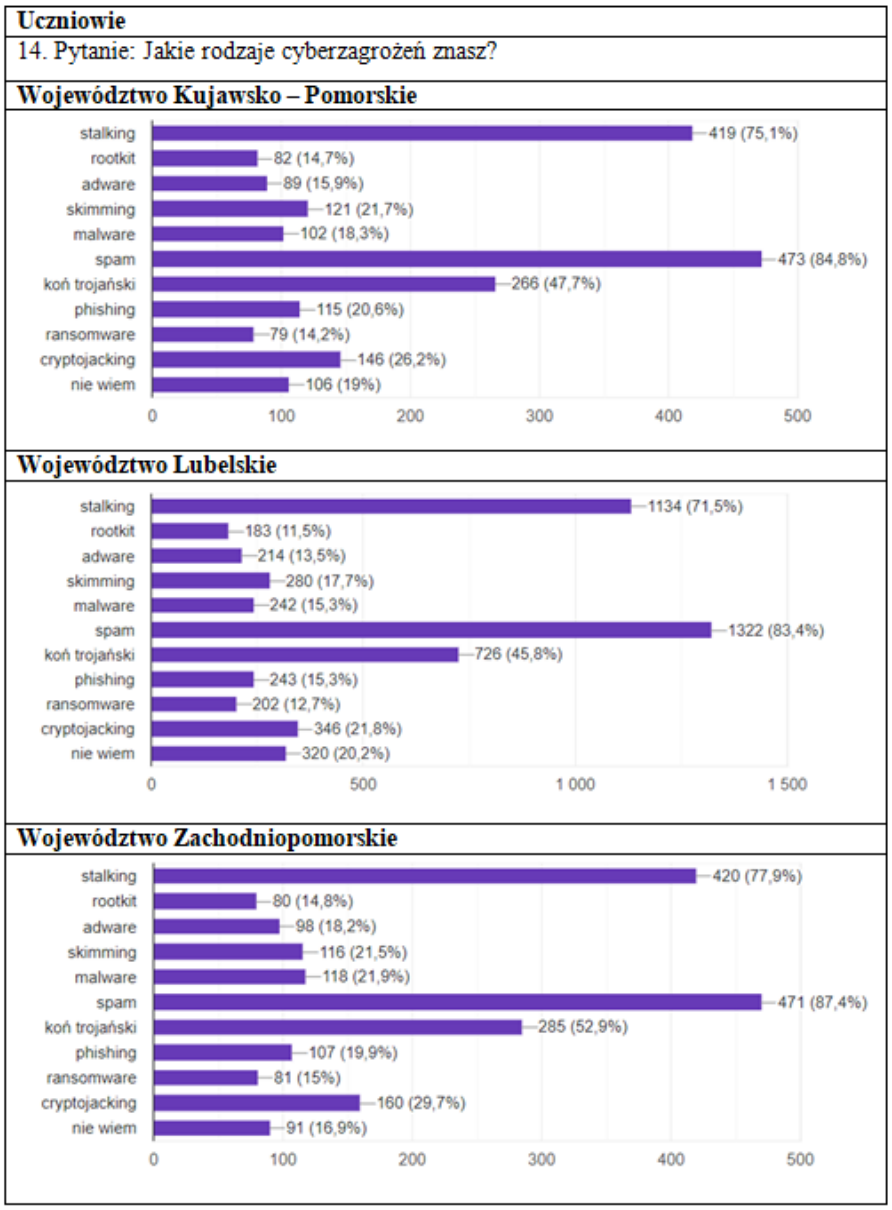
Wykres 6.54. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- otrzymanie komunikatu o wygranej (źródło: opracowanie własne)

Według 41,8% badanych z woj. Kujawsko – Pomorskiego Internet jest miejscem niebezpiecznym (wykres 6.55.). Kolejne 26,3% odpowiadających skłaniało się ku takiej odpowiedzi. Podobne wyniki prezentują pozostałe województwa. W woj. Lubelskim 35,7% badanych definitywnie wskazuje Internet jako miejsce niebezpieczne a w woj. Zachodniopomorskim odsetek ten wynosi 39,1%. Natomiast Internet jako miejsce raczej niebezpieczne określa po 25,2% uczniów z tych dwóch województw. Należy zwrócić uwagę, że około jedna czwarta ankietowanych w poszczególnych województwach nie potrafiła opowiedzieć się po żadnej ze stron. Natomiast około 10 % uczniów w każdym z województw nie uważa Internetu za miejsce niebezpieczne lub skłania się ku takiej odpowiedzi.



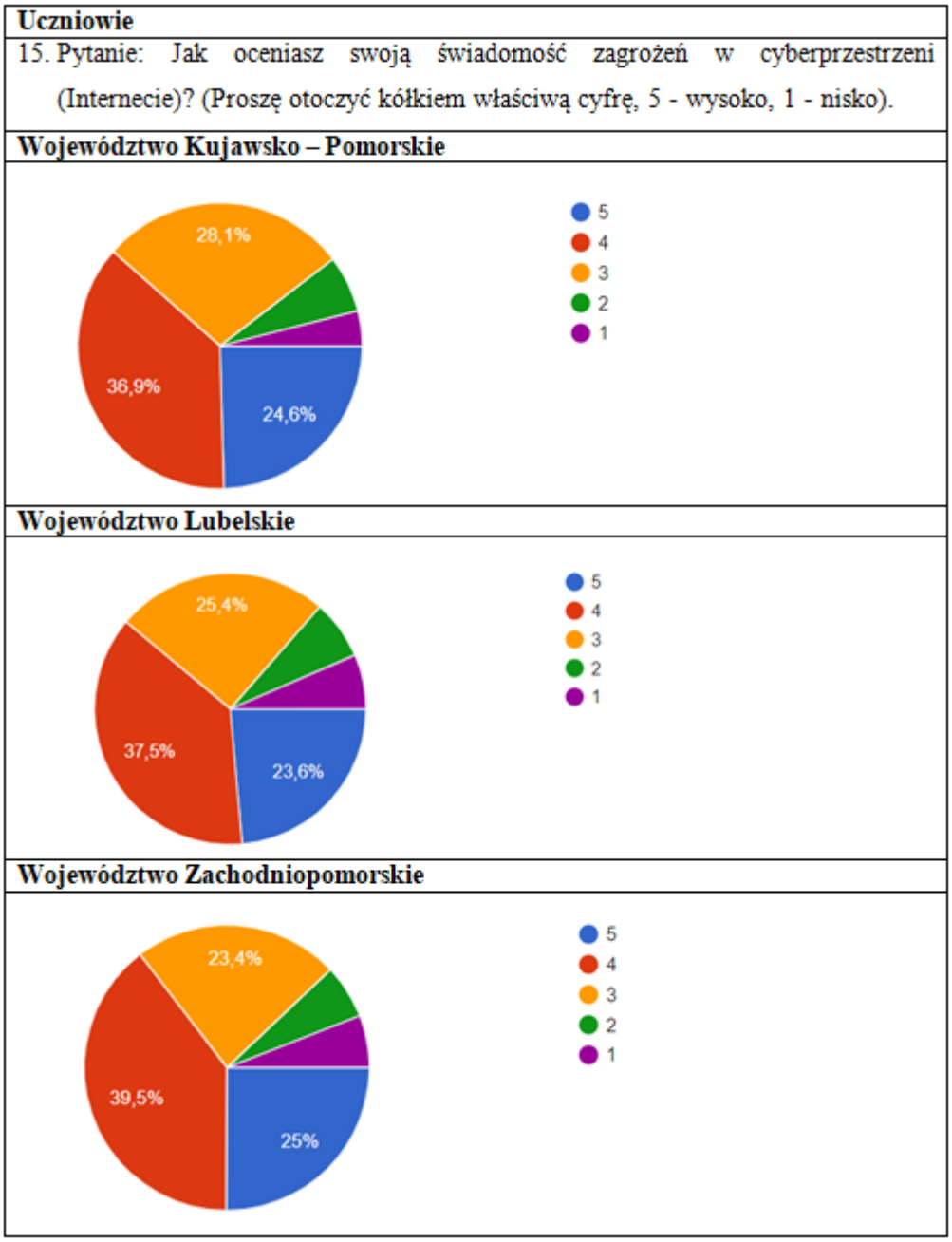
Wykres 6.55. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- zapytanie o opinię (źródło: opracowanie własne)

Spośród występujących w sieci cyberzagrożeń uczniowie we wszystkich województwach najczęściej wskazywali na trzy z nich, są to spam, stalking oraz koń trojański. Kolejnym wyłaniającym się ponad inne zagrożenia jest cryptojacking. Jego znajomość wykazało blisko 29,7% badanych z woj. Zachodniopomorskiego, 26,2% z woj. Kujawsko – Pomorskiego oraz 21,8% z Lubelskiego. Poza tym, ankietowani wymieniali takie cyberzagrożenia m.in. jak rootkit, adware, phishing. W każdym z województw wystąpił dość znaczny odsetek osób wykazujących brak wiedzy na temat cyberzagrożeń. Był on największy w woj. Lubelskim (20,2%), a najniższy w woj. Zachodniopomorskim aż 16,9%.



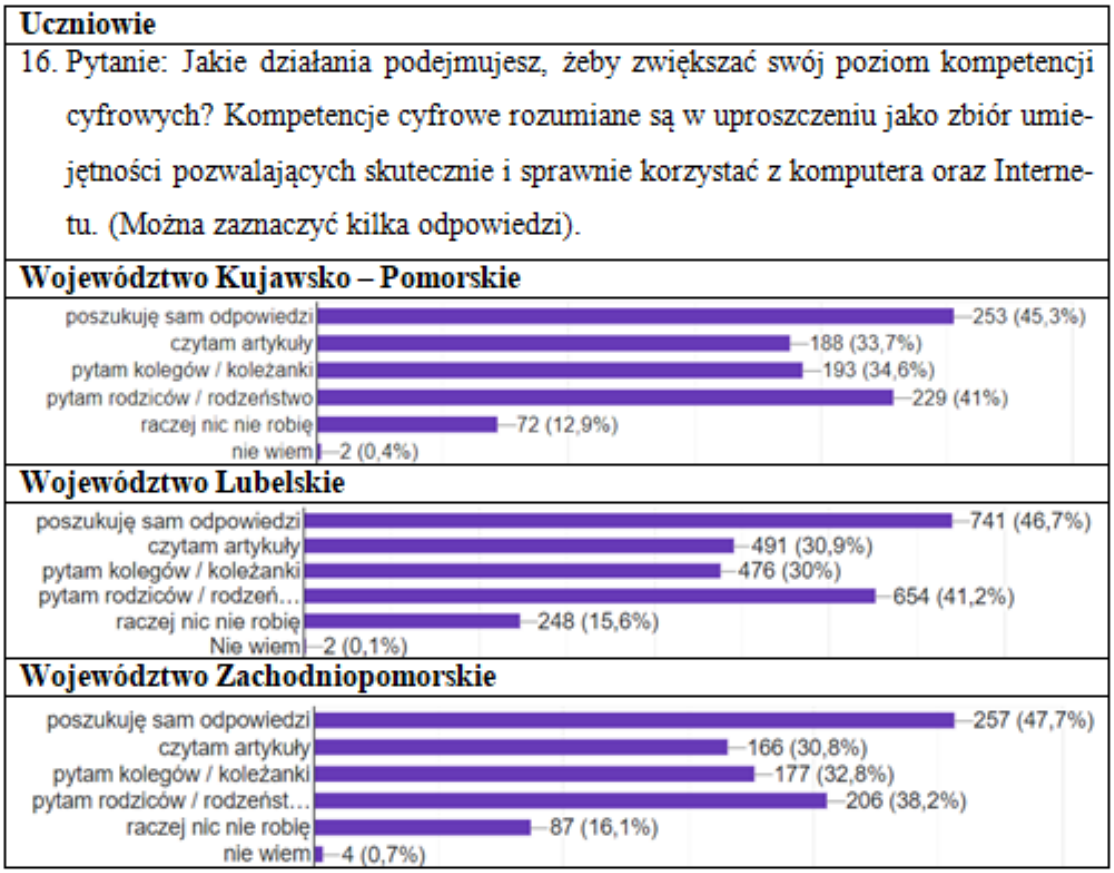
Wykres 6.56. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- rodzaje cyberzagrożeń (źródło: opracowanie własne)

Analizując poniższe wykresy należy wskazać, że większość ankietowanych ocenia swoją świadomość na temat zagrożeń występujących w Internecie na średnią lub wyższą. Wysoką świadomość wykazuje od 36,9% w woj. Kujawsko – Pomorskim do 39,5% w woj. Zachodniopomorskim. Jako średnio świadomych (ocena 3 i 4) określiło się około ponad 52,7% badanych z woj. Kujawsko – Pomorskiego. Natomiast w woj. Lubelskim i Zachodniopomorskim odsetek ten był niecno niższy i wyniósł ok 49%. Pozostali uczniowie podczas samooceny wykazali niską świadomość (ocena 1 i 2) i stanowią oni około 10%.



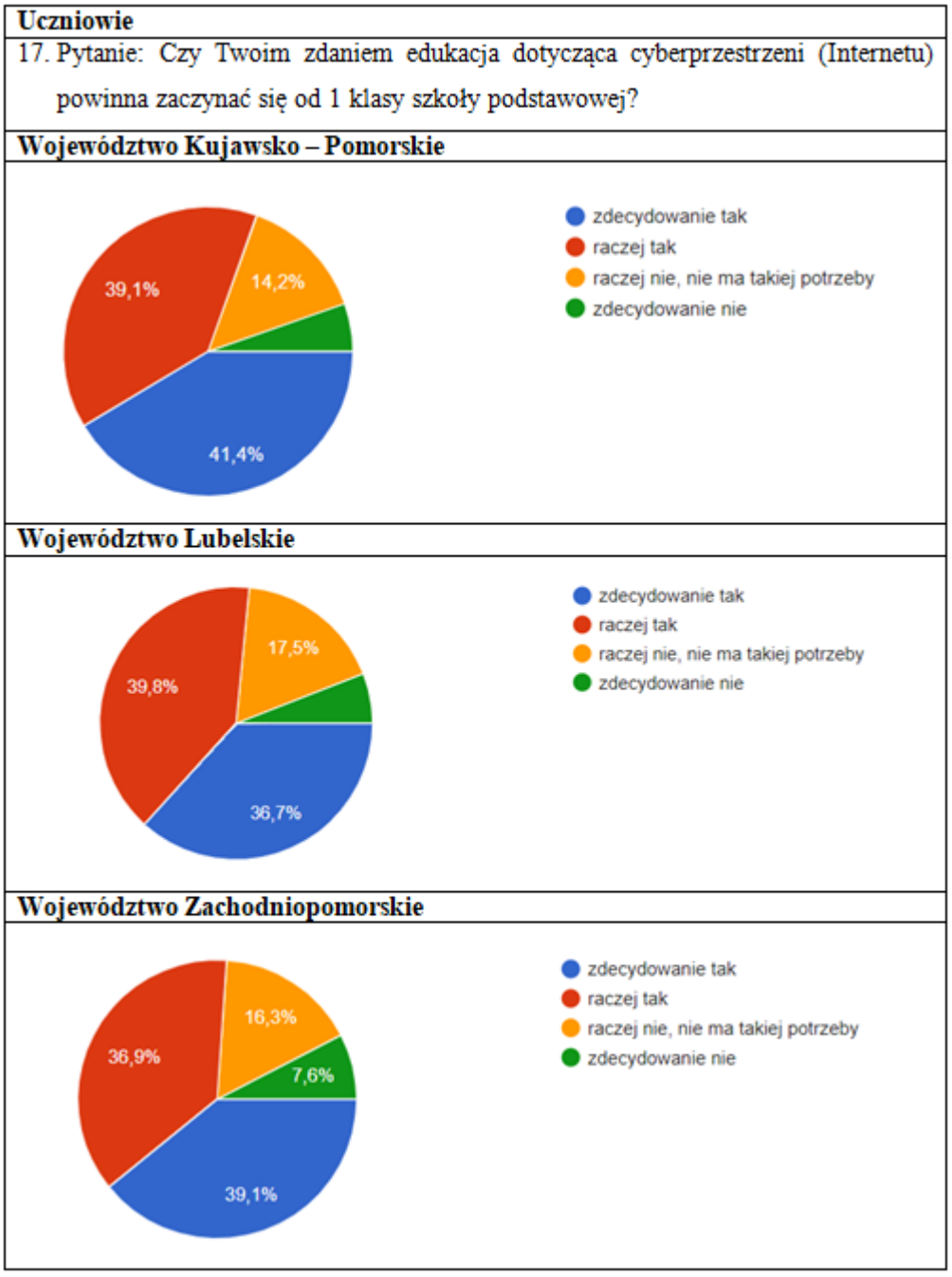
Wykres 6.57. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- świadomość cyberzagrożeń (źródło: opracowanie własne)

Młodzież bardzo sprawnie korzysta z nowoczesnych urządzeń i Internetu. Uczniowie zapytani w jaki sposób podnoszą swoje umiejętności w tym zakresie zgodnie odpowiedzieli, że najczęściej znajdują informacje samodzielnie. Następnie szukają rady u najbliższych. Chcąc poszerzyć swoją wiedzę badani sięgają również po specjalistyczne artykuły oraz szukają wsparcia u znajomych. W każdym województwie wystąpiła również grupa, która nie odczuwa potrzeby rozwoju w zakresie kompetencji cyfrowych. Ma ona największy procentowy udział w woj. Zachodniopomorskim (16,1%), a najmniejszy w woj. Kujawsko-Pomorskim (12,9%). Analizując poniższe wyniki należy zwrócić uwagę na to, jak ważną rolę odgrywają doświadczenia rodziny i bliskich w podnoszeniu kompetencji cyfrowych.



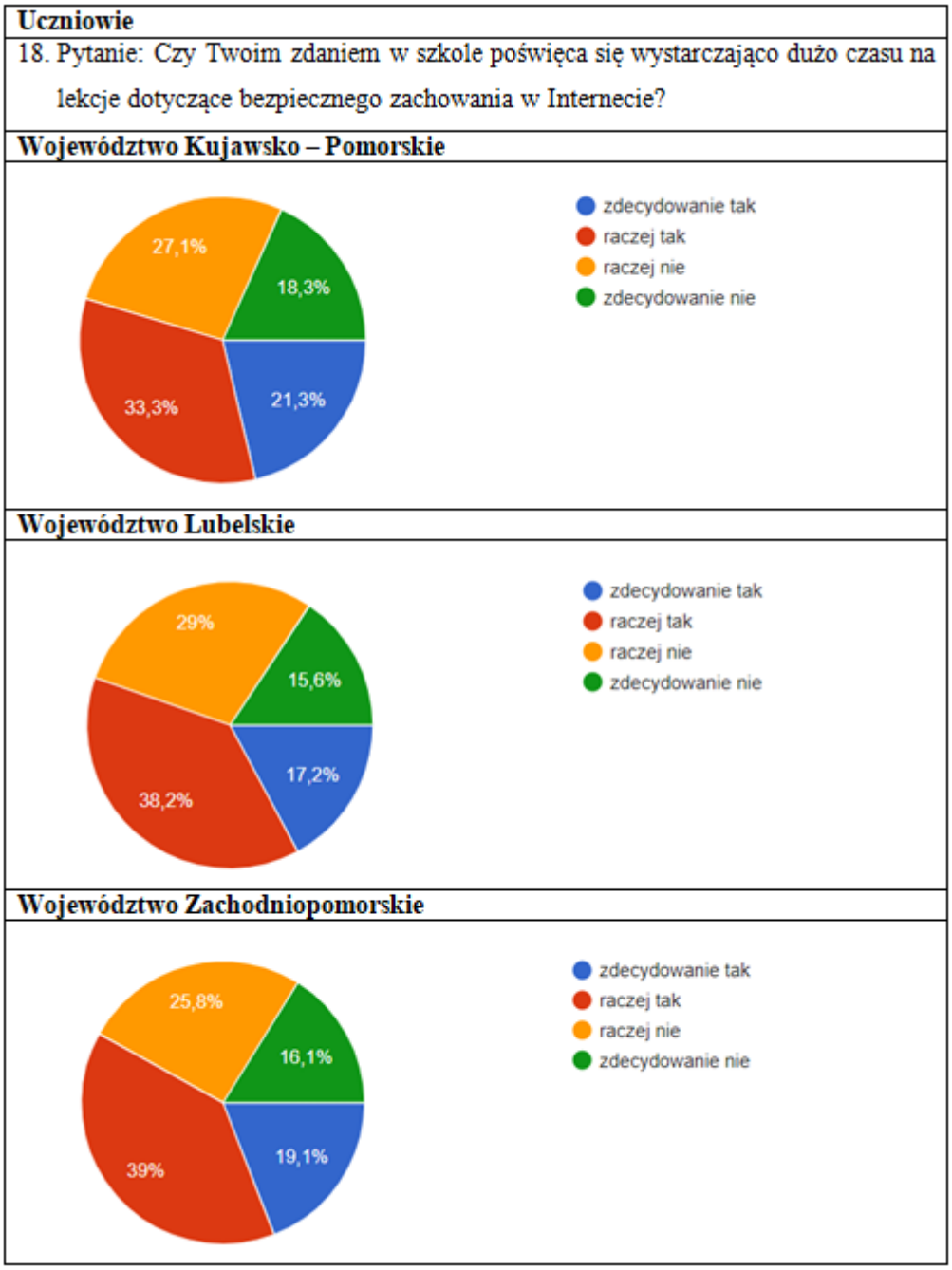
Wykres 6.58. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- zwiększanie poziomu kompetencji cyfrowych (źródło: opracowanie własne)

Uczniowie w badanych województwach dostrzegli konieczność edukacji w zakresie cyberprzestrzeni już od najmłodszych lat. Rozkład odpowiedzi był bardzo zbliżony. Około 40% ankietowanych zdecydowanie opowiedziało się za koniecznością rozpoczęcia nauki już od 1 klasy szkoły podstawowej. Kolejna prawie tak samo liczna grupa skłaniała się ku zdecydowanej odpowiedzi. Brak konieczności wyraża około 20 % badanych w poszczególnych województwach.



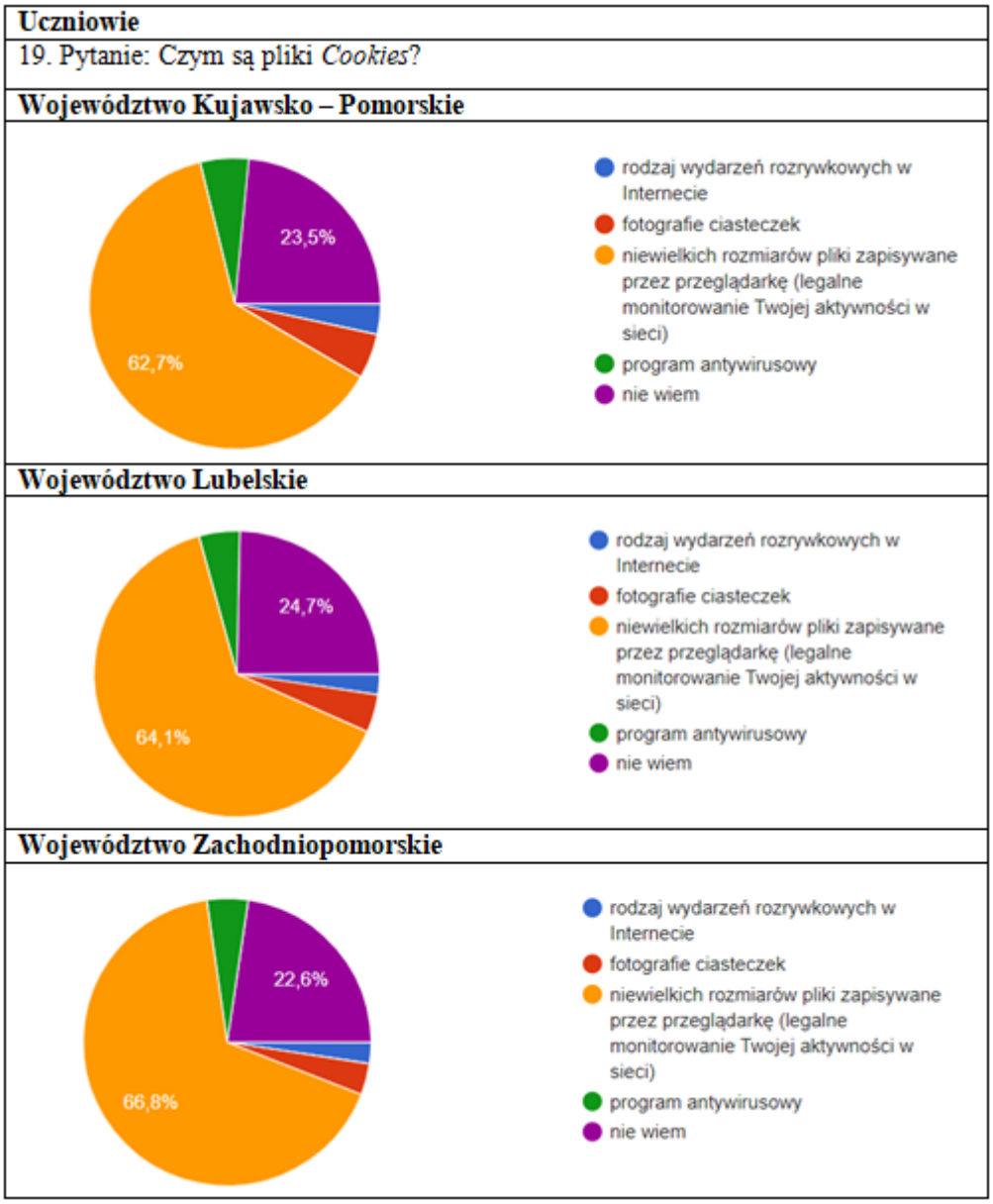
Wykres 6.59. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- edukacja od najmłodszych lat (źródło: opracowanie własne)

Analiza poniższych wyników wskazuje, iż w sprawie ilości czasu poświęcanego na lekcje dotyczące bezpiecznego zachowania w Internecie zdania są podzielone, z niewielką przewagą odpowiedzi twierdzących. Największa ilość badanych twierdzi, że tego rodzaju lekcji jest wystarczająco występuje w woj. Zachodniopomorskim i stanowi 58,1% badanych (z czego w pełni przekonanych jest 19,1%). W pozostałych województwach wyniki są zbliżone i wynoszą około 54%. Tak niewielka różnica może świadczyć o niewystarczającej ilości czasu przeznaczonego na tego rodzaju zajęcia.



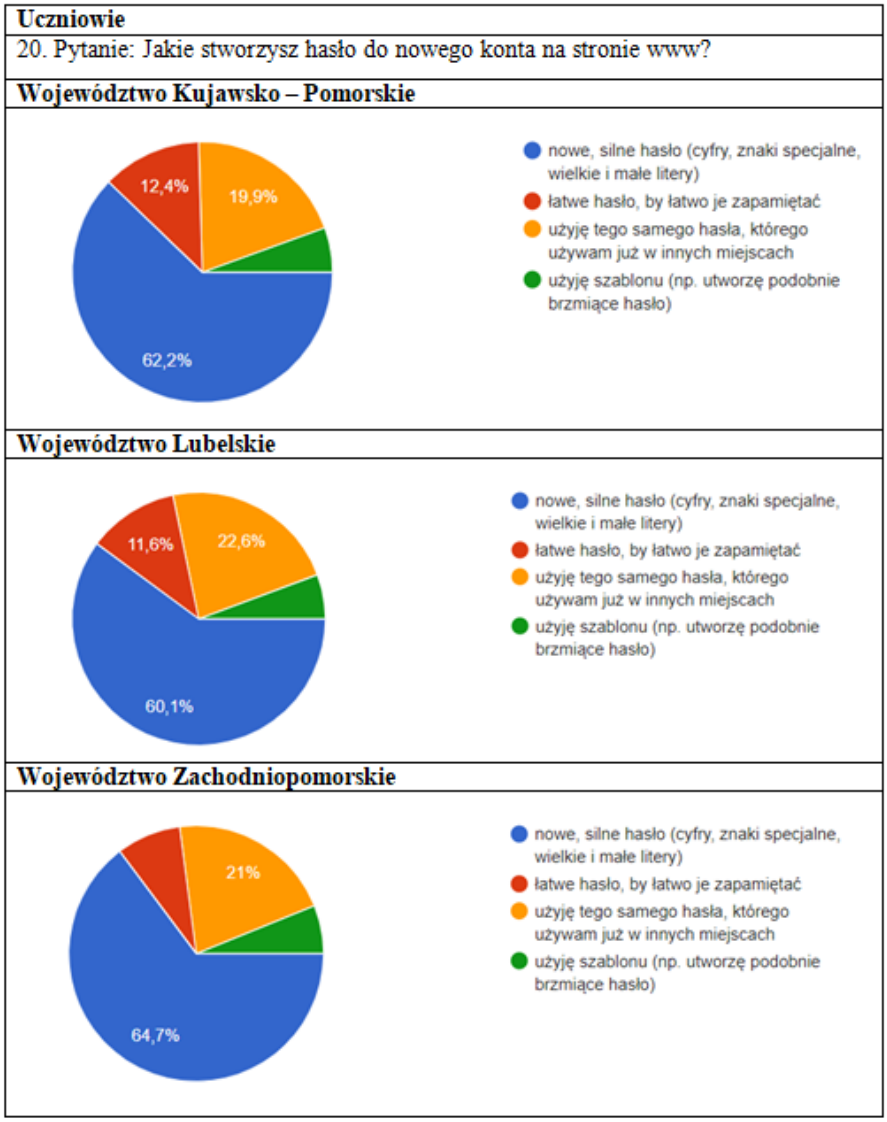
Wykres 6.60. Odpowiedzi ankietowanych uczniów z trzech wybranych województw-
ilość czasu przeznaczanego na lekcje dot. bezpiecznego zachowania w Internecie (źródło: opracowanie własne)

Każda ze stron internetowych próbuje zbierać dane o odwiedzających ją użytkownikach i gromadzi je w postaci *Cookies* (wykres 6.61.). Badani uczniowie w ponad 60% potrafili wskazać prawidłową definicję plików *Cookies*. Najwyższa liczba respondentów udzielająca prawidłowej odpowiedzi wystąpiła w woj. Zachodniopomorskim – 66,8%. A najniższa w woj. Kujawsko – Pomorskim – 62,7%. W każdym z województw wystąpiła ponad dwudziestoprocentowa grupa badanych, która nie wiedziała jaka jest prawidłowa definicji *Cookies*. Tak wysoki odsetek może świadczyć o znacznej niewiedzy uczniów na temat tego jakie informacje gromadzą o nich przeglądane strony internetowe.



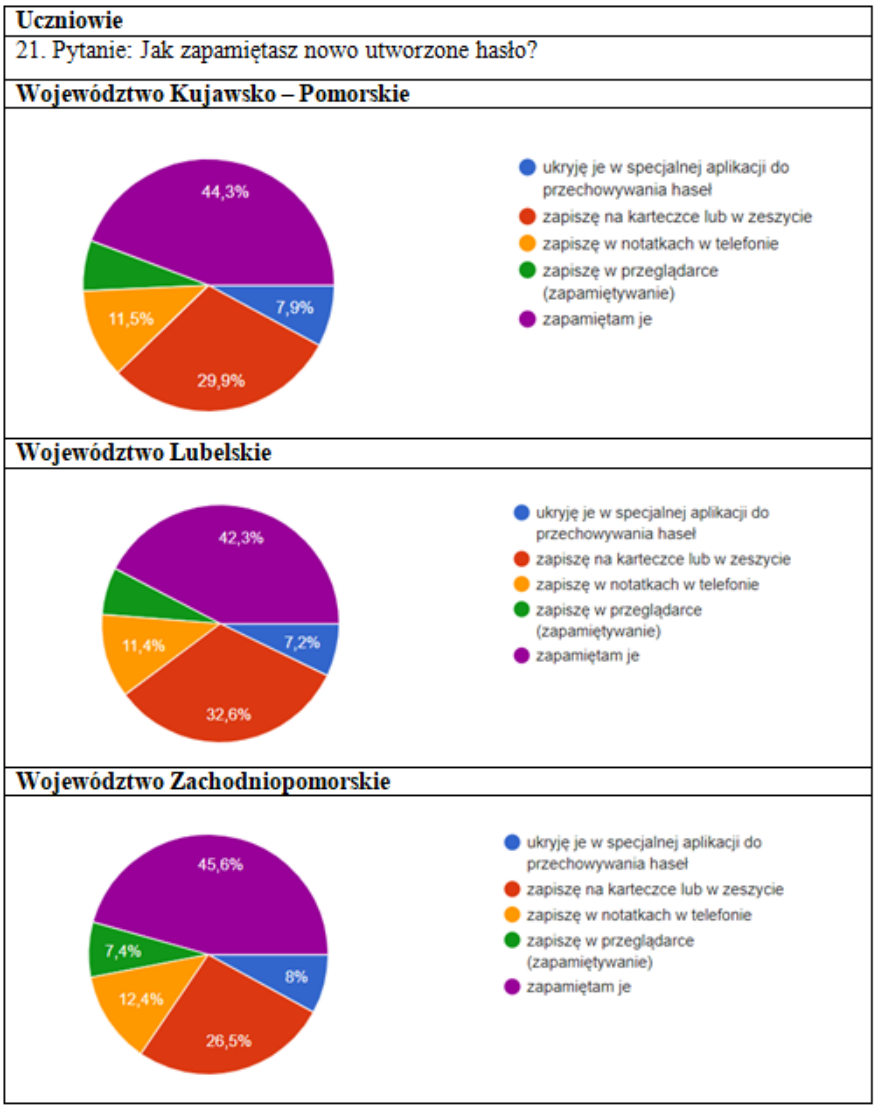
Wykres 6.61. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- umiejętność definicji plików *Cookies* (źródło: opracowanie własne)

Obecnie większość stron internetowych umożliwia nam stworzenie konta użytkownika, które zabezpieczone jest hasłem. W pytaniu numer 20 uczniowie zostali poproszeni o wskazanie ich sposobu na stworzenie hasła. Otrzymane w trzech województwach wyniki są do siebie bardzo zbliżone. Ponad 60% badanych do stworzenia hasła wykorzysta cyfry, znaki specjalne oraz wielkie i małe litery. Jedna piąta ankietowanych nie wysili się i użyje takiego samego hasła jak na innych stronach internetowych. Około dwunastoprocentowa grupa uczniów wybierze łatwe hasło kierując się łatwością w jego zapamiętaniu. Pozostali badani stworzą hasło na bazie szablonu, który wykorzystują w innych miejscach, zmieniając tylko nieznaczną jego część. Jak widać ponad połowa uczniów stara się zadbać o bezpieczeństwo swoich danych w Internecie i tworzy skomplikowane hasło.



Wykres 6.62. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- hasło do nowego konta (źródło: opracowanie własne)

Po stworzeniu nowego hasła istnieje wiele możliwości jego zapamiętania. Większość uczniów po prostu zapamiętuje hasło. Próbując się ochronić przed zapomnieniem hasła 32,6% uczniów z woj. Lubelskiego zapisze je na kartce. W pozostałych województwach odsetek ten jest mniejszy i stanowi 29,9% w woj. Kujawsko – Pomorskim oraz 26,5% w woj. Zachodniopomorskim. Natomiast mobilną formę notatek wybierze około 12% ankietowanych z trzech województw. Coraz bardziej popularne stają się specjalne aplikacje do zabezpieczania swoich haseł. Jednak wśród uczniów sposób ten nie jest powszechnie stosowany. Jak widać taką metodę wybierze tylko około 8% z nich. Pozostała grupa badanych wykorzysta możliwości jakie daje przeglądarka internetowa i to właśnie w niej będzie przechowywać hasło, co stanowi swego rodzaju ryzyko w razie ewentualnej próby włamania do danych przeglądarki.



Wykres 6.63. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- zapamiętanie nowo utworzonego hasła (źródło: opracowanie własne)

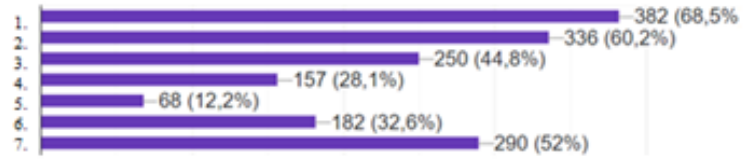
Najczęściej spotykanym problemem jaki napotykali uczniowie podczas zdalnego nauczania było ich zmęczenie spowodowane zbyt długim przebywaniem przed ekranem monitora. Ten problem wskazało 68,5% uczniów z woj. Kujawsko – Pomorskiego, 63,5% z woj. Lubelskiego oraz 62,9% z woj. Zachodniopomorskiego. Jako drugi najczęściej spotykany problem 60,2% uczniów z woj. Kujawsko – Pomorskiego wskazało słabe połączenie internetowe. W pozostałych województwach odsetek ten oscylował w okolicy 50%. Około 53% badanych z woj. Kujawsko – Pomorskiego oraz Zachodniopomorskiego zasygnalizowało, że słabe łącze występuje u nauczyciela. Co interesujące, w woj. Lubelskim grupa ta stanowi jedynie 9,7%. Odwrotnie ma się sytuacja w przypadku umiejętności korzystania z komputera. W woj. Kujawsko – Pomorskim ten problem wskazało 12,2% badanych, w woj. Zachodniopomorskim 9,6%, a w woj. Lubelskim, aż 29,4%. Ponadto blisko połowa badanych zwracała uwagę na trudności w dołączeniu do grupy online. Powyższe dane świadczą o tym, iż większość problemów leży po stronie technicznej, po stronie sprzętu.

Uczniowie

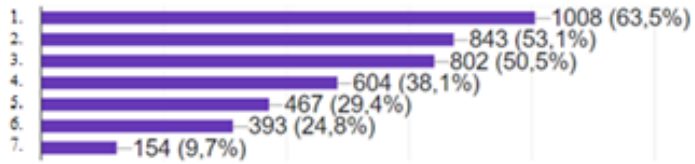
22. Pytanie: Jakie problemy napotkałeś/aś podczas zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).

1. Zmęczenie spowodowane siedzeniem przed ekranem monitora
2. Słabe własne połączenie internetowe
3. Trudności w dołączeniu do grupy online
4. Niewłaściwy sprzęt np. zbyt wolny komputer
5. Niewystarczające umiejętności obsługi komputera / programów
6. Zbyt dużo materiału realizowanego na zajęciach online
7. Słabe połączenie internetowe nauczyciela

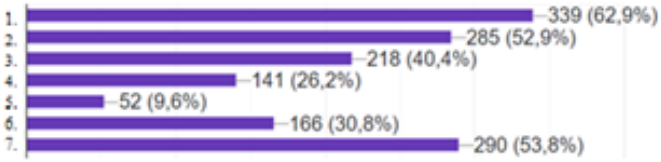
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

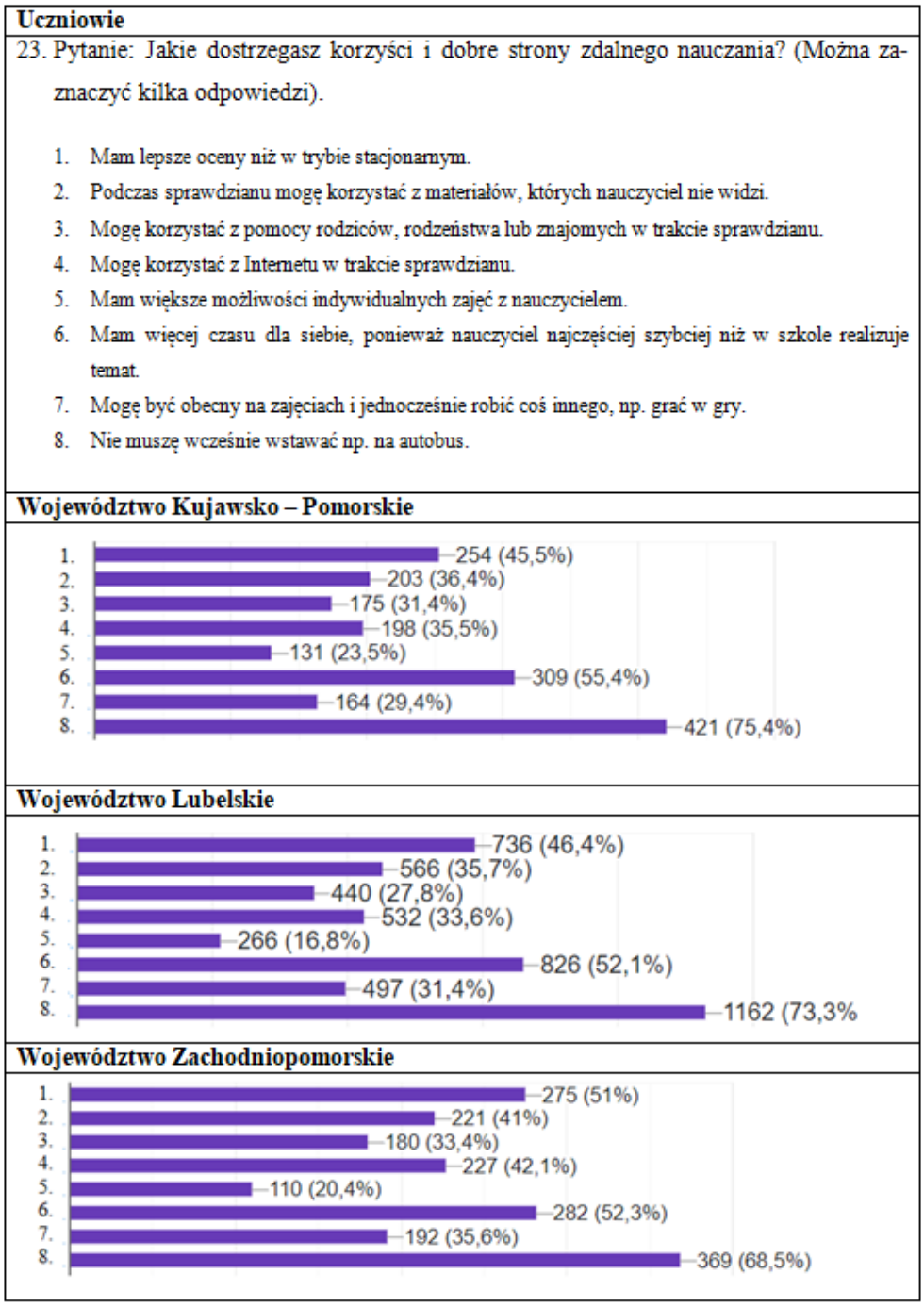


Województwo Zachodniopomorskie



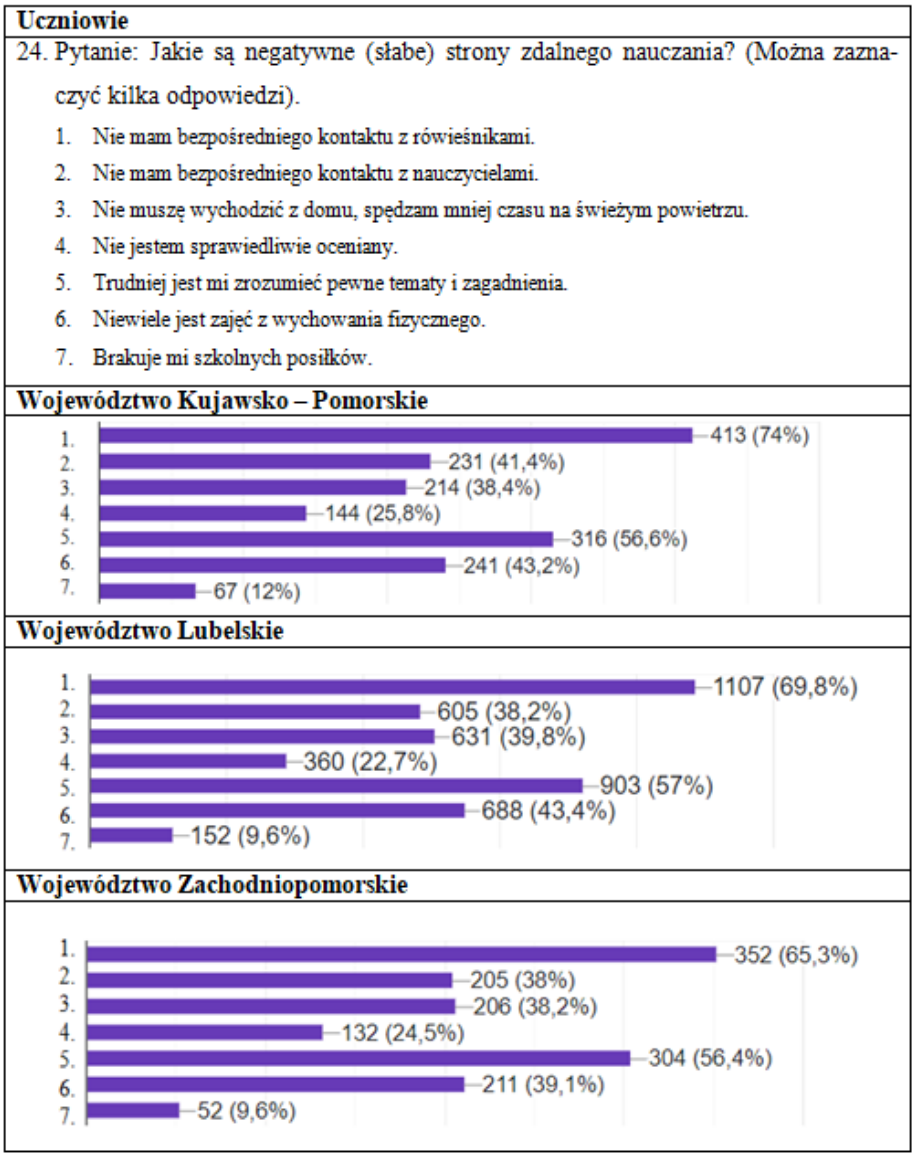
Wykres 6.64. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- problemy uczniów napotkane podczas zdalnego nauczania (źródło: opracowanie własne)

Uczniowie zapytani o zalety zdalnego nauczania we wszystkich trzech województwach wskazali zgodnie brak konieczności wczesnego wstawania do szkoły (ponad 70% badanych). Jako kolejne zalety zaznaczali m.in. zdobywanie lepszych ocen niż w trybie stacjonarnym czy więcej czasu dla siebie. Ponadto ponad trzydziestoprocentowe grup uczniów wskazały na możliwość wykorzystywania pomocy bliskich podczas sprawdzianu. Najmniejsza liczba osób jako zaletę określiła możliwość indywidualnych zajęć z nauczycielem. Wyniki zaprezentowano na wykresie 6.65.



Wykres 6.65. Odpowiedzi ankietowanych uczniów z trzech wybranych województw-plusy zdalnego nauczania (źródło: opracowanie własne)

Wśród największych wad zdalnego nauczania 65,3% uczniów z woj. Zachodniopomorskiego wskazało brak bezpośredniego kontaktu z rówieśnikami. Podobny wyniki wystąpił w woj. Lubelskim (69,8%), zaś w woj. Kujawsko – Pomorskim odpowiedź ta uzyskała aż 74% głosów. Ponad 50% badanych uczniów w każdym z województw jako kolejną wadę wskazało problem w rozumieniu złożonych tematów i zagadnień. Dalej zgodnie z ilością uzyskanych głosów uczniowie podkreślali brak bezpośredniego kontaktu z nauczycielami, mniej czasu na świeżym powietrzu oraz brak zajęć z wychowania fizycznego. Najmniejszą wadą dla badanych był niesprawiedliwość oceniania oraz brak szkolnych posiłków. Odpowiedź ta uzyskała jedynie 12% głosów w woj. Kujawsko – Pomorskim a w pozostałych tylko 9,6%.



Wykres 6.66. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- minusy zdalnego nauczania (źródło: opracowanie własne)

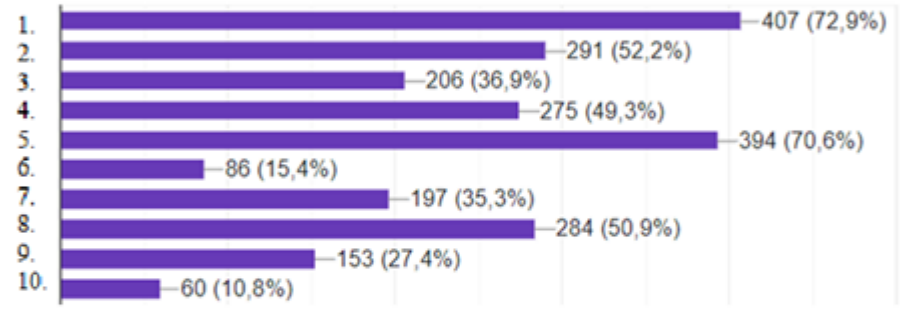
Nauczanie zdalne daje wiele możliwości tak samo nauczycielom jak i uczniom. W pytaniu numer 25 (wykres 6.67.) uczniowie mieli dokonać wyboru najczęściej wykorzystywanych przez nauczycieli form nauczania. Analizując wyniki możemy wskazać dwie główne formy. Pierwsza z nich to wykorzystywanie gotowych filmików edukacyjnych a druga prowadzenie lekcji na żywo. Obie te odpowiedzi otrzymały ponad 70% głosów w woj. Kujawsko – Pomorskim oraz ponad 60% w woj. Lubelskim i Zachodniopomorskim. Nieco rzadziej uczniowie wskazywali na wykorzystywanie przez nauczycieli własnych materiałów do późniejszego samodzielnego uzupełnienia i prezentacji multimedialnych oraz zlecanie uczniom zadań domowych np. polegających na przygotowaniu własnej prezentacji. Trzy wymienione wyżej formy zostały wskazane przez około 50 % badanych. Zdaniem uczniów metodami najrzadziej stosowanymi są indywidualne konsultacje (około 10%) oraz przesyłanie gotowych nagranych wcześniej lekcji.

Uczniowie

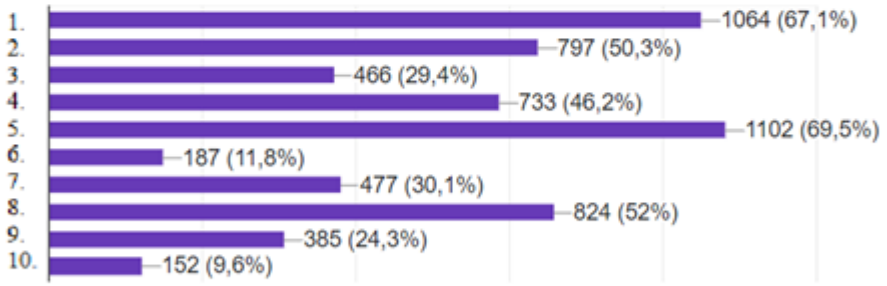
25. Pytanie: Które formy nauczania najczęściej wykorzystywali nauczyciele w trybie zdalnym? (Można zaznaczyć kilka odpowiedzi).

1. Korzystanie z gotowych filmików edukacyjnych w Internecie
2. Przesyłanie swoich materiałów do samodzielnego wypełnienia
3. Przesyłanie / podawanie zakresu z podręcznika do samodzielnego opracowania
4. Korzystanie z prezentacji wykonanej przez nauczyciela
5. Prowadzenie lekcji na żywo przy pomocy np. Zoom, MS Teams i innych
6. Wysyłanie gotowych, nagranych lekcji np. Webinarów
7. Udostępnianie linków do lekcji w Internecie prowadzonych przez innego nauczyciela
8. Zlecanie zadań typu: odrobienie pracy domowej, wykonanie prezentacji
9. Korzystanie z aplikacji do edukacji online np. Google Classroom i innych
10. Prowadzenie indywidualnych konsultacji

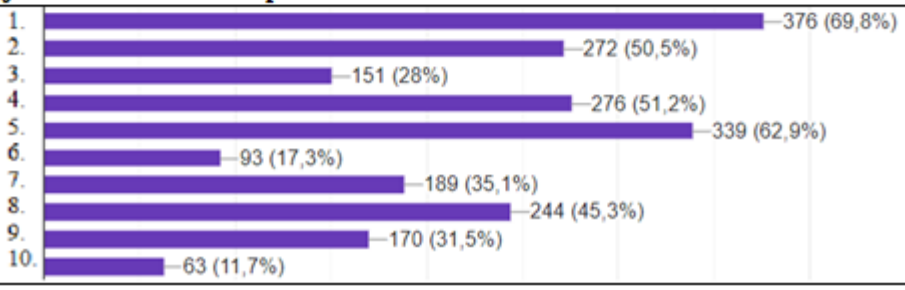
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

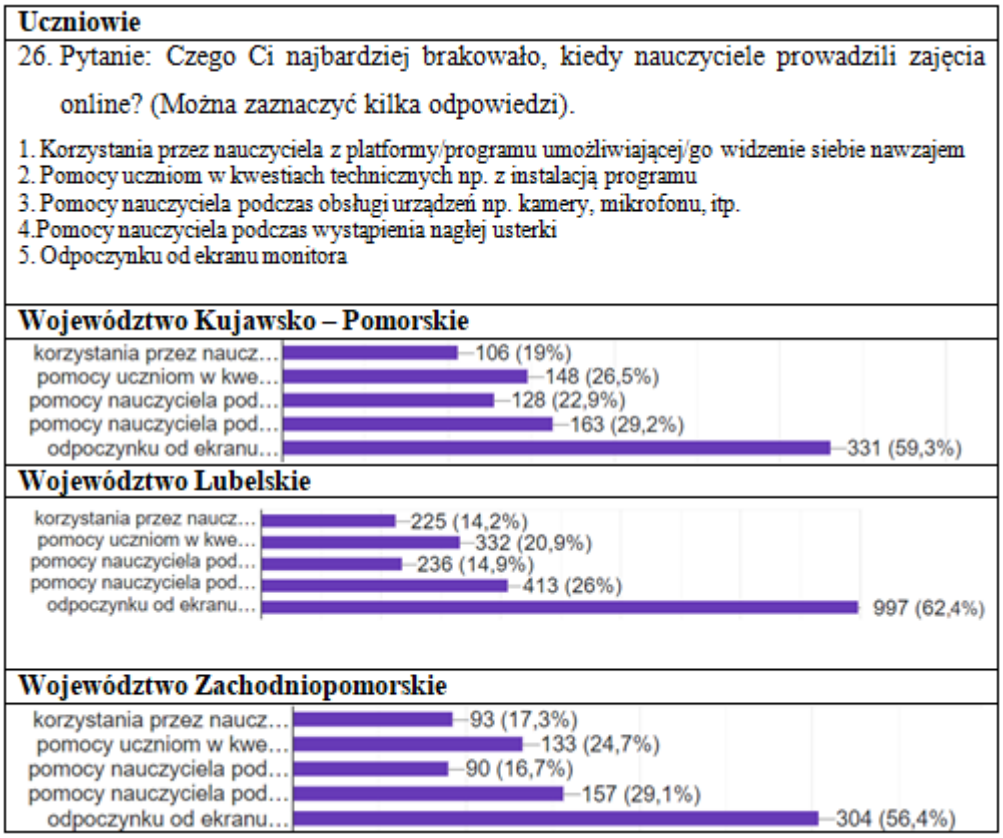


Województwo Zachodniopomorskie



Wykres 6.67. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- najczęściej wykorzystywana forma w zdalnym nauczaniu (źródło: opracowanie własne)

Poza wskazaniem wad i zalet uczniowie zostali poproszeni o zaznaczenie czego najbardziej im brakowało podczas zajęć online. Ponad połowa respondentów w każdym z województw stwierdziła, że najbardziej odczuwają brak odpoczynku od ekranu monitora. Następnie wskazywano także, że istnieje potrzeba pomocy nauczyciela w kwestiach technicznych oraz podczas usterki. Takie problemy zgłaszało pomiędzy 20 a 30% badanych. Najmniej doskwierał uczniom brak wsparcia nauczyciela podczas obsługi kamery i mikrofonu oraz brak obrazu z kamery dorosłego. Te odpowiedzi otrzymały najmniej głosów. Wyniki przedstawiono na poniższym wykresie 6.68.



Wykres 6.68. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- największe braki w nauczaniu w trybie zdalnym (źródło: opracowanie własne)

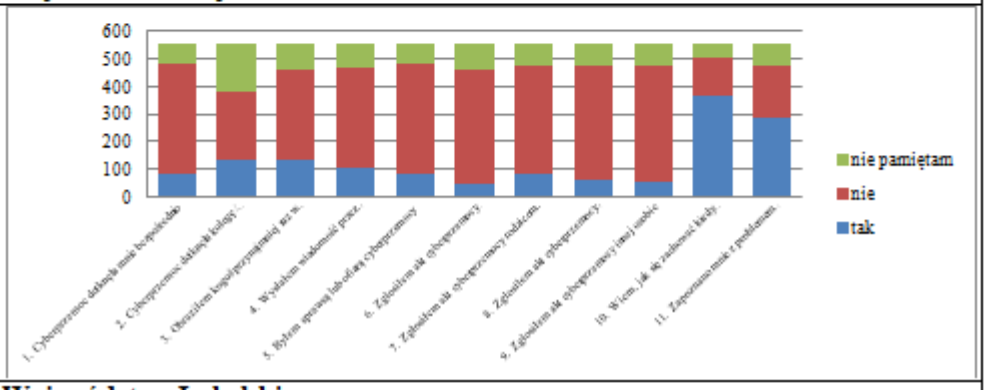
Ostatnie tematyczne pytanie (wykres 6.69.) odnosiło się do zjawiska cyberprzemocy. Jak można ocenić na poniższych wykresach, wyniki ze wszystkich województw są bardzo do siebie zbliżone. Poddając je analizie, większość uczniów bezpośrednio nie doświadczyła cyberprzemocy. Wypowiadając się o swoich rówieśnikach, uczniowie również wykazali niewielki odsetek przypadków wystąpienia cyberprzemocy. W większości cyberprzemoc nie dotykała ich kolegów i koleżanek lub nie pamiętają takiej sytuacji. Ponadto większość badanych uczniów nie przyznaje się do obrażania innych w mediach społecznościowych lub przez komunikatory internetowe. Sondaż potwierdził również, że ankietowani nie czują się sprawcą ani ofiarą cyberprzemocy oraz nie zgłaszali jeszcze aktu cyberprzemocy nauczycielowi, rodzicom, administratorom czy innym osobom. Niewiele ponad połowa badanych uczniów została zapoznana z problemem cyberprzemocy oraz wie, jak się zachować w przypadku wystąpienia takiego zjawiska. Taki wynik może sugerować konieczność zwiększenia nacisku na rozpowszechnienie pojęcia cyberprzemocy w szkołach, aby większa liczba uczniów wiedziała i była świadoma, jak ma się zachować oraz do czego stosowanie cyberprzemocy może prowadzić.

Uczniowie

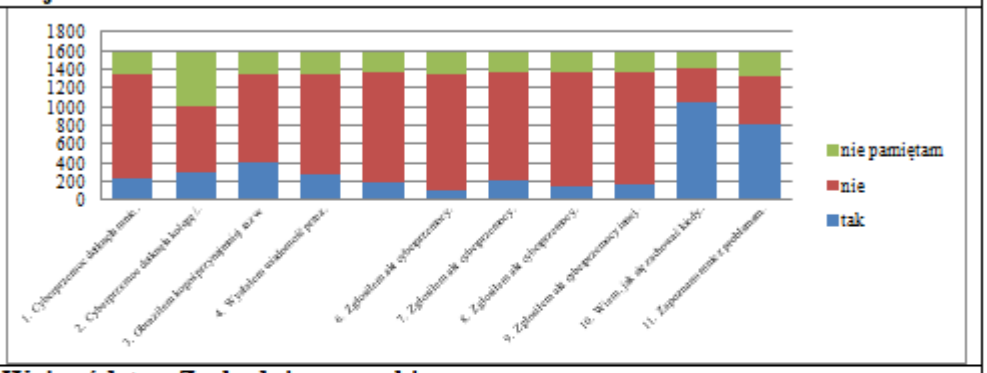
27. Pytanie: Czy spotkałeś się z cyberprzemocą (nękanie, dręczenie, prześladowanie w Internecie)? (Proszę odnieść się do <u>każdego</u> z podpunktów).

1. Cyberprzemoc dotknęła mnie bezpośrednio
2. Cyberprzemoc dotknęła kolegę / koleżankę z klasy
3. Obraziłem kogoś przynajmniej raz w mediach społ.
4. Wysłałem wiadomość przez komunikator (przynajmniej raz), by kogoś obrazić
5. Byłem sprawcą lub ofiarą cyberprzemocy
6. Zgłosiłem akt cyberprzemocy nauczycielowi
7. Zgłosiłem akt cyberprzemocy rodzicom / rodzeństwu
8. Zgłosiłem akt cyberprzemocy administratorowi sieci
9. Zgłosiłem akt cyberprzemocy innej osobie
10. Wiem, jak się zachować, kiedy występuje zjawisko cyberprzemocy
11. Zapoznano mnie z problemem cyberprzemocy

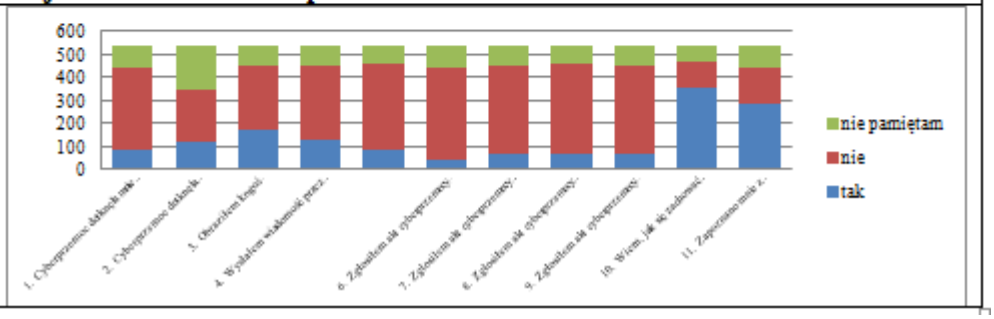
Województwo Kujawsko – Pomorskie



Województwo Lubelskie

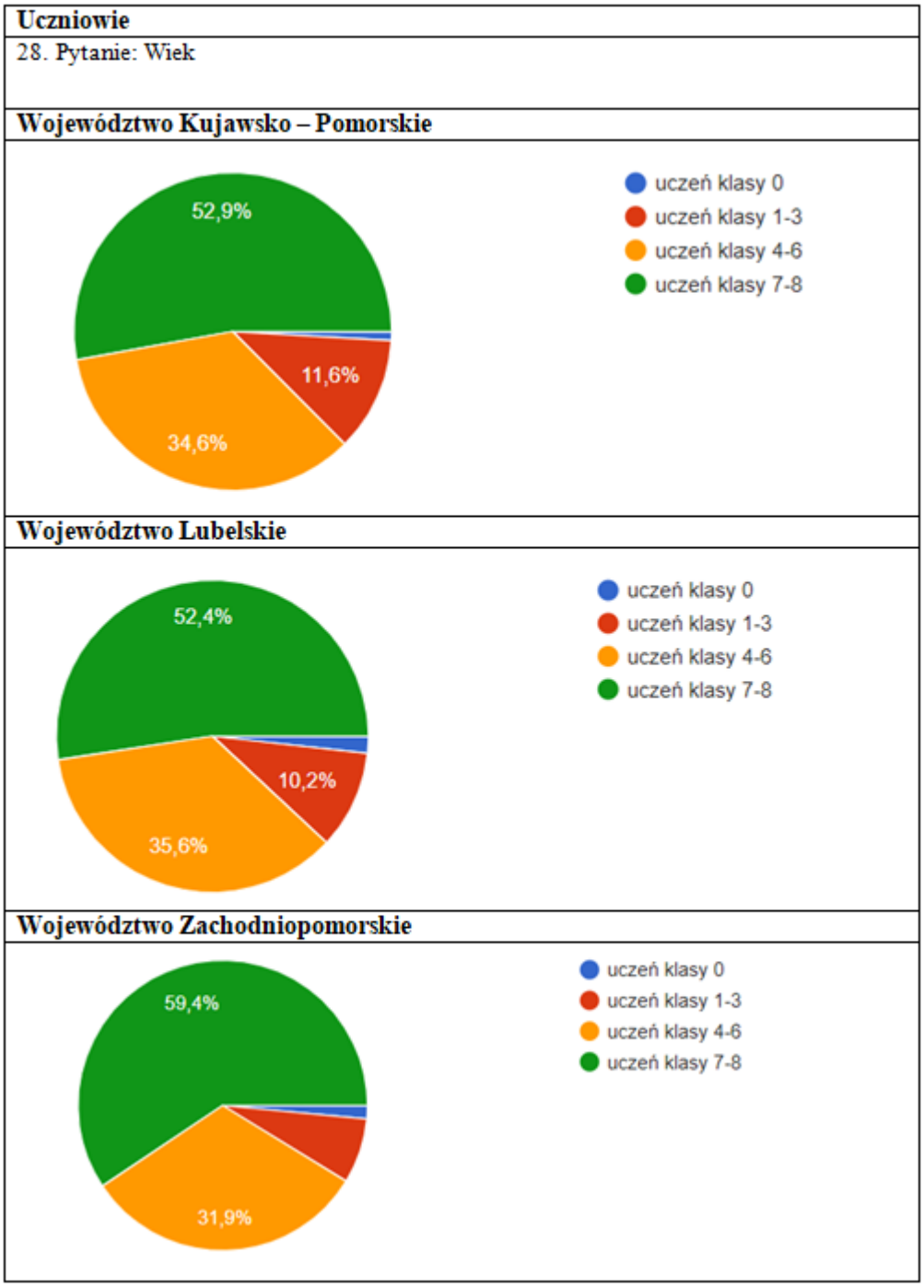


Województwo Zachodniopomorskie



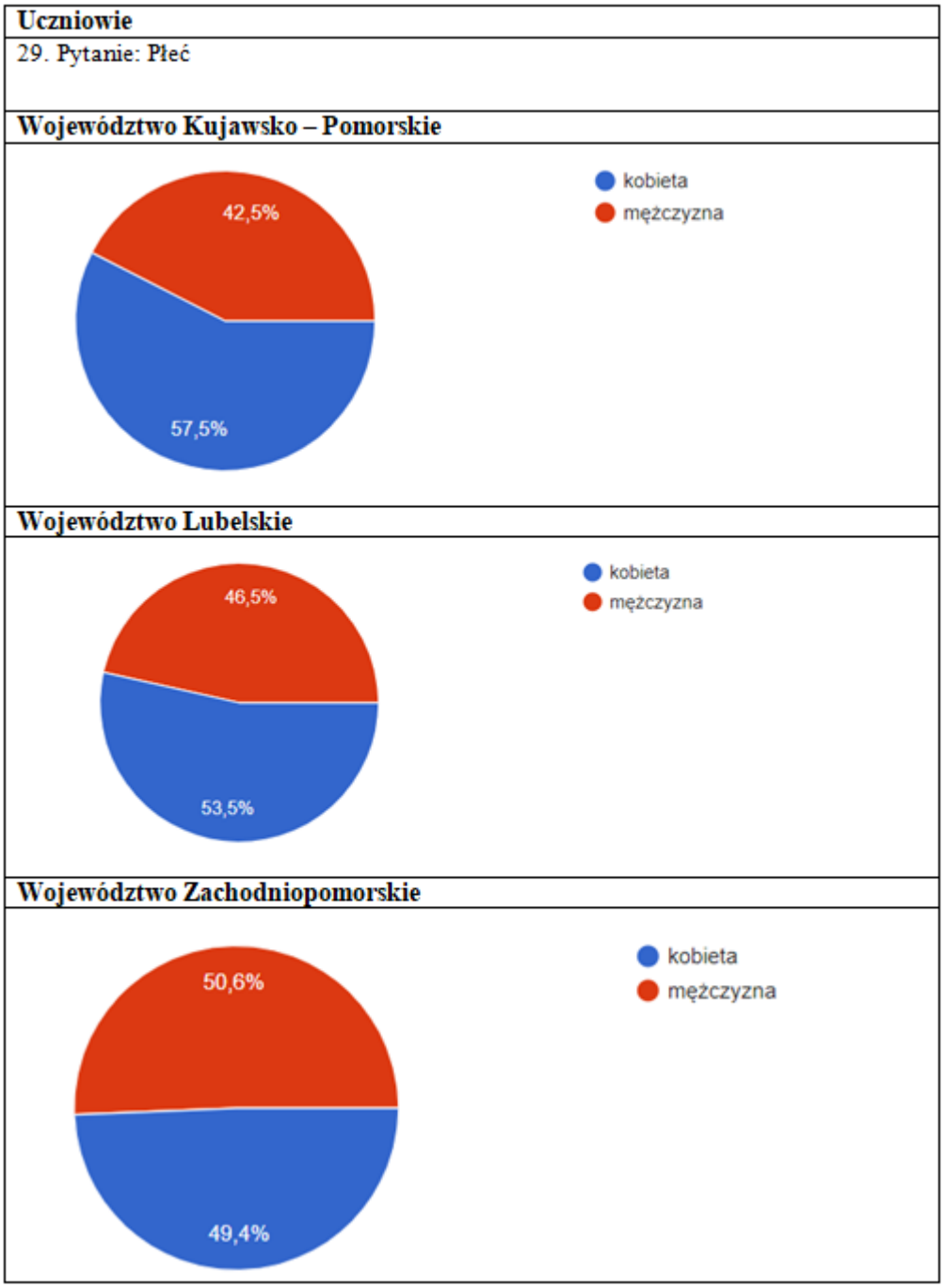
Wykres 6.69. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- zjawisko cyberprzemocy (źródło: opracowanie własne)

Procentowy udział uczniów poszczególnych klas prezentują poszczególne wykresy. Ponad 50% stanowią uczniowie klas 7-8, a w woj. Zachodniopomorskim stanowią oni aż 59,4% badanych. W każdym z województw wystąpiła również ponad 30 % grupa uczniów klas 4-6, a także około 10% grupa uczniów klasy 1-3. Najmniejsza grupę stanowili uczniowie klasy 0. Dane dotyczące wieku uczniów prezentuje poniższy wykres 6.70.



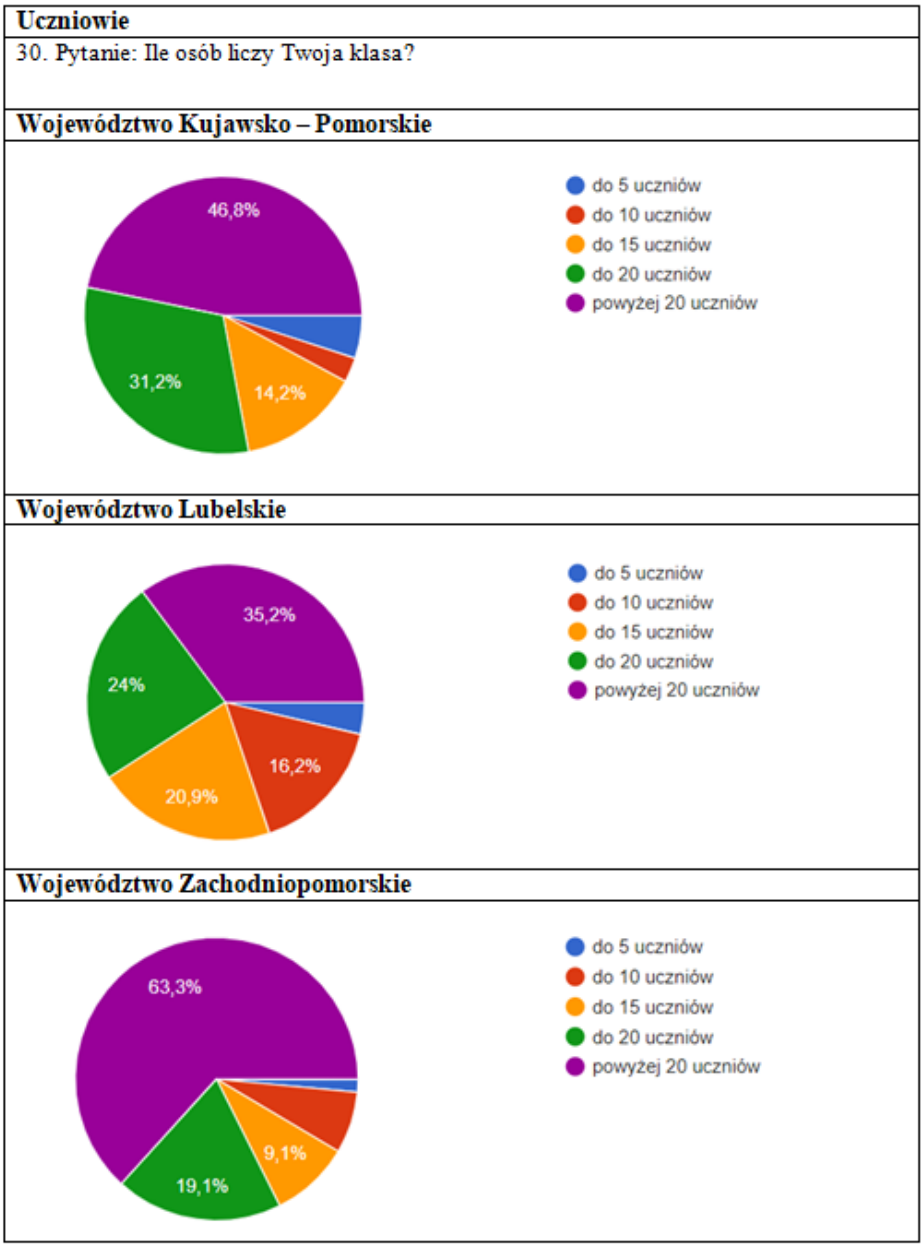
Wykres 6.70. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- wiek uczniów (źródło: opracowanie własne)

W pytaniu numer 29 zapytano o płeć badanych. Rozważając poniższe wykresy można zauważyć, że w badaniu udział wzięło 57,5% kobiet i 42,5% mężczyzn w woj. Kujawsko Pomorskim. W woj. Lubelskim kobiety stanowiły 53,5% badanych a mężczyźni 46,5%. Natomiast w woj. Zachodniopomorskim wystąpiła niewielka przewaga mężczyzn, którzy stanowili 50,6% badanych nad kobietami, których liczebność stanowiła 49,4% ankietowanych.



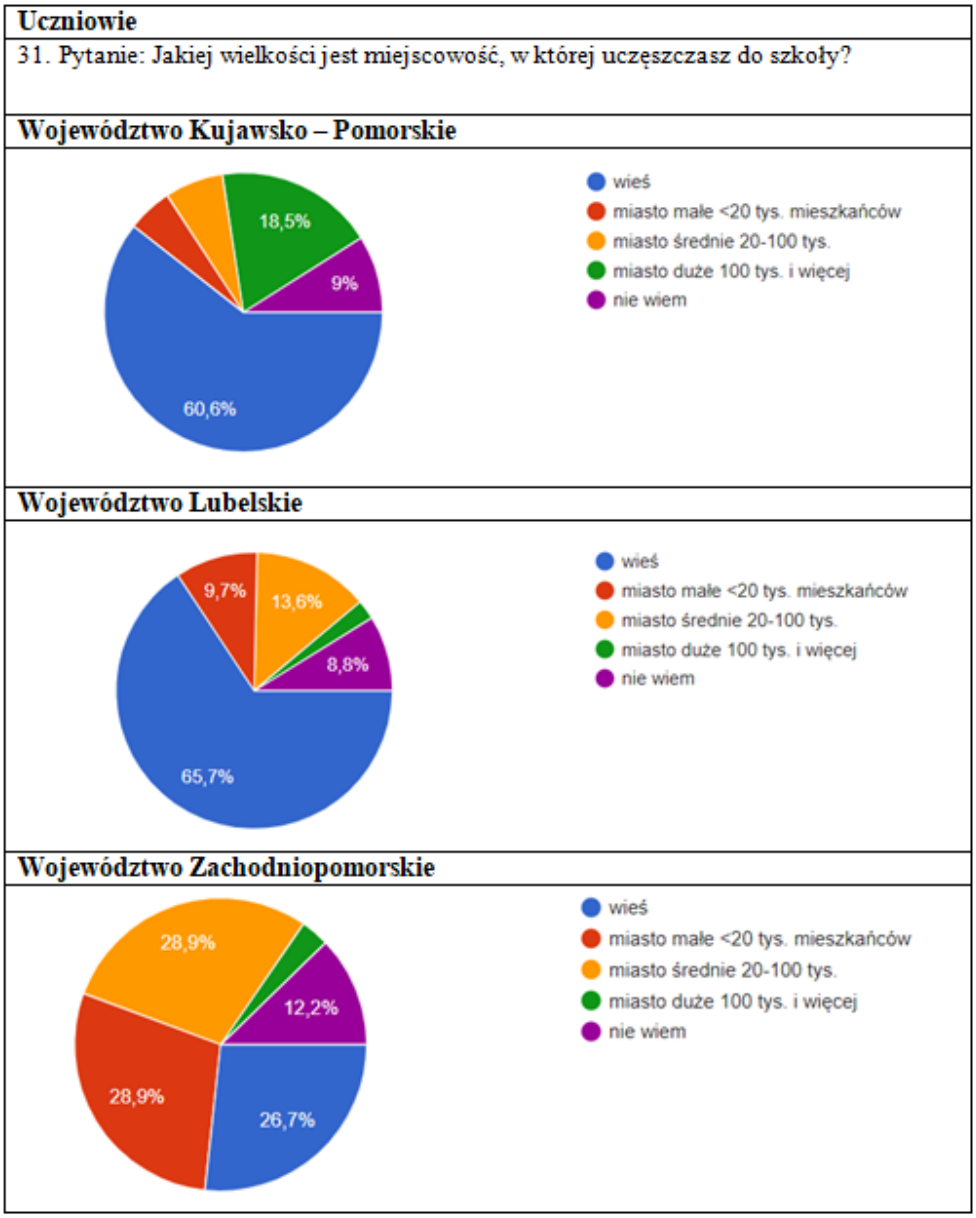
Wykres 6.71. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- płeć badanych (źródło: opracowanie własne)

W pytaniu numer 30 uczniowie zostali poproszeni o określenie liczebności ich klasy. Można spostrzec, że aż 63,3% uczniów z woj. Zachodniopomorskiego uczy się w klasach mających powyżej 20 uczniów. W pozostałych województwach odsetek ten jest znacznie mniejszy i stanowi 46,8% w woj. Kujawsko - Pomorskim oraz 35,2% w woj. Lubelskim. Najmniejsza grupa uczniów uczęszczający do klas liczących maksymalnie 20 uczniów jest w woj. Zachodniopomorskim (19,1%) a największa w Kujawsko – Pomorskim (31,2%). W woj. Lubelskim występuje największy odsetek uczniów klas maksymalnie piętnastoosobowych (20,9%) oraz dziesięcioosobowych (16,2%).



Wykres 6.72. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- liczebność klas (źródło: opracowanie własne)

W ankiecie odpowiedzi udzieliło 60,6% uczniów zamieszkujących wsie w woj. Kujawsko – Pomorskim oraz 65,7% w woj Lubelskim. W woj. Zachodniopomorskim mieszkańców wsi było znacznie mniej (tylko 26,7% badanych). Odwrotnie było w przypadku innych miejscowości. Mieszkańcy średnich i małych miast stanowili po 28,9% badanych w woj. Zachodniopomorskim, a w woj. Lubelskim jedynie 13,6% (średnie miasta) i 9,7% (małe miasta). Kolejną różnicą występującą pomiędzy województwami jest udział mieszkańców dużych miast w badaniu, który wynosi aż 18,5% w woj. Kujawsko – Pomorskim, zaś w pozostałych jest niewielki. Dane przedstawia wykres 6.73.



Wykres 6.73. Odpowiedzi ankietowanych uczniów z trzech wybranych województw- określenie wielkości miejscowości (źródło: opracowanie własne)

Analiza wyników badań wśród uczniów:

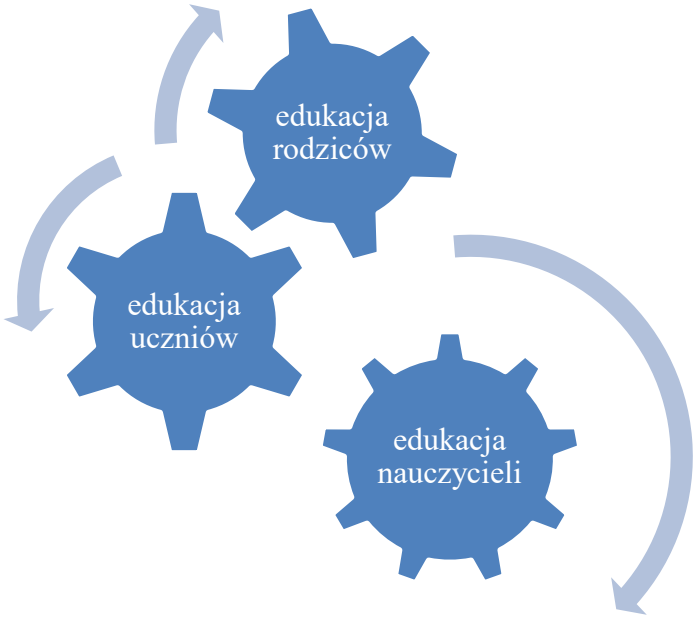
- codzienne korzystanie z komputera deklaruje ok. 40% badanych, również tyle samo osób użytkuje to urządzenie przynajmniej raz w skali tygodnia- co bezsprzecznie potwierdza fakt obecności sieci w życiu człowieka;
- kontrola podczas użytkowania komputera najmniej korzystanie wypada w woj. Zachodniopomorskim, gdzie blisko ¼ uczniów nie jest w jakikolwiek sposób ograniczana, tak więc opiekuni czy rodzice powinni poczuć się zdecydowanie bardziej odpowiedzialni za ten obszar;
- podobnie jak w przypadku nauczycieli, uczniowie potrafią wyszukać informację czy plik w komputerze i sieci, zainstalować aplikacje oraz gry, zamieszczać zdjęcia; trudności występują natomiast w czasie edytowania grafiki, tworzenia prezentacji czy czynności technicznych komputera;
- otwarcie linku otrzymanego od znajomego w serwisie społecznościowym to 10% respondentów, większość zastanowi się przed wykonaniem jakiejkolwiek czynności;
- regulaminy i instrukcje podczas instalowania nowych programów i aplikacji nie są zainteresowaniem blisko 40 % młodych osób, większość z nich przechodzi etap instalacji klikając „dalej, dalej”;
- ¼ ankietowanych nie potafiła zdecydować, czy Internet jest niebezpiecznym miejscem, zaś 10 % nie uważa sieci jako źrodła zagrożeń, co jest podstawą do twierdzenia, iż świadomość cyberzagrożeń jest zdecydowanie zbyt niska;
- najbardziej rozpoznawalne cyberzagrożenia: stalking, spam oraz koń trojański (identycznie jak w przypadku nauczycieli), największy brak wiedzy w tym zakresie wykazali uczniowie woj. Lubelskiego;
- najczęstsze problemy podczas zdalnego nauczania: zmęczenie spowodowane koniecznością pracy przed ekranem monitora; słabe połączenie internetowe nauczyciela jak i własne;
- niespełna 80 % uczniów opowiedziało się za edukacją cyfrową już od najmłodszych lat, jest to pozytywna przesłanka mogąca stanowić podstawę do twierdzenia o potrzebie wczesnego nauczania bezpiecznego zachowania w Internecie, czego odzwierciedlenie znaleźć można w innych odpowiedziach dostrzegających niewystarczającą ilość czasu przeznaczanego na opisywany zakres zajęć;
- ponownie, podobnie jak w przypadku wyników badań wśród nauczycieli, uczniowie najchętniej wykorzystują tradcyjne metody zapamiętywania haseł (tj. za-

pamiętanie w głowie, zapisanie na kartce/ w zeszycie), zaistniały również głosy o użyciu ustawień przeglądarki jako przechowującej hasła, co w momencie uzyskania dostępu do komputera może być niewymagającym celem cyberprzestępcy;

- do najbardziej dotkliwych problemów podczas zdalnego nauczania zaliczono zmęczenie spowodowane przebywaniem przed ekranem monitora i słabe połączenie internetowe, zwrócić uwagę należy na aspekt umożliwienia całemu społeczeństwu korzystania z zasobów Internetu w równym stopniu, niezależnie od miejsca zamieszkania;
- wśród wad edukacji cyfrowej znalazły się odpowiedzi dotyczące braku kontaktu z rówieśnikami (ok. 70 %) czy trudności związane z problemem przekazania i zrozumienia złożonych tematów czy zagadnień;
- cyberprzemoc (nękanie, dręczenie, prześladowanie w Internecie) nie dotknęła większości uczniów; jednak jedynie nieco połowa z nich została zapoznana z tematyką cyberprzemocy w szkole, zatem wynik może sugerować niezbędną konieczność i potrzebę wzrostu świadomości szkolnej w zakresie zapobiegania zjawiskom cyberprzemocy;
- blisko 90 % badanych- uczniowie klas 4-8.

6.3. Koncepcja zmian w zakresie włączenia zadań w obszarze budowania i podnoszenia świadomości społecznej cyberbezpieczeństwa jako elementu struktury krajowego systemu cyberbezpieczeństwa RP

Szkolenie w zakresie bezpiecznych zachowań w cyberprzestrzeni jest procesem, na który składają się różne czynniki. Najważniejsze stanowią podmioty, czyli osoby biorące udział w tym procesie. Ponieważ cyberbezpieczeństwo zależy od wszystkich, począwszy od nauczycieli, przez rodziców, osoby dorosłe, rówieśników, a na uczniach skończywszy. Każdy ma swój wkład w tworzenie bezpiecznego cyfrowego świata.



Rys. 6.1. Istota szkolenia w zakresie cyberbezpieczeństwa najmłodszych
(źródło: opracowanie własne)

Edukacja adresowana do najmłodszych w zakresie bezpieczeństwa w sieci powinna być oparta na rzetelnych doniesieniach i faktach dotyczących[288]:

- cyfrowych praktyk i opinii, wiedzy oraz postaw rodziców wobec sieci- internetu, świadomości cyberzagrożeń;
- cyfrowych praktyk dzieci oraz młodzieży (zasad korzystania z cyfrowych urządzeń, aktywności online, podejmowanych zachowań w sieci), dostrzeganych przez nich problemów związanych z obecnością w cyberprzestrzeni;

[288] A. Borkowska, 2023, *Uczeń w cyfrowym świecie. Jak projektować działania profilaktyczne w szkole i przedszkolu*, Wydawnictwo PIB NASK, Warszawa, s. 14, https://it-szkola.edu.pl/publikacje,plik,97 – [dostęp 04.05.2024 r.].

- efektywnych i skutecznych strategii w zakresie profilaktyki (co nie działa, co działa, dlaczego, w jaki sposób, na jakiego odbiorcę);
- realnych danych odnoszących się do identyfikowanych zagrożeń u dzieci i młodzieży i wynikających z nich ewentualnych, potencjalnych szkód dla ich rozwoju i zdrowia.

Współcześnie, w profilaktyce najczęściej występującym podejściem jest tzw. profilaktyka pozytywna, której celem nie jest koncentracja na usuwaniu samych zagrożeń (ponieważ ich całkowite wyeliminowanie jest wręcz niemożliwe) – celem jest wzmocnienie cech, zasobów i umiejętności, czyli czynników chroniących, dzięki którym młodzi ludzie będą bardziej odporni na zagrożenia. W obszarze bezpieczeństwa w Internecie, można wymienić przykłady działań zmierzających do zintensyfikowania czynników chroniących[289]:

- uczenie i rozwijanie kompetencji cyfrowych;
- uczenie skutecznych sposobów radzenia ze stresem;
- promowanie logicznego korzystania z internetu;
- zwiększanie i rozwój umiejętności psychospołecznych dzieci;
- nabywanie i podtrzymywanie umiejętności krytycznego podejścia do treści dostępnych online;
- angażowanie w zajęcia mające na celu rozwój zainteresowań i wzmacnianie relacji z osobami z najbliższego otoczenia (tj. rówieśnikami, rodzicami, ważnymi dorosłymi). Redukować wpływ czynników ryzyka powinno opierać się na m.in. ograniczaniu dostępu do treści online, kontroli czasu przebywania w sieci, ograniczeniu aplikacji oraz gier nieodpowiednich do wieku dzieci, wdrażaniu do urządzeń dzieci programów kontroli rodzicielskiej i programów blokujących pewne treści np. reklamowe.

Zmiany powinny dotyczyć również podstaw programowych w szkołach. Jak już wcześniej wspomniano, kwestie cyberbezpieczeństwa należy poruszać nie tylko na zajęciach z informatyki. W rzeczywistości tak naprawdę każdy nauczyciel może dodawać „cegiełkę" w procesie budowania świadomości i kompetencji cyfrowych uczniów. Bowiem np. na lekcjach z języka obcego warto jest odkrywać określenia i znaczenia pojęć w zakresie cyberprzestrzeni. Język polski (edukacja polonistyczna) jest idealnym przykładem aby tworzyć opracowanie, historie, przygody różnych bohaterów dotyczące

[289] Ibidem.

bezpiecznych zachowań w sieci. Na zajęciach z plastyki można przygotować grafikę czy plakat ilustrujący kwestie, zasady cyberhigieny w sieci. W ramach edukacji społecznej istotne jest poruszanie tematów związanych z udostępnianiem wizerunku w sieci, czasem spędzanym w sieci czy konsekwencjach wynikających z tego typu „aktywności" (problemy ze wzrokiem, wady postawy, nadwaga, zaburzenia koncentracji, zaburzenia rozwoju, słabszy rozwój tzw. myślenia przestrzennego).

Prof. Śliwerski, stwierdził, że „w procesie doskonalenia i kształcenia zawodowego nauczycieli uświadamia się im, iż są oni włączeni w dynamikę rozwoju społecznego, tak swoich instytucji oświatowych, jak i poza społeczną przestrzeń edukacyjną. Tak więc nauczyciele powinni podjąć aktywną rolę w procesie reformowania oświaty, ale też w szerszej perspektywie uczestniczyć w stymulowaniu rozwoju całej przestrzeni społecznej". W związku z powyższym, na szczególne uwzględnienie zasługuje kształcenie nauczycieli w obszarze cyfrowych kompetencji. Wyzwanie to winno stanowić fundament w planowaniu kierunków rozwoju społeczeństwa informacyjnego w Polsce[290].

Bardzo ważne jest właściwe podejście rodziców w zakresie ograniczania używania urządzeń cyfrowych na co dzień. W jaki sposób ograniczać ekrany przy dziecku? Poniżej wyszczególniono tzw. zasady ekranowe[291]:

- pozostawanie w kontakcie- spędzając czas z dzieckiem, należy starać się być całkowicie obecnym. skupić się na jego potrzebach jak i wspólnych aktywnościach. starać się nie myśleć o telefonie i nie spoglądać na ekran;
- ograniczenie czasu do minimum, korzystając z telefonu przy dziecku. zawsze warto rozważyć, czy skorzystanie z telefonu jest niezbędne i czy nie może poczekać. jeżeli sięga się po telefon, powinno się ograniczać czas ekranowy do minimum;
- strefy bez ekranu- należy ustalić miejsca wolne od telefonu, jak np. pokój dziecka, miejsce spożywania posiłku, kącik do zabaw bądź miejsce do czytania;
- sytuacje bez ekranów- sytuacje kluczowe w relacji z dzieckiem i dla jego komfortu, podczas których nikt nie korzysta z telefonu, np. zasypianie, czytanie, posiłki, wspólna zabawa;

[290] https://cyfrowekompetencje.pl/articles/ksztaltowanie-kompetencji-cyfrowych-nauczycieli-nowe-stare-wyzwania-spoleczenstwa-informacyjnego-w-polsce - [dostęp 04.05.2024 r.].
[291] https://www.domowezasadyekranowe.fdds.pl/problem/ - [dostęp 04.05.2024 r.].

- miejsce na telefon- warto nie trzymać ciągle telefonu przy sobie. pomocne może być wskazane miejsce, gdzie odkłada się telefon na czas interakcji z dzieckiem. miejsce to może być wspólne dla wszystkich domowników;
- wyłączenie powiadomień sprawi, że rodzic i dziecko będą mniej rozproszeni;
- informowanie dziecka- jeśli istnieje konieczność skorzystania z telefonu przy dziecku, należy mu wytłumaczyć, w jakim celu się to robi, tak aby zminimalizować jego frustrację.

Rozwój kompetencji cyfrowych nie jest możliwy w sytuacji zapewnienia dostępu do Internetu i urządzeń cyfrowych. Samo ich posiadanie to zbyt mało. Są to tzw. bariery twarde, których ograniczenie nie jest wystarczające. Coraz większego znaczenia nabierają bariery miękkie, czyli brak właściwych kompetencji czy wiedzy w zakresie sieci.

Kompetencje cyfrowe nie powinny być utożsamiane z kompetencjami informatycznymi. Albowiem w skład kompetencji cyfrowych wchodzą umiejętności techniczne, informatyczne, ale także umiejętności w zakresie m.in. wyszukiwania informacji, oceny jej przydatności i wiarygodności.

Kompetencje cyfrowe jako fundament systemu cyberbezpieczeństwa powinny opierać się na specjalistach w swojej dziedzinie. To znaczy, iż aby mógł się dokonywać rozwój gospodarki, niezbędne będą właśnie osoby z najwyższymi, zaawansowanymi kompetencjami. Ich rozwój uzależniony będzie od specjalistycznych szkoleń, specjalizacji czy studiów doktoranckich. Zaś zachętą do doskonalenia własnej wiedzy i umiejętności będą zapewne wyższe zarobki wymienionych ekspertów.

Powiązana z powyższym twierdzeniem jest konieczność wypracowania mechanizmów podnoszenia i kontroli jakości, przede wszystkim szkoleń. Identyfikacja dobrych praktyk, tzw. lessons learned czy system wykorzystywania doświadczeń pozwoli na jeszcze bardziej złożone dyskusje i wymiany spostrzeżeń oraz wniosków.

6.4. Wnioski

Zidentyfikowane problemy badawcze wraz z odpowiedziami:

- Jakie czynniki i działania mają wpływ na budowanie świadomości cyberzagrożeń oraz cyfrowych kompetencji użytkowników w zakresie cyberbezpieczeństwa?

- personalne (z punktu widzenia użytkownika): wiek, umiejętności, wykształcenie, wiedza, świadomość, rodzaj wykonywanej pracy, uczestnictwo w grupach społecznych, doświadczenia z sieci, miejsce zamieszkania;
- centralne (z punktu widzenia państwa): aktualizacja rozwiązań prawnych i strategicznych, powoływanie instytucji i podmiotów, tworzenie i rozwój towarzystw informatycznych, zwiększanie środków finansowych w obszarze cyberbezpieczeństwa, działania programowe w skali kraju czy nawet europejskiej, rozwój współpracy sektorowej.

Eksperci podkreślają działania na szczeblu całego kraju, tak aby żadna nawet najmniejsza komórka społeczna nie była pozostawiona oddzielnie. Ponadto, uwypukla się znaczenie samorządu terytorialnego, który to powinien prowadzić autonomicznie swego rodzaju działania mające na celu podwyższenie poziomu cyberbezpieczeństwa mieszkańców.

- Które przepisy regulują kwestie cyberbezpieczeństwa w RP?

Pierwszy, jakże znaczący zapis w zakresie bezpieczeństwa państwa (ściślej: bezpieczeństwa cyberprzestrzeni) ujęto w art. 228. Konstytucji RP, który stanowi: „W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.

Wdrożenie sfery cyber do stanów nadzwyczajnych ujęto w ustawie z dnia 30.08.2011 r. o zmianie ustawy o stanie wojennym. Kolejna znowelizowana już ustawa stanowi, iż którykolwiek ze stanów nadzwyczajnych może zostać wprowadzony w związku z działaniami w cyberprzestrzeni.

Pierwsze europejskie prawo w zakresie cyberbezpieczeństwa stanowi wprowadzona w 2016 roku tzw. *Dyrektywa NIS (Network and Information Systems Directive).*

Dokument ten nakłada na państwa członkowskie szereg obowiązków, obliguje je do stworzenia konkretnych instytucji i wprowadza określone mechanizmy współpracy. Pomysł dyrektywy zakładał stan faktyczny, iż kraje UE różnią się od siebie względem poziomu bezpieczeństwa sieci oraz systemów informatycznych, co przekłada się na ogólny poziom cyberbezpieczeństwa całej Unii.

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.

Implementację dyrektywy stanowi w RP – ustawa o krajowym systemie cyberbezpieczeństwa (2018). Ustawa, sama w sobie nie wprowadza środków, które byłyby przełomem czy innowacją w cyberbezpieczeństwie, natomiast stanowi źródło podstaw prawnych do stosowania tychże środków. Środków (organizacyjnych i technicznych), które de facto powinny być realizowane przed określone podmioty już od lat.

Od 27 czerwca 2019 r. obowiązuje *Cybersecurity Act*, co stanowi drugą regulację na poziomie europejskim w dziedzinie cyberbezpieczeństwa.

Akt o cyberbezpieczeństwie wskazuje trzy poziomy certyfikatów, tj. wysoki, istotny oraz podstawowy. Dzięki obranej metodologii np. przedsiębiorcy mogli będą łatwiej i szybciej dobrać certyfikat bezpieczeństwa do indywidualnych potrzeb. W związku z tym, jeśli ocenią, iż do przeciwdziałania podstawowym zagrożeniem właściwy będzie poziom najniższy, mają taką możliwość. Środkowy poziom pozwala na skuteczną ochroną przed atakami z ograniczonymi możliwościami. Najwyższy poziom ochrony wskazuje, iż produkt powinien być odporny na ataki sprawców o znaczących możliwościach i środkach (tak np. przed zorganizowanymi grupami dyponującymi ogromnymi funduszami).

Stosunkowo niedawno przyjęta *Dyrektywa NIS 2* ma na celu wzmocnienie bezpieczeństwa cybernetycznego w wybranych sektorach krytycznych na poziomie krajowym oraz unijnym. Przykładowo, zakres dyrektywy obejmuje szerzej podmioty z branży energetycznej jak i ochrony zdrowia oraz dostawców usług w obszarze infrastruktury cyfrowej. Rozszerzono również zakres samej dyrektywy, tak aby miała zastosowanie do nowych sektorów i podmiotów, tj. administracja publiczna, gospodarka odpadami i sektor spożywczy.

Oprócz wymienionych regulacji prawnych, istnieją także dokumenty strategiczne. W latach 2015-2017 powstawały próby podjęcia strategii i doktryny w zakresie cyberbezpieczeństwa, ale w zasadzie nie stanowiły jasnego wskazania zadań i działań służb państwowych w zakresie ochrony cyberprzestrzeni RP.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 wskazuje najważniejsze zadania: uzyskanie wysokiego poziomu cyberbezpieczeństwa – głównie odporności systemów informacyjnych, operatorów infrastruktury krytycznej, operatorów usług kluczowych, dostawców usług cyfrowych. Strategia określa cele strategiczne i środki polityczne, regulacyjne, mające na celu zyskanie i utrzymywanie wysokiego poziomu cyberbezpieczeństwa.

- Które ze wskazanych w przepisach podmiotów i instytucji mają określone zadania w obszarze budowania świadomości i kompetencji cyfrowych?
  - MEN;
  - Ministerstwo Cyfryzacji;
  - NASK;
  - Centrum Rozwoju Kompetencji Cyfrowych;
  - *ENISA*.

Rozwijanie kompetencji cyfrowych stanowi połączenie praktyki, nauki oraz cyklicznego kontaktu z technologiami cyfrowymi i różnymi narzędziami. Poniżej wskazano działania, które zdaniem autora mogłyby pozwolić na zwiększenie poziomu swoich umiejętności cyfrowych:

- samokształcenie: wiele umiejętności cyfrowych można wykształcić samodzielnie, korzystając z zasobów internetowych, takich jak fora i samouczki dostępne np. na platformie *YouTube*. Na przykład, chcąc nauczyć się programowania, dostępnych jest wiele bezpłatnych zasobów oraz społeczności, w których znaleźć można poradniki i zadania do ćwiczenia swoich umiejętności;
- kursy i samouczki online: istnieją platformy internetowe oferujące kursy w zakresie różnych umiejętności cyfrowych, począwszy od podstawowej obsługi komputera po zaawansowane przedsięwzięcia typu programowanie. Strony takie jak *Khan Academy*, *Coursera* czy *Udemy* zapewniają dostęp do kursów z marketingu cyfrowego, kodowania czy projektowania graficznego;
- współpraca i nawiązywanie kontaktów: dołączanie do społeczności internetowych, grup i forów w mediach społecznościowych związanych z obszarem zainteresowań może stanowić punkt wyjścia do współpracy z innymi, dzielenia się wiedzą i uczenia od doświadczonych profesjonalistów. Tzw. networking może również otworzyć drzwi do samorozwoju, mentoringu i rozwijania kariery;
- praktyczne projekty: jednym z najskuteczniejszych sposobów rozwijania kompetencji cyfrowych jest praca i zaangażowanie nad rzeczywistymi projektami. Niezależnie od tego, czy dotyczy to budowanie strony internetowej, tworzenia aplikacji mobilnej czy analizowania danych, praktyczne doświadczenie umożliwia jednostkom zastosować to, czego się nauczyły i zdobyć (udoskonalić) praktyczne umiejętności;
- ciągła nauka jako proces: cyfrowy krajobraz stale ewoluuje, dlatego kluczowe jest, aby być na bieżąco z najnowszymi technologiami i trendami. Angażowanie się

w ciągłe uczenie się poprzez webinaria, spotkania, kursy online, warsztaty i konferencje zapewnia, że poziom cyberbezpieczeństwa danego użytkownika będzie wzrastał;

- rozwój umiejętności miękkich: oprócz jakże ważnych i aktualnych umiejętności technicznych, rozwijanie umiejętności miękkich, takich jak komunikacja, rozwiązywanie problemów i praca zespołowa, ma kluczowe znaczenie w cyfrowym świecie. Umiejętności te stanowią uzupełnienie wiedzy technicznej i są wysoko cenione przez pracodawców;
- eksperymentowanie i odkrywanie: nie należy obawiać się odkrywać nowych narzędzi i technologii poza tzw. własną strefą komfortu. Wypróbowywanie innego oprogramowania, eksperymentowanie z językami kodowania i odkrywanie nowych technologii, jak obecnie nabierająca na znaczeniu sztuczna inteligencja, może poszerzyć umiejętności i zdolności adaptacyjne;
- szukanie informacji zwrotnych: warto jest rozmawiać o kompetencjach, o świadomości zagrożeń, o tym na co obecnie może być narażony użytkownik sieci. Dzieci, uczniowie powinny otrzymywać od nauczycieli (ale także rodziców) informacje zwrotne w zakresie swoich zachowań w Internecie i możliwości polepszenia danego stanu rzeczy. Konstruktywna krytyka pomoże zidentyfikować obszary wymagające poprawy i udoskonalić swoje kompetencje cyfrowe.

Państwo odgrywa kluczową rolę we wspieraniu rozwoju kompetencji cyfrowych społeczeństwa. Poniżej wskazano rozwiązania mogące wpłynąć na poprawę poziomu kompetencji cyfrowych:

- programy szkoleniowe: oferowanie bezpłatnych programów szkoleniowych w zakresie umiejętności cyfrowych dla obywateli z różnych środowisk i w każdym wieku. Programy mogą obejmować szeroki zakres tematów, tj. podstawowa znajomość obsługi komputera, cyberbezpieczeństwo, analiza danych, kodowanie, marketing cyfrowy. Stała współpraca z organizacjami sektora prywatnego, organizacjami *non-profit* i uniwersytetami może pomóc zwiększyć zasięg i skuteczność tychże inicjatyw;
- reforma edukacji: począwszy od wczesnej edukacji - włączenie umiejętności cyfrowych i myślenia obliczeniowego do programów nauczania, skończywszy zaś na szkolnictwie wyższym. Zmiany mogą dotyczyć aktualizacji istniejących kursów, wprowadzenia nowych przedmiotów i zapewnienia nauczycielom niezbędnych zasobów oraz szkoleń do skutecznego nauczania umiejętności cyfrowych.

- inwestycje w infrastrukturę: zapewnienie i umożliwienie powszechnego dostępu do szybkiego Internetu oraz urządzeń cyfrowych, w szczególności na obszarach o niedostatecznym zasięgu. Działanie to składa się z przedsięwzięć: zapewnianie dotacji dla gospodarstw domowych o relatywnie niskich dochodach na dostęp do Internetu, inwestowanie w infrastrukturę szerokopasmową i jedno z najważniejszych: wyposażanie szkół i domów kultury w komputery i pozostałe niezbędne technologie;
- zapewnienie finansowania, tzw. mentoringu i zasobów w celu wsparcia cyfrowych startupów oraz przedsiębiorców. Rozumie się przez to dotacje na badania i rozwój, programy inkubatorów, a także inne inicjatywy mające na celu łączenie przedsiębiorców z inwestorami oraz ekspertami branżowymi;
- budowanie integracji cyfrowej: przeciwdziałanie podziałom cyfrowym przez docieranie do zmarginalizowanych społeczności i zapewnianie im dostosowanego do ich potrzeb wsparcia w progresie kompetencji cyfrowych. Proces ten może obejmować partnerstwa z organizacjami społecznymi, zapewnianie wsparcia w dostępie do technologii i usług internetowych oraz oferowanie programów szkoleniowych dostosowanych do języka;
- promowanie otwartych danych: zachęcanie do przejrzystości i innowacji przez publiczne udostępnianie określonych danych rządowych w otwartych formatach. Zapewni to obywatelom nie tylko samą możliwość korzystania z danych rządowych, ale również stymuluje rozwój umiejętności analizy i wizualizacji danych;
- polityka i regulacje: opracowanie polityk i regulacji wspierających rozwój cyfrowej gospodarki przy jednoczesnym zagwarantowaniu ochrony praw i prywatności obywateli. W zakres polityki wpisuje się ustawodawstwo związane z ochroną danych, cyberbezpieczeństwem, prawami własności intelektualnej oraz dostępnością cyfrową;
- publiczne kampanie uświadamiające: rozpoczęcie publicznych kampanii uświadamiających, celem podkreślenia znaczenia umiejętności cyfrowych w dzisiejszym społeczeństwie i zachęcenia do uczenia się przez całe życie. Przedsięwzięcia te mogą podkreślać korzyści płynące z uzyskiwania kompetencji cyfrowych w zakresie edukacji, zatrudnienia, rozwoju osobistego i zaangażowania obywatelskiego.

Wdrażając powyższe strategie, rządy mogą odgrywać proaktywną i wiodącą rolę w wyposażaniu swoich obywateli w kompetencje cyfrowe niezbędne do rozwoju w coraz bardziej zdigitalizowanym świecie. Łącząc wymienione wyżej i angażując się w ciągłe uczenie się i doskonalenie, użytkownicy mogą skutecznie rozwijać swoje

kompetencje cyfrowe i z pełną świadomością poruszać się w dzisiejszym cyfrowym świecie.

- Jaki jest istniejący zakres wiedzy użytkowników oraz sposób jej pozyskiwania w zakresie cyberbezpieczeństwa?

Jak wskazuje analiza obszaru badawczego, dostępne wyniki obserwacji i przeglądy innych autorów, badanie zarówno sondażowe jak i eksperckie autora dysertacji, zakres wiedzy użytkowników można opisać jako podstawowy. Eksperci wskazują na zapisy podstawy programowej, które obejmują swoim zakresem wiele obszarów szczególnie istotnych dla najmłodszych. Wiedzę- uczniowie czerpią przede wszystkim od nauczycieli, rodziców, rodzeństwa, mniej natomiast jest dyskusji ze znajomymi. Nauczyciele natomiast zaangażowani bywają w różnego rodzaju kampanie, które zdaniem ekspertów zmieniają się w ramach potrzeb i są dostosowywane do coraz to nowych wyzwań. Odzwierciedlenie nauki i doskonalenia kwestii związanych z bezpiecznym poruszaniem się w świecie cyfrowym ma wskazywane jest podczas zajęć w ramach innych przedmiotów takich jak język polski, wiedza o społeczeństwie, etyka, język obcy nowożytny czy wychowanie do życia w rodzinie. W całym tym procesie nie należy zapominać o kadrach i specjalistach, których znaczenie jest nieocenione w przygotowywaniu świadomych użytkowników.

- Jakie standardy obowiązują w zakresie kompetencji cyfrowych?

Standardy mieszczą się w ramach tzw. *DigComp*, które zostały opisane w podrozdziale związanym z kompetencjami cyfrowymi.

- Jaki jest poziom kompetencji obywateli w zakresie cyberbezpieczeństwa?

W dużej mierze występuje niedobór wiedzy i świadomości w zakresie podstaw związanych z np. działaniem bieżącym w sieci i komputerze, tj. z rozpoznawaniem cyberzagrożeń, zabezpieczaniem swoich danych osobowych czy obsługą pakietu Office.

- Jaki jest poziom świadomości w obszarze cyfrowych zagrożeń wśród użytkowników sieci?

Świadomość zagrożeń jest procesem długotrwałym, na co wskazują zarówno eksperci jak i zebrane badania własne autora oraz innych twórców. Większość ankietowanych oceniło samodzielnie swoją świadomość w zakresie zagrożeń występujących w sieci jako średnia bądź wyższa. Ponad 1/3 przyjęła odpowiedź odnoszącą się do średniego poziomu. Stąd też sądzić można, że rzeczywiście jest wiele pracy do wykonania i do realizacji w obszarze własnego poczucia bezpieczeństwa. Bez wątpienia potwierdzeniem tego są opisywane badania własne, zgodnie z którymi niespełna połowa ankie-

towanych w pełni wierzy, iż sieć jest niebezpiecznym miejscem. To zdecydowanie za mało. W kwestii rozpoznawalności cyberzagrożeń jest również ogromne wyzwanie, ponieważ zaledwie ¼ respondentów potrafi ocenić czym jest phishing. Wiedza ogranicza się do zdefiniowania jedynie tych najbardziej popularnych zjawisk.

- Jakie istnieją metody i obszary edukacji użytkowników?

Do metod zaliczyć należy naukę w szkole, dyskusje z rodziną i znajomymi, samokształcenie, udział w kampaniach uświadamiających oraz szkolenia. Głównymi obszarami są natomiast: rozumienie i analizowanie problemów, rozwiązywanie problemów, posługiwanie się komputerem i urządzenia cyfrowymi, rozwijanie kompetencji cyfrowych, przestrzeganie higieny cyfrowej i kwestii etycznych.

- Które z zagrożeń w dziedzinie cyberbezpieczeństwa mogą oznaczać największe wyzwanie dla funkcjonowania państwa?

Najbardziej znaczącym zagrożeniem wskazane są cyberwojna i cyberterroryzm jako te mogące mieć największe skutki w ramach właściwego funkcjonowania i organizacji państwa. Jednakże, pośrednio już cyberzagrożenia, z którymi spotykają się najmłodsi mogą mieć ogromne znaczenie dla całego systemu. Infrastruktura krytyczna państwa jest elementem szczególnie narażonym na wpływ cyberprzestępców. Mowa nienawiści, hejt czy szkodliwe treści mogą niosą katastrofalne implikacje w rozwoju każdego człowieka. Fake newsy czy deepfake'i przyczynić się mogą do powstania wręcz zamieszek, te zaś związane są bezpośrednio z bezpieczeństwem państwa i narodu. Eksperci wskazują również osobę będącą po drugiej części ekranu jako tę będącą najpoważniejszym zagrożeniem. Ponadto, należy mieć świadomość, iż cyberzagrożeń nie da się wyeliminować. Można jedynie prowadzić działania mające na celu ich redukcję czy likwidację (łagodzenie) ewentualnych ich skutków. Zagrożenia zawsze już będą obecne w sieci.

- Czy kompetencje cyfrowe mogą mieć wpływ na poziom cyberbezpieczeństwa?

Tak, zdecydowanie te kompetencje są kluczowe. Krytyczne, zdroworozsądkowe myślenie ma ogromne znaczenie w kwestii swojego oraz wspólnego cyberbezpieczeństwa. Nikt nie powinien zostać pominięty, cyberbezpieczeństwo musi być rozwijane zarówno w miastach jak i terenach wiejskich, z uwagi na fakt, iż dostęp do Internetu jest w zasadzie powszechny. Warto zwrócić uwagę na tzw. „ślad cyfrowy", który powinien być bezwzględnie chroniony przez każdego użytkownika, dbając o poufność danych, nie ujawniając zbyt wielu informacji i nie nawiązując bliższych znajomości z niezweryfikowanymi osobami. Odzwierciedlenie powyższego ujęto w opiniach ekspertów, zwra-

cających uwagę na istotne znaczenie użytkownika w ramach całego systemu cyberbezpieczeństwa.

Zakończenie

Cyberprzestrzeń i związane z nią zmiany stają sie przedmiotem zainteresowania zarówno polskich badaczy jak i wielu zagranicznych przedstawicieli rożnych dziedzin nauki i organizacji. Rozwój technologii teleinformatycznych definiuje potrzeby wyposażenia społeczeństwa w odpowiednie narzędzia i środki do zapobiegania określonym cyberzagrożeniom. W niniejszej pracy podjęto problem badań diagnozujących poziom kompetencji cyfrowych użytkowników Internetu w kontekście budowania ich świadomości.

W dysertacji celem głównym badań było zbadanie istniejących rozwiązań w zakresie działań państwa polskiego realizowanych w ramach systemu cyberbezpieczeństwa RP na rzecz budowania i podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP. Stąd w strukturze rozprawy cel ten przewijał się częściowo we wszystkich rozdziałach, gdyż odnoszono się w nich do szczegółowych problemów badawczych, które wynikają z głównego problemu badawczego: jakie czynniki i działania mają wpływ na budowanie świadomości cyberzagrożeń oraz cyfrowych kompetencji użytkowników w zakresie cyberbezpieczeństwa?

Dokonano analizy rozwiązań w zakresie działań państwa polskiego realizowanych na rzecz budowania oraz podnoszenia kompetencji cyfrowych użytkowników. Określono miejsce Krajowego Systemu Cyberbezpieczeństwa w całym systemie cyberbezpieczeństwa RP. Wskazano podmioty i instytucje kluczowe w obszarze cyberbezpieczeństwa. Oszacowano poziom wiedzy i umiejętności użytkowników sieci. Zidentyfikowano cyberzagrożenia szczególnie istotne z punktu widzenia funkcjonowania państwa. Poprzez badanie sondażowe wzbogacona została wiedza w zakresie poziomu świadomości cyberzagrożeń i kompetencji cyfrowych. W ramach wywiadów eksperckich dokonano oceny kierunków kluczowych zagrożeń w dziedzinie cyberbezpieczeństwa, uzyskano opinie na temat realizowania zadań w obszarze budowania świadomości i cyfrowych kompetencji oraz ocenę sposobów edukacji i metod użytkowników sieci. Kluczowe wnioski zawarto w zakończeniu podrodziału 6.1. Wywiady eksperckie oraz 6.2. Badanie sondażowe. Zamierzone cele pracy zostały osiągnięte.

Dla zweryfikowania hipotezy o treści: skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa, wygenerowano szczegółowe problemy badawcze rozpatrywane kolejno, zakończone każdorazowo wnioskami.

Hipoteza została zweryfikowana pozytywnie, a problem badawczy – rozwiązany. W trakcie badań opracowano zasadniczy wniosek, jednocześnie założenie teoretyczne, iż systematyczne rozwijanie zdolności i kompetencji cyfrowych wpływać może pozytywnie na poziom cyberbezpieczeństwa danego użytkownika, a tym samym na cały system cyberbezpieczeństwa RP. Toteż, skuteczne i trwałe zwiększanie poziomu świadomości i kompetencji cyfrowych może stanowić kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa.

Autor wyróżnił cztery szczegółowe hipotezy badawcze. 1. Użytkownicy bez odpowiednich kompetencji w zakresie cyberbezpieczeństwa mogą stanowić jedno ze słabszych ognisk systemu cyberbezpieczeństwa. 2. Edukacja może przekładać się bezpośrednio na poziom świadomości użytkowników w cyberprzestrzeni i ich kompetencje cyfrowe. Zdecydowanie tak, badania wykazały, iż nauczyciele są bardziej świadomi zagrożeń aniżeli uczniowie, ponieważ ci nie nabyli jeszcze dostatecznej wiedzy i doświadczenia. 3. Poziom świadomości obywateli korzystających z sieci - w zakresie cyberbezpieczeństwa jest niewystarczający. Potwierdzenie znaleźć można zarówno w wywiadach eksperckich, badaniu ankietowym jak i innych zgromadzonych materiałach. 4. Stałe rozwijanie kompetencji cyfrowych może pozwolić na minimalizację ryzyka wystąpienia określonych zagrożeń w cyberprzestrzeni. Cykliczne i regularne szkolenie, z naciskiem na powtarzalność tego procesu jest kluczem do złagodzenia ewentualnych skutków zagrożeń.

Na podstawie przeprowadzonych analiz kluczowych dokumentów prawno-urzędniczych, dostępnych badań i zrealizowanego własnego badania sondażowego stwierdzono (zgodnie ze wskazaną hipotezą), iż poziom kompetencji cyfrowych użytkowników sieci, tj. uczniów szkół podstawowych oraz nauczycieli jest niewystarczający i wymaga udoskonalenia.

Próbując ustalić diagnozę przyczyn niskiego poziomu umiejętności cyfrowych wskazać można głównie na: niedostateczność trwałych programów (kampanii) edukacyjnych oraz wychowawczych mających na celu uświadamiać nieletnich, rodziców o bezpiecznym użytkowaniu sieci i ewentualnych zagrożeniach płynących z jej korzystania. Stad, należy kształtować u młodych osób właściwe kompetencje, tak aby swo-

bodnie ale z pełnym bezpieczeństwem poruszać sie w Internecie. Dodatkowo, dorośli, nauczyciele i rodzice powinni w zdecydowanie większym stopniu zwracać uwagę na to, co dzieci przeglądają w sieci i do czego mają dostęp. Kwestie ograniczonego wyboru są u najmłodszych najbardziej istotne z uwagi na czyhające zagrożenia.

W ramach podjętej analizie obszaru badawczego stwierdzono, iż proces tworzenia i aktualizacji regulacji oraz programów związanych z kształtowaniem odpowiednich postaw, a także budowaniem świadomości cyfrowej trwa i jest poddawany zmianom. Stanowi to ogromne wyzwanie z uwagi na fakt, iż cyberprzestrzeń ma charakter globalny i dokonuje sie w tzw. cyberświecie, co utrudnia dodatkowo rozwiązywanie pewnych problemów w ramach poszczególnych państw. Konieczne więc z punktu widzenia użytkownika sieci jest dopasowanie legislacji na szczeblach tak krajowym, jak i europejskim.

Zrealizowanie i przeanalizowanie wyników badań własnych (próba ponad 1500 nauczycieli oraz ponad 2500 uczniów) pozwala stwierdzić, że większość badanych z komputera korzysta codziennie bądź przynajmniej raz w tygodniu. Stanowi to o nieodłącznej obecności urządzeń cyfrowych i aplikacji we współczesnym świecie. Niepokojącym jest fakt, iż zaledwie ok. 1/3 rodziców badanych uczniów kontroluje i ogranicza ten czas. Zbyt częste korzystanie młodego człowieka z cyberprzestrzeni wpływa na nieukształtowaną jeszcze jego osobowość i czasami powoduje zaniedbywanie innych obszarów rozwoju czy obowiązków.

Badania ukazały, że występuje znaczący problem w znajomości podstawowych cyberzagrożeń, ponieważ w większości respondenci wskazywali jedynie: spam, stalking i koń trojański. Coraz bardziej popularny i coraz częściej występujący według statystyk (opisanych w czwartym rozdziale) – *phishing* znalazł się na odległej pozycji.

Co istotne, w przeważającej części wskazano również, iż w szkołach nie ma wystarczającej ilości czasu przeznaczanego na lekcje dotyczące bezpiecznego zachowania w Internecie.

Ważnym zaznaczenia jest wniosek, że zdecydowana większość biorących udział w ankiecie nauczycieli jest zdania, iż edukacja w ramach cyberprzestrzeni powinna zaczynać się już od najmłodszych lat. Stąd też, kluczowa jest dyskusja środowisk naukowych i edukacyjnych celem implementacji nowych rozwiązań w szkołach podstawowych.

Autor spostrzega, iż istnieje potrzeba edukacji zarówno nauczycieli jak i uczniów w obszarach związanych z podstawami cyberbezpieczeństwa, tj. bezpieczeń-

stwem danych, osobowym czy związanymi z cyberzagrożeniami. Ponadto, zasadne jest zastanowienie się nad tematem kampanii edukacyjnych i ich skutecznością, gdyż wyniki i wnioski zgromadzone w ramach badania sondażowego wskazują, iż nadal zbyt niski procent respondentów wiedzę czerpie z ww. działań.

Poziom kompetencji cyfrowych może różnić się w zależności od wielu czynników, takich jak lokalizacja geograficzna, dostęp do zasobów cyfrowych, jakość szkolenia nauczycieli i polityki oświatowej.

Wobec powyższych stwierdzono, że:

- poziom kompetencji cyfrowych użytkowników sieci w badanej grupie jest zbliżony i jednocześnie niski w porównaniu do wybranych państw europejskich;
- zarówno w Polsce i Unii Europejskiej podejmowane są przedsięwzięcia mające na celu rozwój użytkowników sieci, jednak jest ich, jak pokazują badania- za mało;
- niezbędne są działania na szczeblu krajowym, działania trwałe, ciągłe i kluczowym jest podejście do kwestii rozwoju kompetencji cyfrowych jako całościowego procesu, który musi być powtarzalny;
- kampanie informacyjne powinny być dostosowywane i uwzględniać dynamicznie zmieniające sie środowisko cyberprzestrzeni zarówno w aspektach indywidualnych jak i mogących mieć wpływ i odnoszących sie do różnych grup społecznych;
- należy podejmować rożnego rodzaju czynności w szkołach związane z wdrażaniem odpowiednich programów prewencyjno-interwencyjnych i edukacyjnych.

Stosunkowo niski poziom kompetencji cyfrowych polskiego społeczeństwa może negatywnie odbić się na skali oraz tempie cyfrowej transformacji, a także wzroście gospodarczym, jak również niższym komforcie życia obywateli. W związku z tym koniecznym jest zapewnienie każdemu mieszkańcowi Polski właściwych warunków do stałego rozwoju kompetencji cyfrowych. Spójna i jednolita polityka rozwoju kompetencji cyfrowych, mająca niebagatelny wpływ na świadomych (i aktywnych cyfrowo) obywateli, jest podstawą do rozwoju nowoczesnego państwa, gospodarki i przemysłu przyszłości.

Szczególnie ważna jest w tym aspekcie zgoda polityczna i chęć do kontynuowania działań podejmowanych przez poprzedników (uwzględniając analizę dotychczasowych przedsięwzięć).

Skuteczne rozwijanie zdolności i budowanie świadomości korzystających z sieci użytkowników wymaga kompleksowego podejścia w obszarze technicznym, społecznym oraz prawnym. Jak już wspomniano, przepisy muszą uwzględniać zmieniające się

środowisko i realia związane z postępem technicznym. Dokonana analiza pozwala stwierdzić, iż kluczowa w ochronie swoich użytkowników jest współpraca międzynarodowa i wymiana informacji.

Miejsce i rola podjętych badań ma niezwykłe znaczenie. Dowodzą one, że użytkownik stale uczy się na bazie własnych doświadczeń i powinien doskonalić swoje umiejętności. Cyberprzestępcy wykorzystując coraz to nowe formy i techniki wyprzedzają częstokroć możliwości zabezpieczenia sie przed nimi, stad przyjąć należy, iż cyberzagrożeń nie da się wyeliminować, można jedynie na nie reagować i próbować się do nich przygotowywać.

W obszarze nauk społecznych przeprowadzone badania oraz ich implikacje, mogą być inspiracją dla kolejnych środowisk naukowych do podjęcia dalszych interdyscyplinarnych badań obejmując swoim zasięgiem większe terytorium czy inne grupy społeczne. Autor ma świadomość przedstawionego ograniczonego charakteru badań do przyjętego przedmiotu. Opracowane i przytoczone wnioski jak i postulaty stanowią propozycje do bardziej pogłębionych analiz i następnych rozważań oraz publikacji. Mając na uwadze powyższe argumenty i analizy, podkreślić należy fakt rosnącego znaczenia edukacji w świecie cyfrowym.

Załączniki: 2 na 13 str.:

Załącznik nr 1 na 7 str.: Kwestionariusz kompetencji cyfrowych nauczycieli w zakresie cyberbezpieczeństwa

Załącznik nr 2 na 6 str.: Kwestionariusz kompetencji cyfrowych uczniów w zakresie cyberbezpieczeństwa

Załącznik nr 1
do rozprawy doktorskiej

ppor. mgr Dawid Duda
Nauki Społeczne
Nauki o Bezpieczeństwie
Szkoła Doktorska Wojskowej Akademii Technicznej
im. Jarosława Dąbrowskiego w Warszawie

KWESTIONARIUSZ
kompetencji cyfrowych nauczycieli w zakresie cyberbezpieczeństwa

Szanowni Państwo!
Jestem doktorantem SDR WAT im. Jarosława Dąbrowskiego w Warszawie. Obecnie prowadzę badania w ramach rozprawy doktorskiej z zakresu cyberbezpieczeństwa. Celem poniższej ankiety jest zebranie informacji dotyczących cyberzagrożeń oraz szeroko rozumianych kompetencji cyfrowych. Otrzymane, dzięki Państwa uprzejmości i uczestnictwie w badaniu - odpowiedzi pozwolą określić poziom wiedzy w obszarze cyberbezpieczeństwa, jak również wskażą możliwości podnoszenia tego poziomu.
Tematyka ta jest niezwykle istotna z punktu widzenia bezpieczeństwa państwa. Wyniki przeprowadzonych badań służyć będą poszerzeniu wiedzy, jak i świadomości w tym obszarze, co finalnie powinno odbyć się z korzyścią dla całego społeczeństwa.
Pragnę zapewnić, że moje badania mają charakter poufny i anonimowy. Żadne informacje uzyskane w wyniku badań nie zostaną powiązane z Państwa danymi osobowymi i posłużą wyłącznie celom naukowym.
Odpowiedzi na pytania proszę zaznaczać przez postawienie znaku „x".
Z góry dziękuję za poświęcony czas oraz wypełnienie niniejszej ankiety!

I CZĘŚĆ MERYTORYCZNA

1. Ile posiada Pan / Pani kont e-mailowych?
□ jedno, które wykorzystuję do wszystkich dalszych działań [np. zakupy, newsletter. itd.]
□ korzystam z kilku adresów e-mail w zależności od celu
□ nie posiadam żadnego konta e-mail

2. Jakie stworzy Pan / Pani hasło do nowego konta na stronie www?
□ nowe, silne hasło (cyfry, znaki specjalne, wielkie i małe litery)
□ łatwe hasło, by łatwo je zapamiętać
□ użyję tego samego hasła, którego używam już w innych miejscach
□ użyję szablonu (np. utworzę podobnie brzmiące hasło)

3. Jak zapamięta Pan / Pani nowo utworzone hasło?
□ ukryję je w specjalnej aplikacji do przechowywania haseł
□ zapiszę na kartce lub w zeszycie
□ zapiszę w notatkach w telefonie
□ zapiszę w przeglądarce (zapamiętywanie)
□ zapamiętam je

4. Otrzymał Pan / Pani maila z komunikatem o nazwie *„Wygrałeś najnowszy model iPhone. Otrzymasz go jeśli wyślesz swój adres i hasło do konta”*. Co dalej?

□ natychmiast wyślę te dane, w końcu coś wygram
□ usunę wiadomość, to może być próba wyłudzenia danych
□ nie wiem

5. Gdzie przechowuje Pan / Pani swoje zdjęcia i filmy, zajmujące zbyt dużo pamięci na dysku twardym (lokalnym)? (Można zaznaczyć kilka odpowiedzi).

□ na zewnętrznym dysku twardym lub pendrive
□ na zaszyfrowanym zewnętrznym dysku twardym lub pendrive
□ w chmurze (w sieci)
□ w chmurze w zaszyfrowanym folderze (w sieci)
□ nie mam zbyt wielu zdjęć i filmów

6. Czy wykonuje Pan / Pani kopie swoich plików (na wypadek utraty danych)?

□ tak, regularnie tworzę kopie zapasowe najważniejszych plików
□ tak, regularnie tworzę kopie zapasowe wszystkich plików
□ tak, tworzę kopie, ale nie robię tego regularnie
□ nie tworzę kopii, ale planuję to zrobić
□ nie tworzę kopii, ponieważ uważam to za niepotrzebne

7. Który adres banku jest Pana / Pani zdaniem prawdziwy – autentyczny?

□ http://pkobp.pl
□ http://pkobpi.pl
□ https://pkobp.pl
□ https://pekobp.pl
□ nie wiem / nie korzystam z usług bankowości internetowej

8. Którą opcję wybiera Pan / Pani płacąc w restauracji przy użyciu karty płatniczej?

□ kelnerka przynosi terminal płatniczy i osobiście dokonuję płatności
□ kelnerka zapisuje szczegóły karty płatniczej i obiecuje zrealizowanie płatności przez siebie, dzięki czemu mogę szybciej wyjść
□ kelnerka zabiera moją kartę do kasy i sama przy kasie realizuje płatność
□ nie płacę w takich sytuacjach kartą

9. Jeśli podczas zakupów w Internecie wprowadza Pan / Pani dane swojej karty płatniczej, jak można zapewnić bezpieczeństwo transakcji? (Można zaznaczyć kilka odpowiedzi).

□ nie muszę niczego robić, strona jest przeze mnie znana
□ włączę tryb *Incognito* w przeglądarce
□ użyję klawiatury wirtualnej do wprowadzania danych
□ szczegółowo sprawdzę poprawność adresu, autentyczność strony i tzw. *„kłódkę”*
□ nie kupuję w Internecie

10. Z jakich stron pobiera Pan / Pani filmy, gry, aplikacje bądź książki?

□ pobieram jedynie z zaufanych źródeł
□ korzystam z różnych źródeł
□ rzadko pobieram tego typu dane i stosuję zasadę ograniczonego zaufania
□ nie korzystam z tego rodzaju usług internetowych

11. Jakich aplikacji używa Pan / Pani do rozmów przez Internet?

□ używam różnych aplikacji na moich urządzeniach
□ używam różnych aplikacji na różnych urządzeniach, niekoniecznie moich
□ używam jedynie sprawdzonych aplikacji i moich urządzeń
□ nie używam Internetu do rozmów

12. W jaki sposób chroni Pan / Pani swoje prywatne dane na komputerze?

□ korzystam ze specjalnego programu z hasłem
□ chowam swój komputer w szafce i nikomu nie pożyczam
□ korzystam tylko z hasła podczas włączania komputera
□ dane ukrywam jedynie, gdy pożyczam komputer

□ nie potrzebuję chronić swoich danych w żaden sposób

13. Jak najczęściej postępuje Pan / Pani instalując nowe programy na komputerze / smartfonie?
□ z uwagą czytam wszystkie wyświetlane informacje
□ klikam *„dalej-dalej-zgadzam się”* nie czytając zawartości
□ proszę o pomoc znajomego lub kogoś obeznanego w temacie komputerów
□ nie instaluję nowych programów

14. Jakie uprawnienia do Pana / Pani urządzenia mają zainstalowane aplikacje mobilne?
□ najczęściej zgadzam się na wymagania i nie myślę o tym
□ pozwalam na różne uprawnienia zależnie od aplikacji
□ staram się zezwalać na wąski zakres uprawnień, tak żeby strzec swojej prywatności
□ nie wiem

15. Otrzymuje Pan / Pani powiadomienie systemowe o potrzebie aktualizacji. Co dalej?
□ zgadzam się, te aktualizacje są ważne dla bezpieczeństwa systemu
□ klikam *„przypomnij później”*
□ najczęściej nie instaluję aktualizacji
□ nie otrzymuję takich powiadomień

16. Jakimi kryteriami sugeruje się Pan / Pani wybierając program antywirusowy? (Można wybrać kilka odpowiedzi).
□ niska cena
□ renomowana marka
□ dobre opinie w Internecie
□ dobre opinie wśród znajomych
□ wysokie miejsca w oficjalnych klasyfikacjach testowych
□ prosty interfejs
□ nie wiem czym się kierować
□ inne (proszę podać) ……..
□ nie korzystam z programu antywirusowego

17. W jakich sytuacjach włącza Pan / Pani skanowanie programem antywirusowym? (Można wybrać kilka odpowiedzi).
□ regularnie skanuję komputer
□ przed kopiowaniem plików np. z pendrive’a
□ przed pobraniem plików z Internetu
□ przed uruchomieniem aplikacji lub przed otwarciem dokumentu z zewnętrznego źródła
□ wierzę, że mój antywirus robi to automatycznie, więc ja nie muszę
□ nie korzystam ze skanowania antywirusowego
□ nie korzystam z programu antywirusowego

18. Jak postąpi Pan / Pani jeśli antywirus blokuje możliwość instalacji programu?
□ tymczasowo wyłączę ochronę antywirusową, żeby obejść blokadę
□ poszukam innego programu w Internecie
□ włączę regułę wyjątku w antywirusie, ponieważ jestem pewien bezpieczeństwa instalowanego programu
□ nie wiem

19. Czy jest Pan / Pani użytkownikiem portalu społecznościowego *(Facebook, Instagram, Twitter, Tumblr, Nasza Klasa)*? <u>(Jeśli nie, proszę przejść do pytania nr 24)</u>
□ tak, często
□ tak, sporadycznie
□ nie, nigdy
□ kiedyś korzystałem, ale obecnie już nie

20. Dostał Pan / Pani wiadomość od znajomego w serwisie społecznościowym. Znajomy prosi kliknąć w przesłany odnośnik. Jaka będzie Pana / Pani reakcja?
□ kliknę od razu, znam tę osobę
□ zapytam znajomego o zawartość tego linku

□ natychmiast oznaczę wiadomość jako spam i dodam znajomego do zablokowanych
□ nigdy nie klikam w jakiekolwiek linki

21. Dostał Pan / Pani wiadomość od znajomego w serwisie społecznościowym. Znajomy pilnie potrzebuje gotówki, prosi o przelew.
□ zrobię to, o co prosi, znam tę osobę
□ zweryfikuję autentyczność znajomego np. dzwoniąc do niego telefonicznie
□ natychmiast oznaczę wiadomość jako spam i dodam znajomego do zablokowanych
□ nigdy nie wykonuję przelewów online

22. Jakie dane udostępnia Pan / Pani publicznie w mediach społecznościowych (nie tylko dla znajomych)?
□ jedynie imię, nazwisko, zdjęcie profilowe
□ praktycznie wszystko, nie chowam tajemnic
□ imię, nazwisko, zdjęcia, posty
□ imię, nazwisko, zdjęcia, posty, zameldowania, statusy
□ staram się udostępniać jak najmniejszą ilość informacji o sobie
□ nie wiem, ponieważ nie wiem jak to sprawdzić

23. Jak postąpi Pan / Pani otrzymując zaproszenie od nieznajomego?
□ zawsze akceptuję zaproszenia, lubię mieć wielu znajomych
□ akceptuję zaproszenie jeśli mamy wspólnych znajomych
□ dodaję osobę jeśli znam ją osobiście
□ mam niewielu znajomych, nikt mnie nie zaprasza
□ piszę najpierw do nieznajomego, żeby dowiedzieć się kim jest

24. Jakie rodzaje cyberzagrożeń Pan / Pani zna?
□ stalking
□ rootkit
□ adware
□ skimming
□ malware
□ spam
□ koń trojański
□ phishing
□ ransomware
□ cryptojacking
□ nie wiem

25. Czym są pliki Cookies?
□ rodzaj wydarzeń rozrywkowych w Internecie
□ fotografie ciasteczek
□ niewielkich rozmiarów pliki zapisywane przez przeglądarkę (legalne monitorowanie Pana / Pani aktywności w sieci)
□ program antywirusowy
□ nie wiem

26. Czy uważa Pan / Pani, że Internet to również niebezpieczne miejsce?
□ tak
□ raczej tak
□ trudno powiedzieć
□ raczej nie
□ nie

27. Proszę dokonać samooceny w obszarze Pana / Pani świadomości zagrożeń w cyberprzestrzeni (Internecie). (Proszę otoczyć kółkiem właściwą cyfrę, 5 – wysoka świadomość, 1 – niska świadomość).
5 4 3 2 1

28. Jakie działania podejmuje Pan / Pani, żeby zwiększać swój poziom kompetencji cyfrowych? Kompetencje cyfrowe rozumiane są w uproszczeniu jako zbiór umiejętności pozwalających skutecznie i sprawnie korzystać z komputera oraz Internetu. (Można zaznaczyć kilka odpowiedzi).

□ uczestniczę w szkoleniach
□ śledzę na bieżąco kampanie edukacyjne dotyczące zachowań w Internecie
□ czytam różnego rodzaju artykuły lub czasopisma
□ rozmawiam ze specjalistami w tej branży
□ wymieniam poglądy ze znajomymi
□ raczej nic nie robię w tym zakresie
□ inne (jakie?)……

29. Czy Pana / Pani zdaniem edukacja dotycząca cyberprzestrzeni powinna zaczynać się od 1 klasy szkoły podstawowej?

□ zdecydowanie tak
□ raczej tak
□ raczej nie, nie ma takiej potrzeby
□ zdecydowanie nie

30. Czy spotkał się Pan / Pani z problemem cyberprzemocy (nękanie, dręczenie, prześladowanie w Internecie)? (Proszę odnieść się do <u>każdego</u> z podpunktów a-h).

a) cyberprzemoc dotknęła
□ mnie bezpośrednio □ innych nauczycieli □ uczniów
□ nie znam osoby, którą dotknęła cyberprzemoc
b) uczniowie odbywają lekcje związane z przeciwdziałaniem cyberprzemocy
□ tak □ nie □ nie wiem
c) nauczyciele odbywają szkolenia związane z przeciwdziałaniem cyberprzemocy
□ tak □ nie □ nie wiem
d) rodzice odbywają szkolenia związane z przeciwdziałaniem cyberprzemocy
□ tak □ nie □ nie wiem
e) szkoła posiada procedury działania w sytuacji cyberprzemocy
□ tak □ nie □ nie wiem
f) szkoła współpracuje z różnymi podmiotami w zakresie cyberprzemocy np. z policją
□ tak □ nie □ nie wiem
g) wiem, jak się zachować kiedy występuje zjawisko cyberprzemocy
□ tak □ nie □ nie wiem
h) udało się ustalić sprawcę cyberprzemocy
□ tak, zawsze □ tak, ale nie w każdym przypadku □ nie □ nie wiem
□ nie znam osoby, którą dotknęła cyberprzemoc

31. Jak, Pana / Pani zdaniem nauczyciele i szkoła poradzili sobie ze zdalnym nauczaniem?

□ bardzo dobrze
□ raczej dobrze
□ raczej słabo
□ bardzo słabo
□ trudno powiedzieć

32. Jakie problemy napotkał Pan / Pani podczas zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).

□ zmęczenie spowodowane siedzeniem przed ekranem monitora
□ słabe własne połączenie internetowe
□ trudności w tworzeniu grup online
□ niewłaściwy sprzęt np. zbyt wolny komputer
□ niewystarczające umiejętności obsługi komputera / programów
□ podejście uczniów – byli po prostu zmęczeni
□ słabe połączenie internetowe uczniów
□ inne (jakie?)……

33. Jakie dostrzega Pan / Pani korzyści i dobre strony zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).

□ mogę korzystać z Internetu – jako pomocy, w trakcie lekcji
□ materiały dydaktyczne są bardziej urozmaicone niż te dostępne w trybie stacjonarnym
□ nieśmiali uczniowie stają się bardziej odważni i zaangażowani
□ mam większe możliwości indywidualnych zajęć z uczniami
□ mogę prowadzić zajęcia i jednocześnie robić coś innego, np. sprzątać w domu
□ mam więcej czasu dla siebie, ponieważ najczęściej szybciej niż w szkole realizuję temat
□ nie muszę wcześnie wstawać, oszczędzam czas (dojazd do pracy)
□ inne (jakie?)……

34. Jakie są Pana / Pani zdaniem negatywne (słabe) strony zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).

□ nie mam bezpośredniego kontaktu z uczniami
□ czasami nie jestem w stanie sprawdzić czy uczniowie „ściągają"
□ brak pełnej kontroli nad czynnościami uczniów
□ brak społecznych umiejętności, które uczniowie nabierają w trakcie tradycyjnych zajęć
□ trudniej jest mi przekazać treść i zrozumienie pewnych tematów i zagadnień
□ nie wszystkie zajęcia da się właściwie przeprowadzić np. wychowanie fizyczne
□ konieczne jest mieć właściwy sprzęt komputerowy i umiejętności
□ inne (jakie?)……

35. Które formy nauczania były najczęściej przez Pana / Panią wykorzystywane w trybie zdalnym? (Można wybrać kilka odpowiedzi).

□ korzystanie z gotowych filmików edukacyjnych w Internecie
□ wysyłanie gotowych, nagranych lekcji np. webinarów
□ przesyłanie swoich materiałów do samodzielnego wypełnienia
□ korzystanie z prezentacji wykonanej samodzielnie
□ przesyłanie / podawanie zakresu z podręcznika do samodzielnego opracowania
□ zlecanie zadań typu: odrobienie pracy domowej, wykonanie prezentacji
□ prowadzenie lekcji na żywo przy pomocy np. Zoom, MS Teams i innych
□ korzystanie z aplikacji do edukacji online np. Google Classroom i innych
□ wykorzystywanie różnych narzędzi elektronicznych np. tablica interaktywna, tablet graficzny
□ udostępnianie linków do lekcji w Internecie prowadzonych przez innego nauczyciela
□ prowadzenie indywidualnych konsultacji
□ inne (jakie?)……

36. Jak ocenia Pan / Pani swoje umiejętności wykonywania poniższych zadań przy komputerze? (Proszę odnieść się do <u>każdego</u> z podpunktów a-o).

a) wyszukanie pliku na komputerze
□ potrafię □ mam trudności □ nie potrafię
b) wyszukanie informacji w Internecie
□ potrafię □ mam trudności □ nie potrafię
c) zainstalowanie aplikacji / gry
□ potrafię □ mam trudności □ nie potrafię
d) tworzenie dokumentów (np. wypracowań, sprawozdań)
□ potrafię □ mam trudności □ nie potrafię
e) edytowanie fotografii cyfrowej / grafiki
□ potrafię □ mam trudności □ nie potrafię
f) zamieszczanie zdjęć, tekstów na portalu społecznościowym
□ potrafię □ mam trudności □ nie potrafię
g) tworzenie prezentacji multimedialnej
□ potrafię □ mam trudności □ nie potrafię
h) tworzenie strony internetowej
□ potrafię □ mam trudności □ nie potrafię
i) tworzenie bazy danych
□ potrafię □ mam trudności □ nie potrafię
j) tworzenie sieci komputerowej
□ potrafię □ mam trudności □ nie potrafię
k) korzystanie z arkusza kalkulacyjnego
□ potrafię □ mam trudności □ nie potrafię
l) zmienianie ustawień komputera (usprawnienie jego pracy)

□ potrafię □ mam trudności □ nie potrafię

m) ochrona swoich danych np. poprzez zaporę, antywirusa
□ potrafię □ mam trudności □ nie potrafię

n) rozwiązywanie problemów technicznych
□ potrafię □ mam trudności □ nie potrafię

o) dzielenie się z innymi informacjami, danymi, plikami
□ potrafię □ mam trudności □ nie potrafię

II METRYCZKA

37. Płeć

□ kobieta
□ mężczyzna

38. Jakie posiada Pan / Pani wykształcenie? (Można zaznaczyć więcej niż jedną odpowiedź).

□ wyższe - licencjackie
□ wyższe - magisterskie
□ studia podyplomowe, kurs kwalifikacyjny
□ inne (proszę podać jakie) .....

39. Proszę wskazać Pana / Pani kierunek wykształcenia.

□ wychowanie przedszkolne/nauczanie początkowe
□ humanistyczny
□ ścisły (w tym przyrodniczy)
□ artystyczny
□ inny (proszę podać jaki) .....

40. Jakie zajmuje Pan / Pani stanowisko w szkole? (Można zaznaczyć kilka odpowiedzi).

□ nauczyciel klasy 0
□ nauczyciel klas 1-3
□ nauczyciel klas 4-8
□ dyrektor szkoły

41. Proszę wskazać ilość uczniów w najbardziej licznej klasie, w której Pan / Pani uczy.

□ do 5 uczniów
□ do 10 uczniów
□ do 15 uczniów
□ do 20 uczniów
□ powyżej 20 uczniów
□ nie dotyczy

42. Jakiej wielkości jest miejscowość, w której Pan / Pani pracuje?

□ wieś
□ miasto małe <20 tys. mieszkańców
□ miasto średnie 20-100 tys.
□ miasto duże 100 tys. i więcej
□ nie wiem

Załącznik nr 2

do rozprawy doktorskiej

ppor. mgr Dawid Duda
Nauki Społeczne
Nauki o Bezpieczeństwie
Szkoła Doktorska Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie

KWESTIONARIUSZ
kompetencji cyfrowych uczniów w zakresie cyberbezpieczeństwa

Szanowni Państwo!
Jestem doktorantem SDR WAT im. Jarosława Dąbrowskiego w Warszawie. Obecnie prowadzę badania w ramach rozprawy doktorskiej z zakresu cyberbezpieczeństwa. Celem poniższej ankiety jest zebranie informacji dotyczących cyberzagrożeń oraz szeroko rozumianych kompetencji cyfrowych. Otrzymane, dzięki Państwa uprzejmości i uczestnictwie w badaniu - odpowiedzi pozwolą określić poziom wiedzy w obszarze cyberbezpieczeństwa, jak również wskażą możliwości podnoszenia tego poziomu.
Tematyka ta jest niezwykle istotna z punktu widzenia bezpieczeństwa państwa. Wyniki przeprowadzonych badań służyć będą poszerzeniu wiedzy, jak i świadomości w tym obszarze, co finalnie powinno odbyć się z korzyścią dla całego społeczeństwa.
Pragnę zapewnić, że moje badania mają charakter poufny i anonimowy. Żadne informacje uzyskane w wyniku badań nie zostaną powiązane z Państwa danymi osobowymi i posłużą wyłącznie celom naukowym.
Odpowiedzi na pytania proszę zaznaczać przez postawienie znaku „x".
Z góry dziękuję za poświęcony czas oraz wypełnienie niniejszej ankiety!

I CZĘŚĆ MERYTORYCZNA

1. Jak często korzystasz z komputera będąc w szkole, domu bądź innych miejscach (biblioteka, kawiarenka internetowa)?

□ codziennie
□ przynajmniej raz w tygodniu
□ przynajmniej raz w miesiącu
□ rzadziej niż raz w miesiącu
□wcale

2. Od ilu lat korzystasz z komputera?

□ od pięciu lub dłużej
□ od trzech do pięciu lat
□ krócej niż trzy lata ale dłużej niż jeden rok
□ krócej niż jeden rok

3. Czy rodzice / opiekuni mają nadzór nad ilością Twojego czasu spędzanego przed komputerem?

□ tak, mam ograniczony czas
□ nie, nie jestem kontrolowany
□ czasami tak, czasami nie

4. Do jakich domowych zadań szkolnych wykorzystujesz komputer? (Proszę odnieść się do każdego z podpunktów a-e).

a) pisanie wypracowań bądź sprawozdań
□ codziennie □ co najmniej raz w tygodniu □ kilka razy w miesiącu □ wcale
b) pisanie testów lub sprawdzianów
□ codziennie □ co najmniej raz w tygodniu □ kilka razy w miesiącu □ wcale
c) opracowywanie prezentacji
□ codziennie □ co najmniej raz w tygodniu □ kilka razy w miesiącu □ wcale
d) wypełnianie ćwiczeń bądź zeszytów
□ codziennie □ co najmniej raz w tygodniu □ kilka razy w miesiącu □ wcale
e) wspólna praca z innymi uczniami
□ codziennie □ co najmniej raz w tygodniu □ kilka razy w miesiącu □ wcale

5. Jak oceniasz swoje umiejętności wykonywania poniższych zadań przy komputerze? (Proszę odnieść się do <u>każdego</u> z podpunktów a-o).

a) wyszukanie pliku na komputerze
□ potrafię □ mam trudności □ nie potrafię
b) wyszukanie informacji w Internecie
□ potrafię □ mam trudności □ nie potrafię
c) zainstalowanie aplikacji / gry
□ potrafię □ mam trudności □ nie potrafię
d) tworzenie dokumentów (np. wypracowań, sprawozdań)
□ potrafię □ mam trudności □ nie potrafię
e) edytowanie fotografii cyfrowej / grafiki
□ potrafię □ mam trudności □ nie potrafię
f) zamieszczanie zdjęć, tekstów na portalu społecznościowym
□ potrafię □ mam trudności □ nie potrafię
g) tworzenie prezentacji multimedialnej
□ potrafię □ mam trudności □ nie potrafię
h) tworzenie strony internetowej
□ potrafię □ mam trudności □ nie potrafię
i) tworzenie bazy danych
□ potrafię □ mam trudności □ nie potrafię
j) tworzenie sieci komputerowej
□ potrafię □ mam trudności □ nie potrafię
k) korzystanie z arkusza kalkulacyjnego
□ potrafię □ mam trudności □ nie potrafię
l) zmienianie ustawień komputera (usprawnienie jego pracy)
□ potrafię □ mam trudności □ nie potrafię
m) ochrona swoich danych np. poprzez zaporę, antywirusa
□ potrafię □ mam trudności □ nie potrafię
n) rozwiązywanie problemów technicznych
□ potrafię □ mam trudności □ nie potrafię
o) dzielenie się z innymi informacjami, danymi, plikami
□ potrafię □ mam trudności □ nie potrafię

6. Czy jesteś użytkownikiem portalu społecznościowego *(Facebook, Instagram, Twitter, Tumblr, Nasza Klasa)*? <u>(Jeśli nie, proszę przejść do pytania nr 10)</u>

□ tak, często
□ tak, sporadycznie
□ nie, nigdy
□ kiedyś korzystałem, ale obecnie już nie

7. Dostałeś wiadomość od znajomego w serwisie społecznościowym. Znajomy prosi kliknąć w przesłany odnośnik. Jaka będzie Twoja reakcja?

□ kliknę od razu, znam tę osobę
□ zapytam znajomego o zawartość tego linku
□ natychmiast oznaczę wiadomość jako spam i dodam znajomego do zablokowanych
□ nigdy nie klikam w jakiekolwiek linki

8. Jakie dane udostępniasz publicznie w mediach społecznościowych (nie tylko dla znajomych)?

□ jedynie imię, nazwisko, zdjęcie profilowe

□ praktycznie wszystko, nie chowam tajemnic
□ imię, nazwisko, zdjęcia, posty
□ imię, nazwisko, zdjęcia, posty, zameldowania, statusy
□ staram się udostępniać jak najmniejszą ilość informacji o sobie
□ nie wiem, ponieważ nie wiem jak to sprawdzić

9. Jak postąpisz otrzymując zaproszenie od nieznajomego?
□ zawsze akceptuję zaproszenia, lubię mieć wielu znajomych
□ akceptuję zaproszenie jeśli mamy wspólnych znajomych
□ dodaję osobę jeśli znam ją osobiście
□ mam niewielu znajomych, nikt mnie nie zaprasza
□ piszę najpierw do nieznajomego, żeby dowiedzieć się kim jest

10. Z jakich stron pobierasz filmy, gry, aplikacje bądź książki?
□ pobieram jedynie z zaufanych źródeł
□ korzystam z różnych źródeł
□ rzadko pobieram tego typu dane i stosuję zasadę ograniczonego zaufania
□ nie korzystam z tego rodzaju usług internetowych

11. Jak najczęściej postępujesz instalując nowe programy/aplikacje na komputerze/smartfonie?
□ z uwagą czytam wszystkie wyświetlane informacje
□ klikam *„dalej-dalej-zgadzam się”* nie czytając zawartości
□ proszę o pomoc znajomego lub kogoś obeznanego w temacie komputerów
□ nie instaluję nowych programów

12. Otrzymałeś maila z komunikatem o nazwie *„Wygrałeś najnowszy model iPhone. Otrzymasz go jeśli wyślesz swój adres i hasło do konta”*. Co dalej?
□ natychmiast wyślę te dane, w końcu coś wygram
□ usunę wiadomość, to może być próba wyłudzenia danych
□ nie wiem

13. Czy uważasz, że Internet to również niebezpieczne miejsce?
□ tak
□ raczej tak
□ trudno powiedzieć
□ raczej nie
□ nie

14. Jakie rodzaje cyberzagrożeń znasz?
□ stalking
□ rootkit
□ adware
□ skimming
□ malware
□ spam
□ koń trojański
□ phishing
□ ransomware
□ cryptojacking
□ nie wiem

15. Jak oceniasz swoją świadomość zagrożeń w cyberprzestrzeni (Internecie)? (Proszę otoczyć kółkiem właściwą cyfrę, 5 - wysoko, 1 - nisko).
5 4 3 2 1

16. Jakie działania podejmujesz, żeby zwiększać swój poziom kompetencji cyfrowych? Kompetencje cyfrowe rozumiane są w uproszczeniu jako zbiór umiejętności pozwalających skutecznie i sprawnie korzystać z komputera oraz Internetu. (Można zaznaczyć kilka odpowiedzi).
□ poszukuję sam odpowiedzi
□ czytam artykuły

□ pytam kolegów / koleżanki
□ pytam rodziców / rodzeństwo
□ raczej nic nie robię
□ inne (jakie?)……

17. Czy Twoim zdaniem edukacja dotycząca cyberprzestrzeni (Internetu) powinna zaczynać się od 1 klasy szkoły podstawowej?
□ zdecydowanie tak
□ raczej tak
□ raczej nie, nie ma takiej potrzeby
□ zdecydowanie nie

18. Czy Twoim zdaniem w szkole poświęca się wystarczająco dużo czasu na lekcje dotyczące bezpiecznego zachowania w Internecie?
□ zdecydowanie tak
□ raczej tak
□ raczej nie
□ zdecydowanie nie

19. Czym są pliki Cookies?
□ rodzaj wydarzeń rozrywkowych w Internecie
□ fotografie ciasteczek
□ niewielkich rozmiarów pliki zapisywane przez przeglądarkę (legalne monitorowanie Twojej aktywności w sieci)
□ program antywirusowy
□ nie wiem

20. Jakie stworzysz hasło do nowego konta na stronie www?
□ nowe, silne hasło (cyfry, znaki specjalne, wielkie i małe litery)
□ łatwe hasło, by łatwo je zapamiętać
□ użyję tego samego hasła, którego używam już w innych miejscach
□ użyję szablonu (np. utworzę podobnie brzmiące hasło)

21. Jak zapamiętasz nowo utworzone hasło?
□ ukryję je w specjalnej aplikacji do przechowywania haseł
□ zapiszę na karteczce lub w zeszycie
□ zapiszę w notatkach w telefonie
□ zapiszę w przeglądarce (zapamiętywanie)
□ zapamiętam je

22. Jakie problemy napotkałeś/aś podczas zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).
□ zmęczenie spowodowane siedzeniem przed ekranem monitora
□ słabe własne połączenie internetowe
□ trudności w dołączeniu do grupy online
□ niewłaściwy sprzęt np. zbyt wolny komputer
□ niewystarczające umiejętności obsługi komputera / programów
□ zbyt dużo materiału realizowanego na zajęciach online
□ słabe połączenie internetowe nauczyciela
□ inne (jakie?)……

23. Jakie dostrzegasz korzyści i dobre strony zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).
□ mam lepsze oceny niż w trybie stacjonarnym
□ podczas sprawdzianu mogę korzystać z materiałów, których nauczyciel nie widzi
□ mogę korzystać z pomocy rodziców, rodzeństwa lub znajomych w trakcie sprawdzianu
□ mogę korzystać z Internetu w trakcie sprawdzianu
□ mam większe możliwości indywidualnych zajęć z nauczycielem
□ mam więcej czasu dla siebie, ponieważ nauczyciel najczęściej szybciej niż w szkole realizuje temat
□ mogę być obecny na zajęciach i jednocześnie robić coś innego, np. grać w gry

□ nie muszę wcześnie wstawać np. na autobus
□ inne (jakie?)……

24. Jakie są negatywne (słabe) strony zdalnego nauczania? (Można zaznaczyć kilka odpowiedzi).
□ nie mam bezpośredniego kontaktu z rówieśnikami
□ nie mam bezpośredniego kontaktu z nauczycielami
□ nie muszę wychodzić z domu, spędzam mniej czasu na świeżym powietrzu
□ nie jestem sprawiedliwie oceniany
□trudniej jest mi zrozumieć pewne tematy i zagadnienia
□ niewiele jest zajęć z wychowania fizycznego
□ brakuje mi szkolnych posiłków
□ inne (jakie?)……

25. Które formy nauczania najczęściej wykorzystywali nauczyciele w trybie zdalnym? (Można zaznaczyć kilka odpowiedzi).
□ korzystanie z gotowych filmików edukacyjnych w Internecie
□ przesyłanie swoich materiałów do samodzielnego wypełnienia
□ przesyłanie / podawanie zakresu z podręcznika do samodzielnego opracowania
□ korzystanie z prezentacji wykonanej przez nauczyciela
□prowadzenie lekcji na żywo przy pomocy np. Zoom, MS Teams i innych
□ wysyłanie gotowych, nagranych lekcji np. webinarów
□ udostępnianie linków do lekcji w Internecie prowadzonych przez innego nauczyciela
□ zlecanie zadań typu: odrobienie pracy domowej, wykonanie prezentacji
□ korzystanie z aplikacji do edukacji online np. Google Classroom i innych
□ prowadzenie indywidualnych konsultacji
□ inne (jakie?)……

26. Czego Ci najbardziej brakowało kiedy nauczyciele prowadzili zajęcia online? (Można zaznaczyć kilka odpowiedzi).
□ korzystania przez nauczyciela z platformy/programu umożliwiającej/go widzenie siebie nawzajem
□ pomocy uczniom w kwestiach technicznych np. z instalacją programu
□ pomocy nauczyciela podczas obsługi urządzeń np. kamery, mikrofonu, itp.
□pomocy nauczyciela podczas wystąpienia nagłej usterki
□ odpoczynku od ekranu monitora
□ inne (jakie?)……

27. Czy spotkałeś się z cyberprzemocą (nękanie, dręczenie, prześladowanie w Internecie)? (Proszę odnieść się do <u>każdego</u> z podpunktów a-g).
a) cyberprzemoc dotknęła
□ mnie bezpośrednio □ kolegę / koleżankę z klasy □ kolegę / koleżankę ze szkoły
□ nie znam osoby, którą dotknęła cyberprzemoc
a) obraziłem kogoś przynajmniej raz w mediach społecznościowych
□ tak □ nie □ nie pamiętam
b) wysłałem wiadomość przez komunikator (przynajmniej raz), by kogoś obrazić
□ tak □ nie □ nie pamiętam
c) byłem sprawcą lub ofiarą cyberprzemocy
□ tak □ nie □ nie pamiętam
d) zgłosiłem akt cyberprzemocy
□ tak, nauczycielowi □ tak, rodzicom / rodzeństwu □ tak, administratorowi sieci
□ nie, nikomu □ nie spotkałem się z cyberprzemocą □ nie pamiętam
e) wiem, jak się zachować kiedy występuje zjawisko cyberprzemocy
□ tak □ nie □ nie wiem
g) zapoznano mnie z problemem cyberprzemocy
□ w szkole □ w domu □ w innym miejscu □ nikt mnie nie zapoznał

II METRYCZKA
28. Wiek
□ uczeń klasy 0
□ uczeń klasy 1-3
□ uczeń klasy 4-6

□ uczeń klasy 7-8

29. Płeć
□ kobieta
□ mężczyzna

30. Ile osób liczy Twoja klasa?
□ do 5 uczniów
□ do 10 uczniów
□ do 15 uczniów
□ do 20 uczniów
□ powyżej 20 uczniów

31. Jakiej wielkości jest miejscowość, w której uczęszczasz do szkoły?
□ wieś
□ miasto małe <20 tys. mieszkańców
□ miasto średnie 20-100 tys.
□ miasto duże 100 tys. i więcej
□ nie wiem

Wykaz literatury

Pozycje książkowe

1. Aleksandrowicz T.R. , Liedel K., 2014, Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia [w:] Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, Liedel K., Piasecka P., Aleksandrowicz T.R. (red.), Wydawnictwo Difin, Warszawa.
2. Apanowicz J., 2000, Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania, Wydawnictwo Diecezji Pelplińskiej Bernardinum, Gdynia.
3. Apanowicz J., 2002, Metodologia ogólna, Wydawnictwo Diecezji IV Bernardinum, Gdynia.
4. Banach C., 2002, Człowiek wobec wyzwań globalizacji i transformacji ustrojowej w Polsce, [w:] Pedagogika wobec zagrożeń, kryzysów i nadziei, Borowska T. (red.), Wydawnictwo Oficyna Wydawnicza Impuls, Kraków.
5. Banasiński C. (red. nauk.), 2018, Cyberbezpieczeństwo. Zarys wykładu, Wydawnictwo Wolters Kluwer Polska, Warszawa.
6. Bańko M. (red.), 2000, Inny słownik języka polskiego, Wydawnictwo Naukowe PWN, Warszawa.
7. Białoskórski R., 2011, Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa.
8. Bralczyk J., 2005, Słownik 100 tysięcy potrzebnych słów, Wydawnictwo PWN, Warszawa.
9. Cieślarczyk M., 2003, Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich, Wydawnictwo Akademii Obrony Narodowej, Warszawa.
10. Denning D. D., 2002, Wojna informacyjna i bezpieczeństwo informacji, Wydawnictwo WNT, Warszawa.
11. Dębowski T., (red. nauk.), 2018, Cyberbezpieczeństwo wyzwaniem XXI wieku, Wyd. ArchaeGraph, Wrocław.
12. Dobrzyniecki K., 2004, Prawo a etos cyberprzestrzeni, Wydawnictwo Adam Marszałek, Toruń.

13. Dysarz J., 2018, Zarys działania krajowego systemu cyberbezpieczeństwa w Polsce, [w:] Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni. Wymiar teoretyczny i praktyczny, Topolewski S. (red.), Gdynia.
14. Franfort-Nachmias Ch., Nachmias D., 2001, Metody badawcze w naukach społecznych, Wydawnictwo Zysk i S-ka, Poznań.
15. Gibson W., 2009, Neuromancer, Wydawnictwo Książnica, Warszawa.
16. Górka M. (red. nauk.), 2017, Cyberbezpieczeństwo dzieci i młodzieży – realny i wirtualny problem polityki bezpieczeństwa", Wydawnictwo Difin, Warszawa.
17. Gwoździewicz S., Tomaszycki K., 2017, Prawne i społeczne aspekty cyberbezpieczeństwa, Wydawnictwo Międzynarodowy Instytut Innowacji Nauka – Edukacja – Rozwój, Warszawa.
18. Gwoździewicz S., Tomaszycki K., 2020, Legal and Social Aspects of Cyberecurity, Wydawnictwo Difin, Warszawa.
19. Kaczmarczyk B., 2014, Bezpieczeństwo i zagrożenia w teorii oraz praktyce, Wydawnictwo SAPSP, Kraków.
20. Kołodziejczyk M.E., 2021, Wprowadzenie stanów nadzwyczajnych w Rzeczypospolitej Polskiej w przypadku działań w cyberprzestrzeni, [w:] Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP, Chałubińska-Jentkiewicz K., Brzostek A. (red.), Warszawa.
21. Krajobraz Cyberzagrożeń 2022- Raport ENISA [2021-2022)].
22. Lakomy M., 2015, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo Uniwersystetu Śląskiego, Katowice.
23. Lombard D., 2008, Globalna wioska cyfrowa. Drugie życie sieci, Wydawnictwo MT Biznes, Warszawa.
24. Łobocki M., 2007, Wprowadzenie do metodologii badań pedagogicznych, Wydawnictwo Oficyna Wydawnicza Impuls, Kraków.
25. Madej M., 2009, Rewolucja informatyczna – istota, przejawy oraz wpływ na przestrzeganie bezpieczeństwa państw i systemu międzynarodowego, [w:] Bezpieczeństwo teleinformatyczne państwa, Madej M., Terlikowski M. (red.), Wydawnictwo PISM, Warszawa.
26. Pilch T., 1995, Zasady badań pedagogicznych, Wydawnictwo Akademickie ŻAK, Warszawa.
27. Puślecki W., 1995, Metody badań pedagogicznych, Wydawnictwo ODN, Kalisz.

28. Pytkowski W., 1981, Organizacja badań i ocena prac naukowych, Wydawnictwo PWN, Warszawa.
29. Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk T., 2019, Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski, Wydawnictwo Naukowe UAM, Poznań.
30. Raport roczny z działalności CERT Orange Polska [2016-2023].
31. Raport roczny z działalności CERT Polska [1996-2023].
32. Smolski W., 2015, Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa, Wydawnictwo Niepaństwowa Wyższa Szkoła Pedagogiczna, Białystok.
33. Szeligiewicz-Urban D. (red. nauk.), 2012, Uczeń bezpieczny w cyberprzestrzeni, Wyd. Humanitas, Sosnowiec.
34. Sztumski J., 1995, Wstęp do metodologii i technik badań społecznych, Wydawnictwo Śląsk, Katowice.
35. Sztumski J., 2005, Wstęp do metod i technik badań społecznych, Wydawnictwo Śląsk, Katowice.
36. Szybowska S., 2024, Środki zarządzania ryzykiem w cyberbezpieczeństwie w polityce bezpieczeństwa ICT i wyzwaniach prawnych, [w:] Wielowymiarowość cyberbezpieczeństwa, Żylińska J., Huczek K., Borkowski K. (red.), Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej, Warszawa.
37. Szyłkowska M., 2014, Ochrona cyberprzestrzeni w systemie bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Wydawnictwo WSPoL, Szczytno.
38. Szyłkowska M., 2019, Piąty wymiar bezpieczeństwa – cyberprzestrzeń. Wyzwania, zagrożenia, implikacje, Wyd. Sine Qua Non, Kraków.
39. Szyłkowska M., 2020, wykład z przedmiotu: Wybrane problemy społeczeństwa informacyjnego- materiał w zbiorach autora, WAT, Warszawa.
40. Szyłkowska M., 2023, Ochrona cyberprzestrzeni- materiał w zbiorach autora: Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania WAT, Warszawa.
41. Szymanek V., 2013, Społeczeństwo Informacyjne w liczbach, Ministerstwo Administracji i Cyfryzacji, Warszawa.
42. Świątkowska J., 2014, Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny, Wydawnictwo Instytut Kościuszki, Kraków.

43. Tekielska P., Czekaj Ł., 2014, Działania służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego [w:] Gorka M. (red.), Cyber-bezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Wydawnictwo Difin, Warszawa.
44. Vuorikari R., Kluzer S., Punie Y., 2022, DigComp 2.2. The Digital Competence Framework for Citizens, Luxembourg Publications Office of the European Union.
45. Wawrzusiszyn A., 2015, Bezpieczeństwo. Strategia. System. Teoria i praktyka w zakresie. Wydawnictwo Difin SA, Warszawa.
46. Wilk M., 2000, Państwo w dobie społeczeństwa informacyjnego – perspektywa strategicznych zmian, [w:] Internet 2000. Prawo – ekonomia – kultura, Skubisz R. (red.), Wydawnictwo Oficyna Wydawnicza Verba, Lublin.
47. Zabłocki E., 2012, System bezpieczeństwa narodowego, Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych, Dęblin.
48. Zaczyński W., 1990, Praca badawcza nauczyciela, Wydawnictwo WSiP, Warszawa.

Artykuły w czasopismach

1. Aid M. M., 2012, Intel wars: The secret history of the fight against terror, New York.
2. Carr J., 2011, Inside Cyber Warfare, 2nd Edition Mapping the Cyber Underworld, O'Reilly Media.
3. Crowther G.A., 2017, The Cyber Defense Review, Vol. 2, No. 3, Army Cyber Institute.
4. Czarkowski J. et al., 2023, Zarządzanie Służbą Więzienną oparte na ochronie dynamicznej z wykorzystaniem luki kompetencyjnej, The Prison Systems Review, nr 118, Warszawa.
5. Dean A., 2012, Cyber Threats in the 21st Century, Security, vol. 49 (9).
6. Drawińska-Kania B., 2017, Koszty cyberprzestępczości-perspektywa rachunkowości, Zeszyty Naukowe SGH w Warszawie, nr 157.
7. Górka M., 2017, Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa, Cywilizacja i polityka, nr 15.
8. Gwoździewicz S., Cieślikowska M., 2020, Determinants of Social Development. About the Power of Expansion of (New) Technologies. International Journal of New Economics And Social Sciences (IJONESS).

9. Hoffman B., 2006, Foreword, [w:] Weimann G., Terror on the Internet. The New Arena, the New Challenges, Washington.
10. Kozłowska-Kalisz P., 2022, Hacking, [w:] Kodeks karny. Komentarz aktualizowany, Mozgawa M. (red.), LEX/el., art. 267.
11. Pieczywok A., 2019, Cyber threats and challenges targeting Man versus his education, Cybersecurity and Law, nr 1.
12. Piękoś K., 2017, Ataki cybernetyczne na systemy bankowe oraz infrastrukturę krytyczną – analiza wybranych przypadków, Krakowskie Studia Małopolskie, nr 22.
13. Rzucidło J., Węgrzyn J., 2015, Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni, Przegląd Prawa Konstytucyjnego, nr 5/27.
14. Sienkiewicz P., 2012, Bezpieczeństwo cyberprzestrzeni państwa, Zeszyty Naukowe Uniwersytetu Szczecińskiego. Seria Ekonomiczne problemy usług, nr 88.
15. Sienkiewicz P., 2015, Ontologia cyberprzestrzeni, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, nr 13.
16. Sienkiewicz P., Świeboda H., 2010, Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa, Polskie stowarzyszenie zarządzania wiedzą, nr 33.
17. Szubrycht T., 2005, Cyberterroryzm jako nowa forma zagrożenia terrorystycznego, Zeszyty naukowe Akademii Marynarki Wojennej, Gdynia.
18. Trubalska J., 2015, Wybrane aspekty ochrony infrastruktury krytycznej w Polsce, Zeszyty Naukowe WSEI. Seria Administracja, nr 1.
19. Waloch A., 2019, Współczesne zagrożenia dla bezpieczeństwa państwa polskiego w cyberprzestrzeni, Studia de Securitate, nr 9.
20. Wasilewski J., 2013, Zarys definicyjny cyberprzestrzeni, Przegląd Bezpieczeństwa Wewnętrznego, nr 9.

Artykuły w materiałach konferencyjnych

1. Ottis R.; Lorents P., 2010, Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security: 5th International Conference on Information Warfare and Security, Academic Conferences Limited, Dayton, Ohio, USA.

Normy

ISO/IEC/27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principle of incident management.

Ustawy

1. Konstytucja RP z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483 z późn. zm.).
2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. 1997 nr 88, poz. 553 z późn. zm.).
3. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r. poz. 655 z późn. zm.).
4. Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. 2016 poz. 542 z późn. zm.).
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64, poz. 565, z późn. zm.).
6. Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. 1997 nr 9 poz. 43 z późn. zm.).
7. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 nr 89, poz. 590, z późn. zm.).
8. Ustawa z dnia 27 grudnia 2019 r. o finansach publicznych (Dz.U. 2009 nr 157 poz. 1240 z późn. zm.).
9. Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz.U. 2017, poz. 2184; 2019, poz. 1815; 2020, poz. 695 z późn. zm.).
10. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323 z późn. zm.).
11. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323 z późn. zm.).
12. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560 z późn. zm.).
13. Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2018 poz. 646 z późn. zm.).
14. Wyrok Trybunału Konstytucyjnego z dnia 12 stycznia 1999 r., sygn. P. 2/98, (Dz. U. 1999, nr 3, poz. 30).

Akty prawa międzynarodowego

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.
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) 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2), art. 16.
3. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM (2007) 267, Bruksela 2007.
4. Rezolucja Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013/2606(RSP)), (Dz.U.UE C z dnia 9 marca 2016 r.) z późn. zm.).
5. 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).
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).

Rozporządzenia

1. Decyzja Nr 151/MON z dnia 14 października 2021 r. zmieniająca decyzję w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.
2. Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla

szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz. U. 2017 r. poz. 356 z późn. zm.).

3. Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz. U. z 2017 r. poz. 356 z późn. zm.).
4. Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz. U. z 2018 r. poz. 467 z późn. zm.).
5. Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie utworzenia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318 z późn. zm.).
6. Zarządzenie nr 69/MON z dnia 20 września 2021 r. zmieniające zarządzenie w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej.

Doktryny, strategie

1. Doktryna Cyberbezpieczeństwa RP, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.
2. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017.
3. Polityka Ochrony Cyberprzestrzeni RP, Warszawa 2013 (M.P. 2013 poz. 111 z późn. zm.).
4. Rządowe Centrum Bezpieczeństwa, Narodowy Program Ochrony Infrastruktury Krytyczne, Warszawa 2013.
5. Strategia Bezpieczeństwa Narodowego, Warszawa 2020 (M.P. 2020 poz. 413 z późn. zm.).
6. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Warszawa 2019 (M.P. 2019 poz. 1037 z późn. zm.).
7. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa 2017 (M.P. 2017 poz. 52 z późn. zm.).

Opracowania i raporty z badań

1. Abramczuk K. et al., 2019, Polskie badanie EU Kids Online 2018, Wydawnictwo naukowe UAM, Poznań.
2. Chaudron S., Di Gioia R., Gemo M., 2018, Young Children (0-8) and Digital Technology. A qualitative study across Europe, Luxembourg.
3. https://aktualnosci.komputronik.com/253528-przepasc-w-zakresie-umiejetnosci-cyfrowych-miasta-deklasuja-obszary-wiejskie [dostęp 17.12.2023 r.].
4. https://cik.uke.gov.pl/aktualnosci-cik/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2021,21.html [dostęp 17.12.2023 r.].
5. https://uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html [dostęp 17.12.2023 r.].
6. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html [dostęp 13.12.2023 r.].

Strony i komunikaty Internetowe

1. Act on Cyber Security, The Government of Czech Republic, 2015, https://nukib.cz/download/publications_en/legislation/nbu_zkb_navrh_130723_senat_EN.pdf [dostęp 01.09.2021.].
2. Australian Government, List of glossary terms, https://www.cyber.gov.au/learn-basics/view-resources/glossary/c [dostęp 01.09.2023 r.].
3. Austrian Cyber Security Strategy, The Government of Austria, 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf [dostęp 01.09.2021 r.].
4. Borkowska A., 2023, Uczeń w cyfrowym świecie. Jak projektować działania profilaktyczne w szkole i przedszkolu, Wydawnictwo PIB NASK, Warszawa, https://it-szkola.edu.pl/publikacje,plik,97 – [dostęp 04.05.2024 r.].
5. Centrum Cyfrowe. Lekcja: Enter. 2020. Online, https://www.isp.org.pl/uploads/drive/aktualnosci/RAPORT_Dyrektorzy_do_zadan_specjalnych_08.06.pdf [dostęp 21.12.2023 r.].
6. Cyber Security Concept of the Slovak Republic for 2015-2020, The Government of Slovak Republic, 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 [dostęp 30.08.2021 r.].
7. Cyber Security Strategy – Republic of Estonia, 2019-2022, The Government of Estonia, 2019, https://www.enisa.europa.eu/topics/national-cyber-security-

strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia [dostęp 01.09.2021 r.].
8. Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space, The Government of the United Kingdom, 2009, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 03.09.2021 r.].
9. Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space, The Government of the United Kingdom, 2009, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 01.09.2021 r.].
10. Cyber Strategy for Germany, 2011, Federal Minister of the Interior and Community, https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 [dostęp 02.09.2021 r.].
11. Cyber Strategy for Germany, 2011, Federal Minister of the Interior and Community, https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 [dostęp 02.09.2021 r.].
12. Cyber Strategy of Romania, The Government of Romania, 2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Romania [dostęp 01.09.2021 r.].
13. Digital Competence Framework for the European Schools, https://www.eursc.eu/BasicTexts/2020-09-D-51-en-2.pdf, Joint Teaching Committee, [dostęp 22.11.2023 r.].
14. 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, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148 [dostęp 02.08.2021 r.].
15. Fireeye, APT28: A Window Into Russia's Cyber Espionage Operations?, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyberespionage-operations.html [dostęp 28.07.2021 r.].
16. Fireeye, M-Trends 2015, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf [dostęp 28.07.2021 r.].

17. French National Digital Security Strategy, 2015, The Government of France, https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf [dostęp 01.09.2021 r.].
18. French White Paper, Defence and National Security, The Government of The Republic of France, 2013, https://ccdcoe.org/uploads/2018/10/White-paper-on-defense-2013-1.pdf [dostęp 01.08.2024].
19. Hanna K. T., Ferguson K., Rosencrance L., cyberterrorism, https://searchsecurity.techtarget.com/definition/cyberterrorism, [dostęp 28.07.2021 r.].
20. http://repozytorium.amu.edu.pl:8080/bitstream/10593/5615/1/19_Marian_Golka_Czym%20jest%20spo%C5%82ecze%C5%84stwo%20informacyjne_253-265.pdf [dostęp 20.11.2021 r.].
21. https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-ataki-rosji-na-nato-wywiad-ocenia-ryzyko [dostęp 23.10.2023 r.].
22. https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-cyberbezpieczenstwo-2030-co-bedzie-najwiekszym-zagrozeniem [dostęp 21.10.2023 r.].
23. https://cyberdefence24.pl/cyberbezpieczenstwo/znamy-wyniki-testu-umiejetnosci-cyfrowych-w-polskich-szkolach-nie-jest-najlepiej- [dostęp 17.02.2024 r.].
24. https://cyberpolicy.nask.pl/akt-o-cyberbepzieczenstwie-certyfikacja-cyberbezpieczenstwa/ [dostęp 10.06.2021 r.].
25. https://cyberpolicy.nask.pl/akt-o-cyberbezpieczenstwie-nowy-mandat-enisa/ [dostęp 22.05.2022 r.].
26. https://cybersecforum.eu/ [dostęp 03.09.2021 r.].
27. https://cyfrowapolska.org/pl/umiejetnosci-cyfrowe-polskich-uczniow-do-poprawy-znamy-wyniki-pierwszego-w-polsce-cyfrowego-testu/ [dostęp 17.12.2023 r.].
28. https://cyfrowekompetencje.pl/articles/ksztaltowanie-kompetencji-cyfrowych-nauczycieli-nowe-stare-wyzwania-spoleczenstwa-informacyjnego-w-polsce - [dostęp 04.05.2024 r.].
29. https://digital-skills-jobs.europa.eu/en/inspiration/research/oecd-skills-digital-transition-2022 [dostęp 22.11.2023 r.].

30. https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers [dostęp 24.02.2024 r.].
31. https://digital-strategy.ec.europa.eu/pl/policies/desi-poland– [dostęp 17.12.2023 r.].
32. https://digital-strategy.ec.europa.eu/pl/policies/desi-poland [dostęp 17.12.2023 r.].
33. https://dyzurnet.pl/ [dostęp 06.03.2022 r.].
34. https://dyzurnet.pl/badania [dostęp 06.03.2022 r.].
35. https://dyzurnet.pl/o-nas [dostęp 06.03.2022 r.].
36. https://ec.europa.eu/commission/presscorner/detail/pl/QANDA_20_2392 [dostęp 03.05.2024 r.].
37. https://ec.europa.eu/eurostat/cache/metadata/en/isoc_sk_dskl_i21_esmsip2.htm [dostęp 10.06.2023 r.].
38. https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21__custom_2397093/bookmark/map?lang=en&bookmarkId=dc481686-c938-4e07-b03c-8e039f532857 [dostęp 17.12.2023 r.].
39. https://encyklopedia.pwn.pl/haslo/3905881/globalizacja.html%20target= [dostęp 29.11.2021 r.].
40. https://eskamedia.pl/2020/05/04/swiat-to-globalna-wioska/ [dostęp 20.11.2021 r.].
41. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020JC0018 [dostęp 03.05.2024 r.].
42. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32019R0881 [dostęp 03.11.2021 r.].
43. https://itwiz.pl/cert-polska-i-skw-ostrzegaja-przed-dzialaniami-rosyjskich-szpiegow/ [dostęp 10.06.2023 r.].
44. https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#:~:text=In%20DigComp%2C%20digital%20competence%20involves,and%20for%20participation%20in%20society [dostęp 22.11.2023 r.].
45. https://kicb.pl/rada-ue-przyjela-nis-2/ [dostęp 11.02.2023 r.].
46. https://ose.gov.pl/ [dostęp 20.05.2022 r.].
47. https://sherloc.unodc.org/cld/uploads/res/lessons-learned/strategia-de-securitate-cibernetica-a-

romaniei_html/STRATEGIA_de_securitate_cibernetic_a_Romanei.pdf [dostęp 01.09.2023 r.].
48. https://sherloc.unodc.org/cld/uploads/res/lessons-learned/strategia-de-securitate-cibernetica-a-romaniei_html/STRATEGIA_de_securitate_cibernetic_a_Romanei.pdf [dostęp 01.09.2021 r.].
49. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html [dostęp 18.02.2024 r.].
50. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html [dostęp 18.02.2024 r.].
51. https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/11/6.pdf [dostęp 01.09.2021 r.].
52. https://www.bbn.gov.pl/pl/wolnytekst/3237,Cyberprzestrzen-w-ustawach-ostanach-nadzwyczajnych.html [dostęp 15.05.2022 r.].
53. https://www.benchmark.pl/aktualnosci/ile-czasu-spedzamy-przed-ekranami-w-erze-pandemii.html [dostęp 06.01.2022 r.].
54. https://www.cisa.gov/national-strategy-secure-cyberspace [dostęp 04.09.2021 r.].
55. https://www.computerworld.com/article/2523545/the-fog-of--cyber--war.html [dostęp 01.08.2022 r.].
56. https://www.czasopismobiologia.pl/artykul/internet-a-edukacja-seksualna-mlodziezy-czyli-o-wyimaginowanym-wizerunku-seksu-oraz-tworzeniu-nieistniejacych-standardow-i-norm-seksualnych-w-sieci [dostęp 06.03.2022 r.].
57. https://www.digcomp.pl/wp-content/uploads/2023/03/DigComp2.2_TEXT_pl_.pdf [dostęp 17.02.2024 r.].
58. https://www.domowezasadyekranowe.fdds.pl/problem/ - [dostęp 04.05.2024 r.].
59. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [dostęp 17.02.2024 r.].
60. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [dostęp 02.05.2023 r.].
61. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [dostęp 02.05.2023 r.].

62. https://www.enisa.europa.eu/news/foresight_2030_infographic.png- [dostęp 03.05.2023 r.].
63. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [dostęp 10.05.2023 r.].
64. https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi [dostęp 10.06.2023 r.].
65. https://www.gov.pl/web/baza-wiedzy/zagr-techniczne [dostęp 15.08.2022 r.].
66. https://www.gov.pl/web/cyfryzacja/akt-o-cyberbezpieczenstwie [dostęp 10.06.2021 r.].
67. https://www.gov.pl/web/cyfryzacja/centrum-rozwoju-kompetencji-cyfrowych [dostęp 17.12.2023 r.].
68. https://www.gov.pl/web/cyfryzacja/dumc-2020-poz3 [dostęp 17.12.2023 r.].
69. https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.].
70. https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 17.12.2023 r.].
71. https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe [dostęp 19.11.2023 r.].
72. https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa [dostęp 15.03.2022 r.].
73. https://www.gov.pl/web/cyfryzacja/ponad-25-mld-na-program-rozwoju-kompetencji-cyfrowych [dostęp 17.12.2023 r.].
74. https://www.gov.pl/web/edukacja-i-nauka/bezpieczenstwo-fizyczne-i-cyfrowe-uczniow--poradnik-men [dostęp 06.03.2022 r.].
75. https://www.gov.pl/web/edukacja-i-nauka/robocze-spotkanie-dotyczace-utworzenia-narodowego-centrum-sztucznej-inteligencji-i-cyberbezpieczenstwa-z-udzialem-ministra-edukacji-i-nauki [dostęp 06.03.2022 r.].
76. https://www.gov.pl/web/obrona-narodowa/departament-cyberbezpieczenstwa [dostęp 06.03.2022 r.].
77. https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp 23.10.2022 r.].
78. https://www.ibm.com/reports/threat-intelligence [dostęp 21.08.2023 r.].
79. https://www.klgates.com/Happy-NIS-Year-Everyone-A-New-Common-Cybersecurity-Framework-for-the-European-Union-1-13-2023 [dostęp 11.02.2023 r.].
80. https://www.nask.pl/pl/aktualnosci/2274,Dolacz-do-Europejskiego-Miesiaca-Cyberbezpieczenstwa.html [dostęp 22.05.2022 r.].

81. https://www.nask.pl/pl/aktualnosci/3977,cyberbezpiecznysamorzad-ruszamy-ze-szkoleniami.html [dostęp 06.03.2022 r.].
82. https://www.nask.pl/pl/aktualnosci/4301,NASK-podczas-Cyber24Day.html [dostęp 06.03.2022 r.].
83. https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html [dostęp 06.03.2022 r.].
84. https://www.porp.pl/kompetencje-cyfrowe-czy-polska-efektywnie-wykorzystuje-potencjal-technologii-cyfrowych [dostęp 22.11.2023 r.].
85. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/2016-scrty-prsprty-en.pdf [dostęp 01.08.2024].
86. https://www.traple.pl/raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa-dotyczacy-zagrozen-dla-bezpieczenstwa-informacji-z-2022-r/ [dostęp 21.08.2023 r.].
87. https://www.verizon.com/business/resources/reports/dbir/ [dostęp 10.05.2023 r.].
88. https://www.weforum.org/agenda/2022/04/europe-basic-digital-skills/ [dostęp 03.05.2023 r.].
89. https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/ncbc-dkwoc-dzieli-sie-wiedza/ [dostęp 15.05.2022 r.].
90. https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf [dostęp 01.06.2023 r.].
91. https://www.wojsko-polskie.pl/woc/zadania/ [dostęp 15.05.2022 r.].
92. https://www.youtube.com/watch?v=K2c0fCbUBKc [dostęp 03.09.2021 r.].
93. Luiijf E., Besseling K., De Graff P., 2013, Nineteen national cyber security strategies, International Journal of Critical Infrastructures, vol. 9, ½, https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies [dostęp 01.09.2021 r.].
94. National Cyber Security Agenda. A cyber secure Netherlands, The Government of the Netherlands, 2018, https://www.cyberwiser.eu/sites/default/files/NL_NCSS_2018_en%20%282%29.pdf [dostęp 06.09.2021 r.].
95. National Cyber Security Agenda. A cyber secure Netherlands, The Government of the Netherlands, 2018, https://www.cyberwiser.eu/sites/default/files/NL_NCSS_2018_en%20%282%29.pdf [dostęp 01.09.2021 r.].

96. National Cyber Security Strategy 2016-2021, The Government of the United Kingdom, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [dostęp 05.09.2021 r.].
97. National Cyber Security Strategy for Greece, The Government of the Hellenic Republic, 2020, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/GRNCSS_EN.pdf [dostęp 01.09.2021 r.].
98. National Cyber Security Strategy, The Government of The Republic of Lithuania, 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf [dostęp 01.09.2023 r.].
99. National Infromation Security Strategy, The Government of Uganda, 2011, https://www.cert.ug/sites/default/files/2022-05/National%20Information%20Security%20Strategy%202011.pdf [dostęp 01.09.2021].
100. National Strategy to Secure Cyberspace, U.S. Department of Homeland Security, 2003, https://georgewbush-whitehouse.archives.gov/pcipb/ [dostęp 04.09.2021 r.].
101. New Zeland's Cyber Security Strategy, The Government of New Zeland, 2015, https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf [dostęp 01.09.2021].
102. Smigol, Cyberświat, https://www.twojewiersze.pl/pl/wiersz,aTFWNjMyQDNrN0I5KDk8MGQzcTE [dostęp 02.01.2022 r.].
103. Słownik pojęć z zakresu społeczeństwa informacyjnego, Komisja Europejska, https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http://eurovoc.europa.eu/6140 [dostęp 04.09.2021 r.].
104. Statystyki w Internecie, www.internetworldstat.com/stats.htm [dostęp 02.06.2021 r.].
105. Strategy of the Czech Republic in the field of cybernetic security, The Government of Czech Republic, 2015, https://nukib.gov.cz/en/cyber-security/strategy-action-plan/ [dostęp 01.09.2023 r.].

106. The Cyber Security Environment in Lithuania, The Government of The Republic of Lithuania, 2018, https://www.vkontrole.lt/failas.aspx?id=3504 – [dostęp 01.09.2021 r.].
107. The Cyber Security National System, The Government of Romania, 2013, https://cyberwiser.eu/romania-ro#:~:text=The%202013%20strategy%20includes%20a,capabilities%2C%20increasing%20the%20resilience%20of [dostęp 01.09.2023 r.].
108. The Cyber Security National System, The Government of Romania, 2013, https://cyberwiser.eu/romania-ro#:~:text=The%202013%20strategy%20includes%20a,capabilities%2C%20increasing%20the%20resilience%20of [dostęp 01.09.2023 r.].
109. Waloch A., 2019, Annales Universitatis Paedagogicae Cracoviensis, https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2019/11/11.pdf [dostęp 01.09.2021 r.].

Spis rysunków

Spis tabel

Spis wykresów

Streszczenie

Rozprawa doktorska podejmuje tematykę poziomu kompetencji cyfrowych użytkowników sieci (Internetu) i ich możliwego wpływu na system cyberbezpieczeństwa RP. Celem głównym rozprawy jest zbadanie istniejących rozwiązań państwa polskiego w zakresie działań realizowanych na rzecz budowania oraz podnoszenia kompetencji cyfrowych użytkowników określonych w dokumentach strategicznych i regulacjach prawnych w zakresie cyberbezpieczeństwa RP. Hipoteza jest następująca: skuteczne zwiększanie poziomu świadomości i kompetencji cyfrowych może mieć kluczowe znaczenie dla kształtowania systemu cyberbezpieczeństwa państwa.

Praca ma charakter teoretyczno-empiryczny. Rozdziały I-V poświęcone zostały przybliżeniu oraz wyjaśnieniu podstaw związanych z cyberbezpieczeństwem, cyberprzestrzenią, kompetencjami cyfrowymi oraz regulacjami prawnym w tym zakresie. W następnej części dysertacji dokonano analizy przeprowadzonych wywiadów eksperckich i badania ankietowego. Celem pozyskania danych niezbędnych do uzyskania odpowiedzi na pytania przedstawione w pracy, przeprowadzono pięć wywiadów eksperckich oraz sondaż wśród 1500 nauczycieli oraz 2500 uczniów.

I rozdział rozprawy został poświęcony metodologicznym podstawom dysertacji. Ujęte zostały przyczyny podjęcia badań, przedmiot badań, ich cel, problemy naukowe. Wyszczególniono również hipotezy robocze, metody badawcze i ograniczenia badawcze. Dokonano analizy stanu wiedzy, która zawierała przegląd literatury przedmiotu.

Część II o tytule *„Istota cyberbezpieczeństwa”* obejmowała przede wszystkim kwestie terminologiczne i zakresy pojęciowe *„cyberprzestrzeni”* oraz *„cyberbezpieczeństwa”.* Na końcu rozdziału, tak jak w poprzednim zawarto skonkretyzowane wnioski własne autora.

Rozdział III dotyczył dokumentów strategicznych i regulacji prawnych w obszarze cyberbezpieczeństwa. Uwzględniono zarówno krajowe, jak i międzynarodowe uwarunkowania prawne. Wyszczególniono podmioty i instytucje właściwe w obszarze budowania świadomości i kompetencji cyfrowych. We wnioskach znalazły się skonkretyzowane treści i przykłady.

Odnosząc się do regulacji prawnych poszczególnych państw, rozbieżności w zakresie cyberbezpieczeństwa należy niwelować. Każde państwo członkowskie UE musi spełniać określone kryteria, jakie są przed nim stawiane. Ma to ułatwić współtworzenie systemu zintegrowanego, zapewniającego skuteczne bezpieczeństwo w cyberprzestrzeni. Działania te powinny być ukierunkowane na bezpieczeństwo obywateli jak i całego państwa, tak aby każdy użytkownik mógł swobodnie i bez obaw w pełni korzystać z wynalazków jakie niesie za sobą cyfryzacja i rozwój technologii teleinformatycznych.

W kolejnej części pracy wskazano identyfikację, klasyfikację i charakterystykę zagrożeń cyberprzestrzeni, tj. ataki, kradzieże, blokowanie dostępu, spam czy ataki socjotechniczne i wynikające z nich wyzwania cyberprzestrzeni.

Analizując problem zagrożeń w cyberprzestrzeni spotkać się można z opiniami, iż zagrożenia te nie należą do szczególnie istotnych, ponieważ w obszarze systemów cywilnych człowiek nie może zostać fizycznie poszkodowany, doznać uszczerbku na zdrowiu czy też życiu. Argumentacja ta nie jest trafna. Ataki hakerów na niektóre z cywilnych systemów informatycznych spowodować mogą powstanie bezpośrednich zagrożeń zdrowia i życia ludzi np. w kwestii systemów kierowania ruchem lotniczym bądź systemów sterujących przebiegiem telechirurgicznych operacji.

W rozdziale V rozprawy dokonano analizy poziomu kompetencji cyfrowych użytkowników ze szczególnym uwzględnieniem uczniów szkół podstawowych i nauczycieli. Dzięki pogłębionej eksploracji wskazanego obszaru możliwe było opracowanie porównania na tle europejskich państw. Wskazano różne rozumienie pojęcia „kompetencji cyfrowych" w kluczowych instytucjach państwowych i międzynarodowych oraz wypracowano własną charakterystykę tego terminu. Analizując podział kompetencji cyfrowych należy mieć na uwadze ich zakresy (tj. m.in. umiejętność korzystania z oprogramowania, umiejętność rozwiązywania problemów cyfrowych, umiejętność tworzenia treści cyfrowych czy umiejętność współpracy online).

Ostatni element dysertacji dotyczy kluczowego, z punktu widzenia niniejszej pracy zagadnienia, jakim są wywiady eksperckie i badanie ankietowe. Pracę podsumowuje koncepcja zmian, zakończenie i wykaz bibliografii.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, kompetencje cyfrowe

Summary

The dissertation addresses the topic of the level of digital competences of network (Internet) users and their possible impact on the cyber security system of the Republic of Poland. The main aim of the dissertation is to examine existing solutions of polish state within the scope of activities implemented for building and improvement of digital competences of users specified in strategic documents and strategic documents and legal regulations on the cybersecurity of the Republic of Poland. Hypothesis is as follows: effective raising of awareness and digital competences may be of key importance for shaping the system of the country's cyber security.

The work is of a theoretical and empirical. Chapters I-V are devoted to introduce and explain the basics related to cyber security, cyber digital competences and legal regulations in this area. The next part of the dissertation analyses the expert interviews and survey conducted survey. In order to obtain the data necessary to answer the questions presented in the dissertation, five expert interviews and a survey of 1,500 teachers and 2,500 students were conducted.

Chapter I was devoted to the methodological foundations of the dissertation. It covers the reasons to undertake the research, the subject of the study, its purpose, and the research problems. The working hypotheses, research methods and research limitations are also detailed. A analysis of the state of knowledge, which included a review of the literature on the subject.

Part II, entitled ‘The essence of cyber security’ mainly covered terminological issues and the conceptual scopes of ‘cyberspace’ and ‘cyber security’. At the end of the chapter, as in the previous one, the author's own conclusions were concretised.

Chapter III handle with strategic documents policy documents and legal regulations in the area of cyber security. Consideration was given to both national and international legal conditions. Entities and institutions competent in the area of building digital awareness and competence. The conclusions include concretised content and examples.

With reference to the legal regulations of individual countries, discrepancies in the area of cyber security should be bridged. Each EU member state must comply with certain criteria that are set before it. This is to facilitate co-development of an integrated system to ensure effective security in cyberspace. These measures should focus on the security of citizens and the country as a whole, so that every user can freely and without fear of taking full advantage of the inventions brought about by digitisation and the development of ICT technologies.

The following part of the dissertation indicates identification, classification and characteristics of threats in cyberspace, i.e. attacks, theft, blocking of access, spam or socio-technical attacks and the resulting challenges of of cyberspace.

When analysing the problem of threats in cyberspace, one can find opinions that these threats are not particularly significant, because in the area of civil systems, people cannot be physically harmed, harmed in health or harmed in life. This argumentation is not accurate. Attacks by hackers on some of the civilian IT systems may cause direct threats to the health and lives of people, e.g. in terms of air traffic control systems or systems controlling the course of telesurgical operations.

Chapter V of the dissertation contains an analysis of the level of digital competences of users, with particular emphasis on primary school students and teachers. Thanks to an in-depth exploration indicated area it was possible to develop a comparison with European countries. Different understandings of the concept of 'digital competence' in key national and international institutions and developed their own characterisation of the term. When analysing the division of digital competences, their ranges should be kept in mind (i.e., among other things, the ability to use software, digital problem-solving skills, digital content creation skills or online collaboration skills). or online collaboration skills).

The final element of the dissertation concerns deals with the key issue, from the point of view of this work, which is expert interviews and a survey. The dissertation concludes with a concept for changes, a conclusion and a list of bibliographies.

Keywords: cyber security, cyber threat, digital competences