WOJSKOWA AKADEMIA TECHNICZNA

im. Jarosława Dąbrowskiego

Rada Dyscypliny Naukowej "Nauki o Bezpieczeństwie"

ROZPRAWA DOKTORSKA

Temat:

KSZTAŁTOWANIE ŚWIADOMOŚCI SYTUACYJNEJ W SYSTEMACH ZARZĄDZANIA KRYZYSOWEGO Z WYKORZYSTANIEM WYBRANYCH PLATFORM IT

Autor:

mgr inż. Marcin STARUCH

Promotor:

prof. dr hab. inż. Piotr ZASKÓRSKI

Promotor pomocniczy:

dr Jacek WOŹNIAK

Warszawa 2024

Streszczenie

Celem rozprawy jest ocena poziomu świadomości sytuacyjnej społeczeństwa w odniesieniu do zagrożeń oraz identyfikacja i analiza aktualnie stosowanych technologii oraz ocena ich przydatności w zakresie kształtowania świadomości sytuacyjnej w sytuacjach kryzysowych.

Hipoteza główna jest następująca: System informowania ludności posiada istotne luki, co ujemnie wpływa na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów, które można eliminować poprzez wykorzystanie nowoczesnych rozwiązań teleinformatycznych (IT/ICT[1]).

Hipoteza główna została zdekomponowana na pięć hipotez szczegółowych:

1. Świadomość sytuacyjna ludności o zagrożeniach i ryzyku utraty bezpieczeństwa w warunkach materializacji zagrożeń i kryzysów kształtuje się na niskim poziomie.
2. W funkcjonującym systemie informowania ludności o zagrożeniach poziom świadomości sytuacyjnej ludności nie jest determinowany złożonością tego systemu.
3. Skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej a sprawnością systemu informowania w warunkach zagrożeń i kryzysów.
4. Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów.
5. Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja.

Główny problem badawczy koncentruje się wokół odpowiedzi na pytanie:

1. Jak zdefiniować poziom świadomości sytuacyjnej na potrzeby systemu informowania ludności w sytuacjach kryzysowych i jak zapewnić oczekiwany (pożądany) jego poziom?

[1] IT/ICT - zróżnicowany zestaw narzędzi technicznych i zasobów używanych do komunikowania się, przechowywania, tworzenia, udostępniania lub wymiany informacji.

Dla głównego problemu badawczego sformułowane zostało pięć **szczegółowych problemów badawczych**:

1.1. W czym wyraża się istota i jakie mogą być systemowe determinanty świadomości sytuacyjnej ludności o zagrożeniach i sytuacjach kryzysowych?

1.2. Jaki jest aktualny poziom i jakie są determinanty świadomości sytuacyjnej (w tym wykorzystywane dotychczas technologie ICT) ludności o zagrożeniach i sytuacjach kryzysowych w istniejącym systemie zarządzania kryzysowego RP?

1.3. Czy i jak współczesne technologie IT/ ICT mogą wpływać na skuteczność i wydajność procesu informowania ludności i zwiększenia jej świadomości sytuacyjnej?

1.4. Czy i dlaczego należy wprowadzać współczesne technologie w celu zwiększenia świadomości sytuacyjnej ludności i jak skutecznie zwiększyć tę świadomość poprzez wprowadzenie współczesnych technologii IT/ICT w kontekście eliminacji lub dublowania tradycyjnych środków przekazu?

1.5. Jaki może być poziom implementacyjności proponowanej koncepcji oraz użyteczności i funkcjonalności przewidywanych rozwiązań technologicznych?

Odpowiedź na powyższe pytania pozwoliła na zbadanie możliwości wzrostu poziomu świadomości sytuacyjnej obywateli oraz zespołów zarządzania kryzysowego, co może przyczynić się do skuteczniejszego przygotowania się na zagrożenia oraz udoskonalenia procesu zwalczania skutków zaistniałych sytuacji kryzysowych.

Na podstawie kwerendy literatury, przeprowadzonych badań oraz wywiadu eksperckiego wykazano, że istnieją luki w obecnie funkcjonującym SZK, a możliwości jego udoskonalenia upatruje się zarówno we współczesnych technologiach IT/ICT jak i tradycyjnych rozwiązaniach, które odpowiednio przygotowane mogą przyczynić się do wzrostu świadomości sytuacyjnej na temat zagrożeń oraz udoskonalenia działań służb ratowniczych i Zespołów Zarządzania Kryzysowego.

Summary

The aim of the Ph.D. thesis is to assess the level of situational awareness of society in relation to threats and to identify and analyze currently used technologies and assess their usefulness in shaping situational awareness in crisis situations.

The main hypothesis is as follows: The population information system has significant gaps, which negatively affect the level of situational awareness of the population in conditions of threats and crises, which can be eliminated through the use of modern ICT solutions (IT/ICT).

The main hypothesis was decomposed into five detailed hypotheses:

1. The situational awareness of the population about threats and the risk of loss of security in the conditions of materialization of threats and crises is at a low level.
2. In the functioning system of informing the population about threats, the level of situational awareness of the population is not determined by the complexity of this system.
3. The effectiveness and efficiency of the population information system when crisis situations occur is too low and there is a negative correlation between the level of situational awareness and the efficiency of the information system in situations of threats and crises.
4. Modern information and communication technologies (ICT's) are fully useful and can constitute an alternative to traditional means, an efficient way of communication in shaping the desired level of situational awareness of the population in conditions of threats and crises.
5. There is a strong positive correlation between the use of modern information and communication technologies (ICT's) in population information systems and the level of situational awareness of the population.

The main research problem focuses on answering the question:

1. How to define the level of situational awareness for the needs of the population information system in crisis situations and how to ensure its expected (desired) level?

For the main research problem, five detailed research problems were formulated:

1.1. What is the essence and what may be the systemic determinants of the population's situational awareness of threats and crisis situations?

1.2. What is the current level and what are the determinants of situational awareness (including the ICT technologies used so far) of the population about threats and crisis situations in the existing crisis management system of the Republic of Poland?

1.3. How modern IT/ICT technologies can affect the effectiveness of the process of informing the population and increasing its situational awareness?

1.4. Should modern technologies be introduced and why to increase the situational awareness of the population and how to effectively increase this awareness by introducing modern IT/ICT technologies in the context of eliminating or duplication of traditional media?

1.5. What may be the level of implementability of the proposed concept and the usability and functionality of the expected technological solutions?

The answer to the above questions allowed us to examine the possibility of increasing the level of situational awareness of citizens and crisis management teams, which may contribute to more effective preparation for threats and improvement of the process of combating the effects of crisis situations.

Based on a literature search, research and expert interviews, it was shown that there are gaps in the currently functioning Crisis Management System, and the possibilities of its improvement are seen in both modern IT/ICT technologies and traditional solutions, which, when properly prepared, can contribute to the increase in situational awareness. on threats and improving the activities of rescue services and Crisis Management Teams.

SPIS TREŚCI

WSTĘP

Zagrożenia oraz zakłócenia w systemach działania mogą wywołać chaos skutkujący ryzykiem obniżenia zdolności systemu do realizacji założonych zadań. W przypadku systemu bezpieczeństwa państwa tego typu zjawisko przenosi się na całe społeczeństwo. Niezależnie od tego, czy dotyczy ono sytuacji kryzysowej wywołanej różnorodnymi zagrożeniami będącymi następstwem działań sił natury, działalności człowieka, czy też katastrof i awarii technicznych lub aktów terrorystycznych, zawsze powstaje realne ryzyko dla różnych komponentów tego systemu, a w tym dla władz lokalnych i systemów dziedzinowych (zdrowie, ekonomia, transport, telekomunikacja itp.), a przede wszystkim dla poszczególnych interesariuszy tych systemów, tj. centrów i organów zarządzania kryzysowego oraz podmiotów opiniodawczo-badawczych i całego społeczeństwa lub wybranych społeczności. Temat zarządzania kryzysowego staje się coraz ważniejszy w dzisiejszym niepewnym i dynamicznym środowisku, a wykorzystanie współczesnych technologii IT/ICT może przyczynić się do bardzo trafnej diagnozy i szybkiego rozwiązania kryzysu. Odpowiednio przetworzona informacja jest jednym z najważniejszych czynników skutecznego zarządzania kryzysowego, ponieważ zapewnia podstawę do podejmowania właściwych decyzji, komunikowania się z właściwymi interesariuszami, koordynowanie działań oraz przeciwdziałanie skutkom zagrożeń. Wraz z szybkim rozwojem technologii informacyjnej IT/ICT na znaczeniu zyskuje przepływ informacji i wykorzystanie różnych form komunikowania się w celu ograniczenia negatywnych skutków kryzysu.

W sytuacjach kryzysowych wyzwania związane ze zrozumieniem obecnego stanu są ściśle powiązane z umiejętnościami przetwarzania informacji dostarczanych z różnych źródeł takich jak media społecznościowe, Internet, telewizja, prasa itp. Rozwój współczesnych technologii teleinformatycznych IT/ICT powoduje, że media społecznościowe mogą zapewnić dodatkowe źródło informacji na temat zagrożeń w czasie rzeczywistym pod warunkiem, że informacje przekazywane za ich pośrednictwem są dokładnie weryfikowane, dzięki czemu możliwe jest kreowanie świadomości sytuacyjnej na temat zagrożeń oraz podniesienie poziomu bezpieczeństwa.

W sytuacjach bezpośredniego zagrożenia życia, bądź w przypadku możliwości jego wystąpienia, pojawia się niepewność, a brak odpowiedniej wiedzy na temat zagrożenia może wywołać dezorientację i panikę. Skuteczne zapobieganie sytuacji kryzysowej to kształtowanie świadomości sytuacyjnej na temat zagrożenia, oszacowanie potencjalnego ryzyka jej wystąpienia oraz opracowanie odpowiednich działań

zapobiegawczych przy wykorzystaniu tradycyjnych i współczesnych technologii IT/ICT. Odpowiednie edukowanie obywateli, a w tym pracowników, studentów i innych osób w zakresie świadomości sytuacyjnej oraz działań podejmowanych na wypadek wystąpienia sytuacji kryzysowej może zmniejszyć liczbę ofiar na obszarze dotkniętym kryzysem oraz ograniczyć straty materialne. Niemniej jednak warto zwrócić uwagę na fakt, że opisywanie świadomości sytuacyjnej jest znacznie łatwiejsze niż proces jej uzyskania. Podobnie jak większość elementów gotowości obronnej państwa w sytuacjach kryzysowych, świadomość sytuacyjna dotyczy przygotowania się na wypadek wystąpienia zagrożenia oraz niwelowania jego skutków. Niezbędne zatem jest zrozumienie istoty świadomości sytuacyjnej tj. jak poruszać się po jej trzech poziomach (postrzeganie, zrozumienie i prognozowanie) oraz w jaki sposób uzyskać i utrzymać wysoki jej poziom?

Możliwość prognozowania przyszłych zdarzeń oraz zrozumienie zjawisk zachodzących w środowisku ma kluczowe znaczenie dla kształtowania oczekiwanego poziomu świadomości sytuacyjnej. Niezdolność do poruszania się po trzech poziomach świadomości sytuacyjnej (postrzeganie, zrozumienie, prognozowanie) może zakłócić proces decyzyjny. Zarządzanie kryzysowe wymaga zatem podejmowania właściwych decyzji w dynamicznym środowisku.

Celem rozprawy jest ocena poziomu świadomości sytuacyjnej ludności na temat zagrożeń, a także identyfikacja i analiza obecnie wykorzystywanych technologii wraz z oceną ich przydatności w sytuacjach kryzysowych w zakresie kształtowania świadomości sytuacyjnej. Na podstawie przeprowadzonych badań weryfikacji poddana zostanie możliwość wykorzystania współczesnych technologii informacyjnych w procesie skutecznego i wieloaspektowego informowania ludności o zagrożeniach oraz potencjalny obszar ich zastosowania. Całość rozprawy zawarta została w siedmiu rozdziałach, które obejmują problematykę istoty świadomości sytuacyjnej ludności w systemach zarządzania kryzysowego i możliwości jej kreowania z wykorzystaniem wybranych platform informatyczno-komunikacyjnych. Praca opatrzona jest wstępem i zakończeniem oraz wykazem literatury i materiałami pomocniczymi, a w tym wykazem rysunków i tabel oraz załącznikami. Każdy rozdział kończy się syntetycznym podsumowaniem. Załączniki zawierają szczegółowe wyniki badań i dokumenty z tym związane (ankiety, wywiad ekspercki itp.).

Tematyka i zakres rozprawy umiejscowione są w dziedzinie nauk społecznych, w dyscyplinie nauk o bezpieczeństwie. Całość rozprawy jest profilowana sfor-

mułowanymi hipotezami badawczymi związanymi ściśle ze schematem badawczym a w tym z celami i problemami badawczymi przyjętymi w rozprawie oraz zbiorem metod i technik badawczych opisanych w części metodologicznej.

W rozdziale pierwszym przedstawione są podstawowe terminy, definicje i charakterystyki dziedziny podejmowanego problemu.

W rozdziale drugim przedstawione są metodologiczne podstawy badań, a w szczególności cele rozprawy i zhierarchizowane problemy i hipotezy badawcze oraz specyfikacja metod i narzędzi badawczych wraz z ramowym zamiarem i zakresem ich wykorzystania, a także źródła danych i podstawowe założenia oraz ograniczenia badawcze.

W rozdziale trzecim przedstawione są uwarunkowania strukturalno-organizacyjne funkcjonowania systemu rozpoznawania świadomości sytuacyjnej oraz scharakteryzowana jest struktura zadaniowo-funkcjonalna Rządowego Centrum Bezpieczeństwa (RCB). Podjęta jest także próba identyfikacji klęsk żywiołowych i jej stanów. Ponadto w rozdziale przedstawiona jest istota zarządzania kryzysowego oraz świadomości sytuacyjnej z uwzględnieniem informacyjnej ciągłości działania jako wieloraki czynnik świadomości sytuacyjnej, a także zakres i interpretacja wyników badań związanych z weryfikacją założonej hipotezy badawczej.

W rozdziale czwartym zidentyfikowano problemy związane z informowaniem ludności o sytuacjach kryzysowych w RP. Przedstawiona jest istota procesu informowania ludności w sytuacjach kryzysowych oraz proces wymiany informacji w czasie zaistnienia zagrożenia. W rozdziale tym zaprezentowane są również modele świadomości sytuacyjnej. Ponadto w rozdziale dokonano przeglądu aktualnie wykorzystywanych rozwiązań w procesie informowania ludności w sytuacjach kryzysowych, a także zaprezentowano zakres i interpretację wyników badań związanych z weryfikacją założonych dwóch hipotez badawczych.

W rozdziale piątym zidentyfikowano i dokonano oceny przydatności współczesnych technologii w systemach zarządzania kryzysowego. Scharakteryzowano funkcjonalność współczesnych technologii oraz możliwości ich wykorzystania w procesie informowania ludności. Zaprezentowano także analizę aktualnego stanu wyposażenia technologicznego Systemu Zarządzania Kryzysowego RP, określono możliwości udoskonalenia procesu przepływu informacji oraz kształtowania świadomości sytuacyjnej obywateli i osób funkcyjnych w Zespołach Zarządzania Kryzysowego

(ZZK). Ponadto przedstawiono zakres i interpretację wyników badań związanych z weryfikacją założonej hipotezy badawczej.

W rozdziale szóstym przedstawione są propozycje wykorzystania tradycyjnych i współczesnych technologii IT/ICT w celu udoskonalenia funkcjonowania ZZK oraz w procesie kształtowania świadomości sytuacyjnej na temat zagrożeń.

W rozdziale siódmym zawarta jest ocena implementacyjności opracowanej koncepcji z uwzględnieniem danych z badania ankietowego, wywiadu eksperckiego oraz autooceny w bezpośrednim związku z weryfikacją przyjętej hipotezy badawczej.

Praca zakończona jest całościowym **podsumowaniem i wnioskami**, które wynikają z analizy literatury przedmiotu oraz ze zrealizowanego procesu badawczego.

ROZDZIAŁ I
DZIEDZINA PROBLEMU

1.1. Świadomość sytuacyjna

Świadomość można interpretować na różne sposoby. Samo słowo świadomość wywodzi się z języka łacińskiego (*conscientia*) i składa się z dwóch członów *con* (z) oraz *scientia* (wiedza)[2]. Już sama analiza łacińskiego tłumaczenia świadomości pozwala określać świadomość jako wiedzę na temat jakiejś sytuacji bądź wydarzenia. Bardziej szczegółowo pojęcie świadomości zdefiniowane jest w *Encyklopedii PWN*, według której świadomość interpretowana jest jako „najwyższy poziom regulacji zachowania człowieka; specyficznie wewnętrzna zdolność bezpośredniego poznania otoczenia, własnej osoby i relacji z otoczeniem, przebiegająca na trzech poziomach: percepcyjnym, pojęciowo-werbalnym i samoświadomościowym”[3].

J. Hołówka uważa, że pojęcie świadomości można interpretować przez wiele stanów, a kluczową rolę odgrywa świadomość otoczenia, samego siebie oraz własnego życia psychicznego[4]. Zupełnie inaczej pojęcie świadomości określa D. Chalmers, według którego jest to stan bycia świadomym czegoś. Mówiąc dokładniej, jest to zdolność do bezpośredniego poznawania i postrzegania, odczuwania lub bycia świadomym wydarzeń.[5] Definicja ta jest przyjęta na potrzeby niniejszej pracy, ponieważ eksponuje zagadnienie związane z procesem postrzegania, który silnie determinuje poziom świadomości sytuacyjnej.

Świadomość sytuacyjna to pojęcie, które coraz częściej pojawia się w teorii zarządzania kryzysowego. C. Kennedy uważa, że świadomość sytuacyjna to wiedza na temat otoczenia oraz zjawisk w nim zachodzących[6]. Warto jednak podkreślić, że sama wiedza na temat zjawisk zachodzących w otoczeniu jest nie wystarczająca i należy stale ją poszerzać, analizować i weryfikować otrzymane informacje zanim zostaną podjęte działania. Świadomość sytuacyjna odgrywa istotną rolę w procesie identyfikacji nie tylko istniejących zagrożeń lub potencjalnych, przyszłych czynników ryzyka, ale także sposobów przeciwdziałania ich skutkom.

---

[2]B. Hennig, *Cartesian Conscientia,* “British Journal for the History of Philosophy”, 2007, Vol. 15, No.3, s. 455-484.

[3] D. Borowska-Mostafa, *Encyklopedia PWN A-Z Oryginalna Azetka*, Wydawnictwo Naukowe PWN SA, Warszawa, 2012, s. 1022.

[4] J. Hołówka, B. Dziobkowski, *Panorama współczesnej filozofii*, Wydawnictwo Państwowe Wydawnictwo Naukowe, Warszawa, 2016, s. 329.

[5] D. Chalmers, *The Conscious Mind: In Search of a Fundamental Theory,* „Oxford University Press”, 1997, s. 225.

[6] C. Kennedy, *Situational Awareness: The Urban Preppers Ultimate Guide to Situational Awareness and Survival Paperback*, “CreateSpace Independent Publishing Platform”, USA, 2016, s. 6.

W momencie wystąpienia zagrożenia należy uświadomić sobie, z jakim zagrożeniem przyszło nam się zmierzyć oraz jakie są możliwe sposoby zapewnienia bezpieczeństwa i odpowiedniego wsparcia. Dlatego też świadomości sytuacyjnej nie należy rozpatrywać wyłącznie w aspekcie umiejętności, ale przede wszystkim logicznego myślenia i racjonalnych zachowań. Rozwijanie świadomości sytuacyjnej poprzez odpowiednie ćwiczenia, takie jak kojarzenie faktów, zapamiętywanie i obserwacja różnych wydarzeń oraz ich analiza pod kątem właściwego zachowania może przyczynić się do podjęcia odpowiednich działań na wypadek wystąpienia zagrożenia. Można zatem przyjąć, że świadomość sytuacyjna to świadomość gdzie się znajdujemy, gdzie należy być, jakie zachowania są właściwie i czy coś lub ktoś stanowi zagrożenie[7]. Niektórzy Autorzy uważają, że świadomość sytuacyjna musi uwzględniać cztery komponenty[8]:

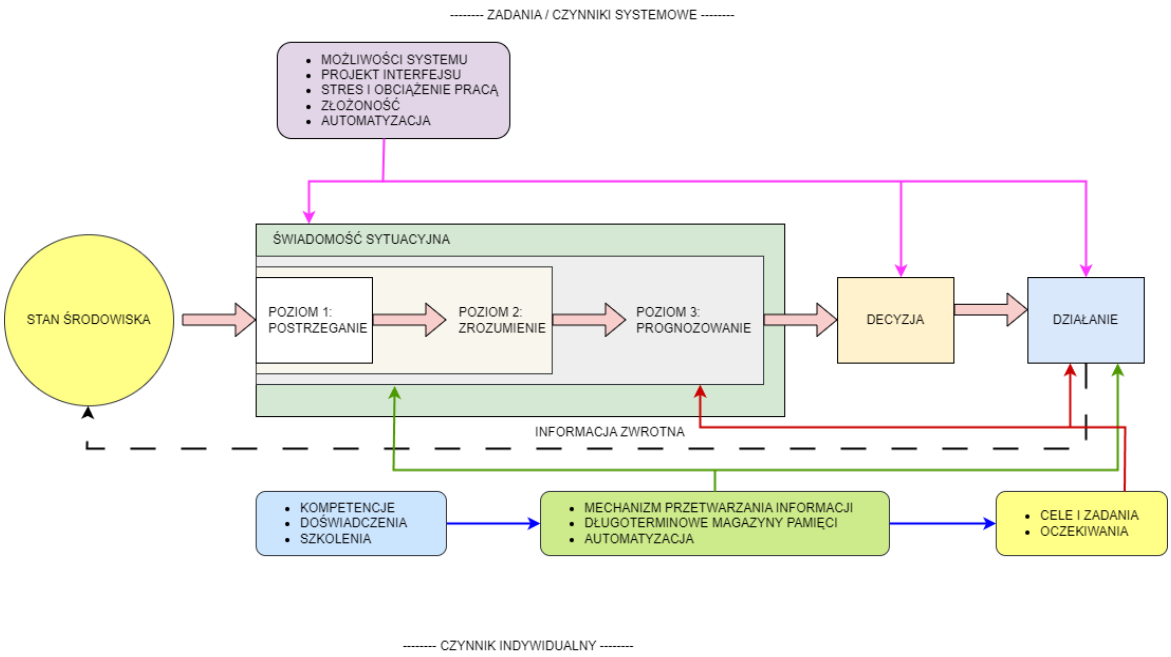
- pozyskiwanie informacji ze środowiska,
- integrowanie tych informacji z odpowiednią wiedzą wewnętrzną w celu wygenerowania mentalnego obrazu obecnej sytuacji,
- wykorzystanie tego obrazu do kreowania skutecznej percepcji w ciągłym cyklu eksploracji dostępnych zasobów informacyjnych,
- przewidywanie przyszłych wydarzeń.

Można zatem założyć, że świadomość sytuacyjna może być interpretowana jako ciągłe wyodrębnianie informacji o środowisku, integracja tych informacji z wcześniejszą wiedzą w celu utworzenia spójnego obrazu mentalnego oraz wykorzystanie tego obrazu w zapewnieniu trafnego postrzegania i przewidywania przyszłych wydarzeń. Świadomość sytuacyjną należy interpretować zatem jako postrzeganie elementów środowiskowych i zdarzeń w odniesieniu do czasu i przestrzeni, rozumienie ich znaczenia oraz projekcja ich przyszłego stanu[9].

M.R. Endsley przedstawiła trójpoziomowy model świadomości sytuacyjnej (rys. 1.1), który jest najczęściej stosowanym ze wszystkich modeli prezentowanych w literaturze przedmiotu.

---

[7] J. Szczepańska, *Świadomość sytuacyjna – Vademecum kierowcy* „Drogownictwo", Warszawa, 2010, nr 10, s.339-343.
[8] C. Domiguez, M. Vidulich, M.E. Vogel, G. McMilan, *Situation awerenesss: Papers and annotated bibliography*, Human System Center,1994, s. 17-28.
[9] M. R. Endsley, *Toward a theory of situation awareness in dynamic systems*, Human Factors, 1995, s. 35.



Rysunek 1.1. Model świadomości sytuacyjnej w kontekście procesów decyzyjnych i wykonawczych autorstwa M.R. Endsley

Źródło: Źródło opracowanie własne na podstawie: P. M. Salmon, N. A Stantion, G. H. Walker, D. P.Jenkins, Distributed Situation Awareness Theory, Measurement and Application to Teamwork, Wydawnictwo: Ashigate, Wielka Brytania 2009, s. 10

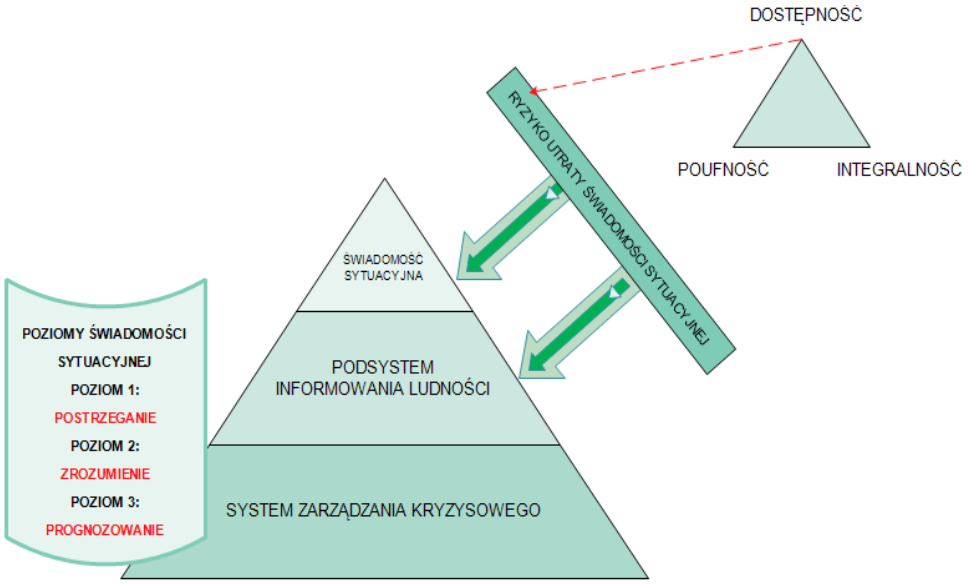
W modelu M.R. Endsley (rys.1.1) świadomość sytuacyjną przedstawia się jako wewnętrzny produkt poznawczy, który obejmuje trzy hierarchiczne poziomy, takie jak:[10]

- postrzeganie,
- zrozumienie,
- prognozowanie.

Poziomy te skojarzone są z procesami (określanymi jako ocena sytuacji) zapewniającymi ich osiągnięcie oraz zamierzonego celu (stanu świadomości). Trójpoziomowy model M.R. Endsley to wzajemnie ze sobą powiązane poziomy (rys. 1.2)[11]:

- poziom 1 – postrzeganie elementów w otoczeniu,
- poziom 2 – zrozumienie obecnej sytuacji,
- poziom 3 – prognozowanie przyszłego statusu.

[10] P. M. Salmon, N. A Stantion, G. H. Walker, D. P.Jenkins, *Distributed Situation Awareness Theory, Measurement and Application to Teamwork*, Ashgate Publishing Limited, Farnham, 2009, s. 10.
[11] Tamże, s. 10.



Rysunek 1.2. Poziomy świadomości sytuacyjnej

Źródło opracowanie własne na podstawie: P. M. Salmon, N. A Stantion, G. H. Walker, D. P.Jenkins, Distributed Situation Awareness Theory, Measurement and Application to Teamwork, Wydawnictwo: Ashgate Publishing Limited, Farnham, 2009, s. 10

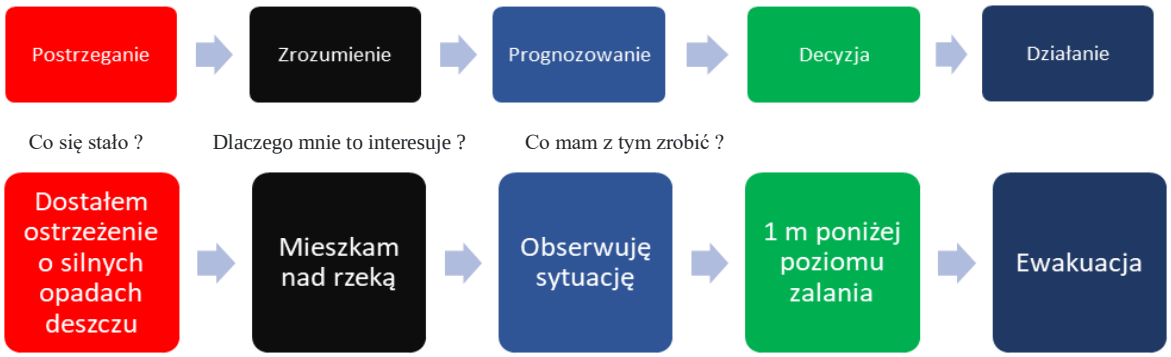
Świadomość sytuacyjna jest ważną kategorią dla skutecznego zarządzania kryzysowego. Jest to świadomość tego, co dzieje się w otoczeniu bliskim i dalszym oraz co i kto stanowi zagrożenie dla zdrowia i bezpieczeństwa danego podmiotu. Wiedza, doświadczenie i wykształcenie umożliwiają, zrozumienie tego, co dzieje się w otoczeniu danego systemu działania i jak ocenić poziom bezpieczeństwa. Oznacza to, że świadomość sytuacyjna dla wszystkich jest indywidualna i potencjalnie inna. Jest też tak dokładna, jak postrzeganie sytuacji i jej ocena. Stres i zmęczenie to jedne z głównych czynników obniżających świadomość sytuacyjną[12].

Na skutek stresu i zmęczenia zmniejsza się zdolność przetwarzania złożonych informacji oraz opóźnia się czas reakcji na zaistniałe sytuacje. Tymczasowa utrata lub brak świadomości sytuacyjnej jest przyczyną wielu zagrożeń, a nie dostrzeganie zjawisk zachodzących w otoczeniu może stanowić poważne zagrożenie dla bezpieczeństwa[13].

Osiągnięcie wysokiego poziomu świadomości sytuacyjnej jest bardzo trudne, ponieważ sytuacje kryzysowe są nieprzewidywalne w skutkach, a tempo zachodzących zmian szybkie. Za główny problem można tu zatem uznać sposób na zwiększe-

[12] Tamże s.11.
[13] Tamże s.11.

nie poziomu świadomości sytuacyjnej. Można więc przyjąć, że istotę świadomości sytuacyjnej stanowi model zaprezentowany przez M.R. Endsley[14], który jest powszechnie używany oraz model pętli OODA[15]. Są to uniwersalne koncepcje, które ułatwiają identyfikację świadomości sytuacyjnej. Niemniej forma przedstawionego przez M.R. Endsley modelu może zostać niewłaściwie zinterpretowana. W celu zrozumienia jego istoty można go rozpatrywać przez pryzmat procesu obrazującego sytuację kryzysową, np. powódź (rys. 1.3).



Rysunek 1.3. Kształtowanie świadomości sytuacyjnej na podstawie modelu M.R. Endsley

Źródło: opracowanie własne.

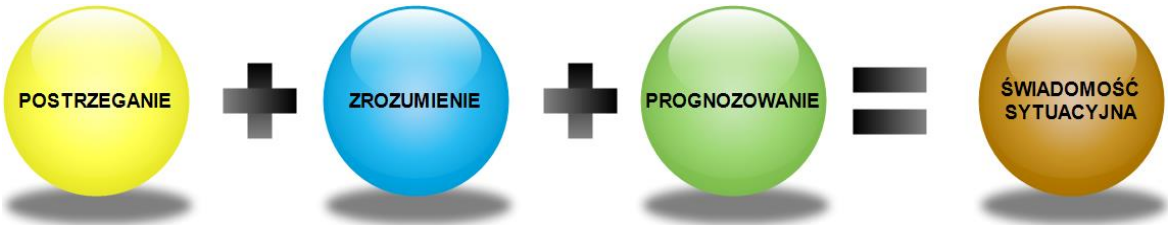
Na rysunku 1.3 przedstawiony został sposób postępowania w momencie otrzymania alertu „o opadach deszczu" – zagrożenie powodziowe. Zaprezentowana sytuacja kryzysowa dotyczy obywateli zamieszkujących tereny nad rzeką. Poprzez stałe monitorowanie poziomu wody możliwe jest podjęcie właściwych działań zmierzających do zmniejszenia bądź zniwelowania skutków zagrożenia. Ponadto wiedza na temat zagrożeń może przyczynić się do zwiększenia poziomu świadomości sytuacyjnej ludności i usprawnienia procesu informowania na temat zaistniałej sytuacji kryzysowej. Niezbędne zatem jest odpowiednie informowanie o potencjalnych zagrożeniach. Głównym problemem zatem jest wybór sposobu informowania ludności o zagrożeniach.

W celu określenia najskuteczniejszej formy przekazywania informacji na temat zagrożeń niezbędne jest przeanalizowanie aktualnie wykorzystywanych rozwiązań

[14] M. R. Endsley, *Toward a theory of situation awareness in dynamic systems*, Human Factors Journal 37(1), 1995, s. 35.
[15] J. Boyd, *The essence of winning and losing*. June 28, 1995; dostępne na stronie: https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf (data dostępu 10.11.2022).

oraz przeprowadzenie badań wśród obywateli w celu określenia skutecznej formy komunikowania się.

W systemach zarządzania kryzysowego świadomość sytuacyjna interpretowana jest jako zdolność do identyfikacji, przetwarzania oraz zrozumienia określonego zjawiska w sytuacjach kryzysowych. Oznacza to, że odpowiednie postrzeganie zagrożeń pozwala na ich zrozumienie oraz prognozowanie przyszłych zdarzeń zmierzających do dostostowania się do nowego otoczenia, w którym dany podmiot będzie się znajdował. Można zatem przyjąć, że na świadomość sytuacyjną składają się trzy komponenty: postrzeganie, zrozumienie oraz prognozowanie (rys. 1.4)[16].



Rysunek 1.4. Komponenty kształtowania świadomości sytuacyjnej
Źródło: Opracowanie własne

Świadomość sytuacyjna w głównej mierze odnosi się do różnych podmiotów działania, a w tym do obywatela. Kluczową rolę w fazie zapewniania świadomości sytuacyjnej odgrywa zapewnianie ciągłości działania w sytuacjach kryzysowych. Ciągłość działania należy interpretować jako zdolność państwa lub uprawnionego podmiotu (indywidualnego lub zbiorowego/instytucjonalnego) do zaplanowania, przygotowania oraz podjęcia odpowiednich działań zaradczych na wypadek wystąpienia zagrożenia w celu utrzymania realizacji statutowych zadań państwa[17]. Brak świadomości na temat zagrożeń oraz niewłaściwie zdefiniowane etapy, które należy wykonać w początkowej fazie sytuacji kryzysowej negatywnie wpływają na możliwość zapewnienia ciągłości działania państwa. Trwająca pandemia COVID-19 pokazała, że wiele państw oraz organizacji nie było przygotowanych na tego typu zagrożenie, co wywołało negatywne skutki w prawidłowym ich funkcjonowaniu.

Aby skutecznie przygotować się na tego typu zdarzenia niezbędne jest opracowanie planu zapewnienia ciągłości działania obejmującego następujące etapy[18]:

[16] M. Pawlak. Świadomość sytuacyjna a czynniki kulturowe. https://www.academia.edu/11791913/Świadomość_sytuacyjna_a_czynniki_kulturowe (data dostępu 19.02.2021).
[17] https://www.bmc.com/blogs/bcp-business-continuity-planning/ (data dostępu: 21.03.2021).
[18] https://resilia.pl/blog/iso-22301-ciaglosc-dzialania-czym-jest-jakie-daje-korzysci/ (data dostępu 28.04.2021).

- **Etap 1.** Przeprowadzenie oceny ryzyka i oceny jego wpływu na daną organizację, (firmę, państwo, województwo, gminę itp.) w zależności od obszaru, którego dotyczy zagrożenie.

Pierwszym etapem w planowaniu ciągłości działania jest wykonanie czynności związanych z oceną ryzyka, która obejmuje:

  - identyfikację potencjalnych zagrożeń na podstawie otoczenia,
  - analizowanie zagrożeń pod kątem prawdopodobieństwa wystąpienia,
  - ocenę tych zagrożeń,
  - określenie odpowiednich środków ograniczania ryzyka, takich jak unikanie, akceptowanie, zmniejszanie lub zniwelowanie skutków jego wystąpienia.

- **Etap 2.** Opracowanie strategii ciągłości działania.

Wyniki oceny ryzyka i działań są wykorzystywane w strategiach ciągłości działania, które uwzględniają działania przed, w trakcie i po wystąpieniu sytuacji kryzysowej oraz określają właściwe rozwiązania. Wybór strategii zależy w dużej mierze od tego, jaki poziom i jakie straty mogą być akceptowalne dla danego podmiotu, którego dotyczy zagrożenie.

- **Etap 3.** Udokumentowanie planu ciągłości działania.

Zgodnie z normą ISO 22301: 2019[19] dotyczącą wymagań związanych z systemem zarządzania ciągłością działania należy podjąć odpowiednie kroki natychmiast po zakłóceniu (zagrożeniu). Tego typu plan powinien zawierać:

  - cel,
  - role i obowiązki,
  - działania mające na celu wdrożenie rozwiązań zmierzających do zniwelowania skutków zagrożenia.

Zarządzanie ciągłością działania to proces polegający na podejmowaniu decyzji przy wykorzystaniu tradycyjnych i współczesnych technologii IT/ICT w celu zidentyfikowania potencjalnych skutków zagrożeń oraz opracowywania planów reagowania, których zadaniem jest zwiększenie odporności organizacji, w tym całego państwa na sytuacje kryzysowe i zniwelowanie ich skutków.

Plan zapewnienia ciągłości działania na wypadek wystąpienia sytuacji kryzysowej powinien zatem składać się z trzech faz[20]:

[19] Tamże.

- planowanie i zapobieganie (faza rozwiązywania problemów),
- reagowanie na zagrożenia (faza reagowania),
- powrót do funkcjonowania po zakończeniu zagrożenia (faza odbudowy).

Ramy ciągłości działania powinny nakreślać potencjalne reakcje państwa na zagrożenia. Pomimo możliwości technologicznych ze względu na złożoność sytuacji kryzysowych skuteczne zarzadzanie kryzysowe i zapewnienie ciągłości działania stanowi wyzwanie dla zespołów zarządzania kryzysowego. Dlatego też niezbędne jest wdrożenie odpowiednich procedur w tym planu zarządzania kryzysowego, aby możliwe było odpowiednie przygotowanie się na zagrożenia oraz zmniejszenie ich skutków.

1.2. Bezpieczeństwo

Według *Słownika terminów z zakresu bezpieczeństwa narodowego* bezpieczeństwo to „stan dający poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych”[21]. J. Świniarski twierdzi, że bezpieczeństwo jest to „taki stan, który zapewnia trwanie, przetrwanie i rozwój oraz doskonalenie[22], natomiast E. Poseł-Częścik uważa, że bezpieczeństwa nie należy interpretować jako synonim braku zagrożeń. Autorka uważa, że osiągnięcie stanu bezpieczeństwa polega na podjęciu kroków zmierzających do likwidacji bądź częściowego zniwelowania skutków zagrożeń. Warto jednak pamiętać, że nie jest możliwe usunięcie wszystkich zagrożeń, a zapewnienie odpowiedniego poziomu bezpieczeństwa polega na maksymalnym zmniejszeniu podatności państwa, wybranej organizacji lub obywatela na zagrożenia[23]. Biuro Bezpieczeństwa Narodowego definiuje bezpieczeństwo jako „teorię i praktykę, która zapewnia możliwość przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie

[20] https://www.businesstechweekly.com/operational-efficiency/business-continuity/business-continuity-crisis-management/#What-is-Business-Continuity (data dostępu 28.01.2023)
[21] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa narodowego,* Akademia Obrony Narodowej, Warszawa 2008, s. 14.
[22] J. Świniarski, *O naturze bezpieczeństwa,* Wydawnictwo Agencja Wydawnicza ULMAX, Warszawa 1999, s 12–13.
[23] E. Poseł-Częścik, *Kryteria bezpieczeństwa państwa,* Wydawnictwo Kryteria bezpieczeństwa międzynarodowego państwa, PISM, Warszawa 2003, s.178.

się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów". W literaturze przedmiotu można zidentyfikować następujące podstawowe rodzaje bezpieczeństwa[24]:

- bezpieczeństwo cyberprzestrzeni,
- bezpieczeństwo informacyjne,
- bezpieczeństwo wewnętrzne,
- bezpieczeństwo narodowe,
- bezpieczeństwo zewnętrzne,
- bezpieczeństwo zintegrowane,
- i inne związane z różnymi wymiarami i obszarami działania (społeczne, ekonomiczne, militarne itp.)

Bezpieczeństwo cyberprzestrzeni to kategoria obejmująca działania organizacyjno-prawne, techniczne, fizyczne oraz edukacyjne, których zadaniem jest zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni[25]. B. Pacek i R. Hoffmann uważają, że „bezpieczeństwo cyberprzestrzeni można określić jako brak ryzyka utraty danych informacyjnych w cyberprzestrzeni, a zasobem, który chronimy, jest informacja[26]".

Z kolei bezpieczeństwo informacyjne to obszar bezpieczeństwa odnoszący się do środowiska informacyjnego (w tym cyberprzestrzeni). Celem bezpieczeństwa informacyjnego jest zapewnienie bezpiecznego funkcjonowania w przestrzeni informacyjnej. Osiągnięcie takiego stanu możliwe jest poprzez realizację takich zadań, jak np.: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed destrukcyjnymi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów), działań ofensywnych w tym obszarze[27].

---

[24] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, w: R. Jakubczak i inni, Podstawy bezpieczeństwa narodowego Polski w erze globalizacji, Warszawa 2008, s. 244

[25] Twórcą pojęcia cyberprzestrzeni jest William Gibson który po raz pierwszy zdefiniował ją w książce pt. *Neuromancer*. Gibson określił cyberprzestrzeń jako „Graficzne przedstawienie danych wyabstrahowanych z banków każdego komputera w ludzkim systemie".

[26] B. Pacek, R. Hoffmann, *Działania sił zbrojnych w cyberprzestrzeni,* Wydawnictwo AON, Warszawa 2013 s. 84.

[27] Projekt Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej, Warszawa 2015, s. 3, za: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (data dostępu 26.01.2022).

Bezpieczeństwo narodowe to stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa[28]. Natomiast bezpieczeństwo wewnętrzne państwa (bezpieczeństwo krajowe) to trans-sektorowy obszar bezpieczeństwa, którego treść (cele, warunki, sposoby i środki) odnosi się do środowiska wewnętrznego państwa (środowiska krajowego)[29]. Z kolei bezpieczeństwo zewnętrzne państwa to trans-sektorowy obszar bezpieczeństwa, którego treść (cele, warunki, sposoby i środki) odnosi się do środowiska zewnętrznego państwa (środowiska międzynarodowego[30]).

W tym miejscu należy również zaznaczyć, że Bezpieczeństwo zintegrowane (kompleksowe, całościowe) to bezpieczeństwo, w którym występują (naturalne i celowo ustanowione) sprzężenia i interakcje między różnymi jego podmiotami i ich elementami, ogniwami oraz rodzajami, dziedzinami, sektorami, działami, obszarami itd., integrujące go w wewnętrznie spójną całość zapewniające jego większą skuteczność dzięki efektowi synergii [31]. Natomiast B. Jagusiak rozszerza tradycyjnie rozumiane pojęcie bezpieczeństwa i wskazuje, że jego istotę stanowią procesy społeczno-gospodarcze zachodzące wewnątrz państw, metody i sposoby rozwiązywania spraw publicznych i ważnych kwestii społecznych, których podstawowym warunkiem jest spokój społeczny[32].

Na potrzeby pracy została przyjęta definicja opracowana przez Biuro Bezpieczeństwa Narodowego rozszerzona o poglądy B. Jagusiaka według, którego zapewnienie wspomnianego spokoju społecznego możliwe jest poprzez zapewnienie bezpieczeństwa informacji, które związane jest z procesami społeczno-gospodarczymi zachodzącymi wewnątrz państw.

Zapewnienie odpowiednio wysokiego poziomu bezpieczeństwa stanowi jeden z podstawowych problemów państwa, organizacji i obywatela. Gwarantem zapew-

---

[28] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydawnictwo AON, Warszawa 2008, s. 169.

[29] K. Stańczyk, *Geopolityczne aspekty bezpieczeństwa*, Wydawnictwo Akademickie AMW, Gdynia, 2019, s.128.

[30] J. Stańczyk, *Kres „zimnej wojny". Bezpieczeństwo europejskie w procesie zmiany międzynarodowego układu sił (na przełomie lat osiemdziesiątych. i dziewięćdziesiątych XX w.)*, Wydawnictwo Adam Marszałek, Toruń 2004.

[31] https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (data dostępu 26.05.2021).

[32] B. Jagusiak, *Bezpieczeństwo socjalne współczesnego państwa*, Wydawnictwo Difin, Warszawa 2015, s. 14-16.

nienia takiego poziomu jest podejmowanie działań mających na celu ochronę przed zagrożeniami[33]. Tego typu działania stanowią jedno z podstawowych zadań państwa, a ich realizacja odbywa się na zasadach, które określone są zgodnie z Konstytucją RP[34]. W art. 5. Konstytucji RP mowa jest o tym, że 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. Zapewnienie wysokiego poziomu bezpieczeństwa określonego w konstytucji stanowi wyzwanie dla każdego państwa. Świadomość sytuacyjna może przyczynić się do poprawy tego poziomu. Stosowanie się do zasad trójpoziomowego modelu M.R. Endsley może usprawnić proces zarządzania kryzysowego oraz poprawić poziom bezpieczeństwa państwa i obywateli poprzez postrzeganie, zrozumienie i prognozowanie zagrożeń oraz możliwości ich materializacji w postaci ryzyka. Istotną rolę w zapewnieniu pożądanego poziomu bezpieczeństwa odgrywa prognozowanie, które ma na celu analizę zjawisk z wykorzystaniem metody analogii, które zachodziły w przeszłości i dzieją się w teraźniejszości w celu uniknięcia tego typu sytuacji kryzysowych w przyszłości. Taka analiza zdarzeń pozwala na prognozowanie wydarzeń, które mogą mieć miejsce w przyszłości. Zbieranie danych o zagrożeniach w dłuższym horyzoncie czasowym (tzw. danych historycznych) może w znacznym stopniu przyczynić się do poprawy bezpieczeństwa w całym państwie (jak i dla innych podmiotów) poprzez wyprzedzanie przyszłych wydarzeń. Warto podkreślić, że zasoby informacyjne współcześnie stanowią jeden z najważniejszych składników struktury zasobów organizacji (różnych poziomów)[35]. Podstawową zatem kategorią wymagającą analizy jest bezpieczeństwo informacji.

Istota bezpieczeństwa informacji związana jest z informacją jako kategorią, która wywodzi się z łacińskiego *informatio* i oznacza przedstawienie, obraz, kształtowanie. Mówiąc najprościej, informacja to dane, którym przypisane zostało jakieś znaczenie[36]. Według P. Potejko bezpieczeństwo informacyjne to zbiór działań, a także metody i procedury podejmowane przez uprawnione przedmioty, których ce-

[33] K. Szwarc, P. Zaskórski, *Ciągłość działania systemów zapewniania bezpieczeństwa*, w: , B. Jagusiak (red.) Współczesne wyzwania bezpieczeństwa Polski, WAT, Warszawa 2015. s. 49.
[34] KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ z dnia 2 kwietnia 1997 r.
[35] J. Barney, *Firm resources and sustained competitive advantage*, "Journal of Management" 1991, nr 2, s. 112.
[36] M. Staruch, praca inż. pt. „*Analiza porównawcza wybranych maszyn wirtualnych*" napisana pod kierunkiem, dr inż. R. Hoffmana, WAT, Warszawa, 2014 s. 15.

lem jest zapewnienie integralności dla przetworzonych i gromadzonych zasobów, a także zabezpieczenie ich przed nieautoryzowanym (nieuprawnionym) dostępem[37]. K. Liderman uważa, że bezpieczeństwo informacyjne to uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji[38]. Według J. Czekaj zdefiniowanie pojęcia bezpieczeństwa informacji jest problematyczne ze względu na rozwój technologii, a do właściwego sformułowania definicji niezbędne jest powiązanie z atrybutami bezpieczeństwa[39]. R.Y. Wang i D.M. Strong zdefiniowali 179 atrybutów bezpieczeństwa informacji, a pośród nich dominują takie, jak[40]:

- poufność,
- integralność,
- dostępność,
- autentyczność,
- rozliczalność,
- niezawodność,
- niezaprzeczalność.

Na potrzeby tej pracy przyjęta została przedstawiona powyżej definicja autorstwa K. Lidermana niemniej jednak precyzyjne sformułowanie definicji wymaga zidentyfikowania atrybutów bezpieczeństwa, co zostanie rozszerzone o ujęcie R.Y. Wanga i D.M. Stronga[41].

Można zatem przyjąć, że bezpieczeństwo należy postrzegać w kontekście wszystkich przedsięwzięć zmierzających do przeciwdziałania i niwelowania skutków zaistniałych sytuacji kryzysowych[42]. Poprzez odpowiednie rozpoznanie elementów wchodzących w skład zarządzania kryzysowego i radzenia sobie w sytuacjach kryzysowych, a także sformułowanie odpowiednich wymagań i atrybutów bezpieczeństwa, możliwe jest rozpoznawanie zagrożeń i skuteczna ocena ryzyka potencjalnego zakłócenia funkcjonowania państwa oraz jednostki. Dlatego też istota zapewnienia bezpieczeństwa każdemu podmiotowi powinna opierać się na wdrożeniu skutecznych rozwiązań, które umożliwią przygotowanie się na sytuacje kryzysowe i zagro-

[37] P. Potejko, *Bezpieczeństwo informacyjne,* Wydawnictwo Bezpieczeństwo państwa, Warszawa 2009, s. 194.
[38] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo PWN, Warszawa 2012, s.22.
[39] J. Czekaj, *Podstawy zarządzania informacją*, Wydawnictwo Uniwersytet Ekonomiczny w Krakowie, 2012*, s. 126-129.*
[40] R.Y. Wang, *Journal of Management Information Systems,* 1996, Vol. 12, No. 4, s. 5-33.
[41] Tamże s. 5-33.
[42] M. Nadarzewski, *Procesy i zjawiska zachodzące w bezpieczeństwie Polski*, w: A. Tyburska (red.) *Ochrona infrastruktury krytycznej*, WSPol, Szczytno, 2010, s. 57.

żenia. W tym celu niezbędne jest poznanie istoty sytuacji kryzysowej oraz zagrożeń poprzedzających ją.

1.3. Sytuacja kryzysowa

W celu zdefiniowania sytuacji kryzysowej warto na samym początku przybliżyć pojęcie kryzysu, które wywodzi się z języka greckiego *κρίσις krisis* i interpretowany jest jako dokonywanie wyboru, zmaganie się z jakimś problem pod presją czasu[43].

R. Wróblewski uważa, że kryzys to kulminacja konfliktów związana z różnymi dziedzinami życia społecznego, które są nieuniknione i wszechobecne. Ponadto stwierdza, że kryzys poprzez rozwój wydarzeń może stanowić zagrożenie dla całego państwa, a jego szybkie postępowanie wymusza na władzach podjęcie radykalnych, nadzwyczajnych środków[44]. C. Sapriel określa kryzys jako „wydarzenie, objawienie, zarzut lub zbiór okoliczności, które zagrażają integralności, reputacji lub przetrwaniu jednostki lub organizacji”[45]. P. Shrivastava określa sytuację kryzysową jako „sytuację będącą konsekwencją wykorzystania podatności systemu, powodującą osłabienie takich cech jak: stabilność, sterowalność, efektywność, a tym samym zagraża zdolności przetrwania i rozwoju systemu”[46]. Ustawa z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym definiuje sytuację kryzysową jako incydent, który w sposób negatywny wpływa na poziom bezpieczeństwa wśród ludzi oraz ich mienia, a także środowiska przez co wywołuje znaczące ograniczenia w funkcjonowaniu organów administracji publicznej. Może też wynikać z braku odpowiednich sił i środków[47]. Definicja zawarta w Ustawie z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym zostanie przyjęta na potrzeby tej rozprawy, ponieważ w sposób precyzyjny określa sytuację kryzysową oraz skutki, jakie może wywołać. Immanentnymi cechami kryzysu są niepewność lub ryzyko, a o sukcesie zarządzania kryzysowego decyduje wiele czynników, wśród których informacja i komunikacja odgrywają znaczącą rolę.

1.4. Zarządzanie kryzysowe

Według *Słownika terminów z zakresu bezpieczeństwa narodowego* zarządzanie w sytuacjach kryzysowych należy rozumieć jako reakcję na zbliżający się lub

---

[43] H. G. Liddell, R. Scott, H. S. Jones, *A Greek–English Lexicon*, “Oxford University Press”, Wielka Brytania, 1940.
[44] R. Wróblewski, *Wprowadzenie do strategii wojskowej*, Wydawnictwo AON, Warszawa, 1998, s.10.
[45] C. Sapriel *Effective crisis management: tools and best practice for the new millennium*, “Journal of Communication Management”, 2003,vol. 7, No.4 , s.348.
[46] P. Shrivastava, *Crisis theory / practice: towards a sustainable future*, “Industrial & Environmental Crisis Quarterly”, USA, w: Sage Publications, 1993, Vol 7 no. 1, s. 25.
[47] Ustawa z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r., Nr 89).

trwający kryzys i próbę wyeliminowania jego wpływu na cykl zdarzeń i działań, począwszy od zapobiegania kryzysowi i planowania antykryzysowego wraz z reagowaniem na codzienne zdarzenia do czasu odbudowy terenów, które uległy zniszczeniu (przygotowanie, reagowanie, odbudowa)[48].

J. Konieczny definiuje zarządzanie w sytuacjach kryzysowych jako „systematyczne i metodyczne przedsięwzięcia zmierzające do zapobieżenia lub zredukowania wpływu kryzysu na zasoby i wartości społeczne za pomocą środków kierowania i kontroli oraz koordynacji”[49]. System Zarządzania Kryzysowego w Polsce ma wieloszczeblową strukturę i składa się z następujących komponentów[50]:

- organy zarządzania kryzysowego,
- organy opiniodawczo-doradcze właściwe w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego,

System Zarządzania Kryzysowego funkcjonuje w czterech fazach: zapobieganie, przygotowanie, reagowanie, odbudowa[51], gdzie:

- Zapobieganie – obniżenie poziomu ryzyka wystąpienia zagrożenia poprzez zmniejszanie prawdopodobieństwa wystąpienia zagrożenia lub sytuacji kryzysowej oraz minimalizowanie skutków zaistniałej sytuacji.
- Przygotowanie – wdrożenie działań planistycznych na wszystkich szczeblach administracyjnych oraz wstępne sondowanie na temat sposobu reagowania na występujące zagrożenia lub sytuacje kryzysowe. W tej fazie możliwy jest wpływ na przebieg zagrożenia i ograniczenie lub eliminacja jego negatywnych skutków. Ponadto faza ta obejmuje także działania mające na celu zwiększenie niezbędnych zasobów, sił i środków niezbędnych do efektywnego reagowania, zarządzania, organizowania i prowadzenia szkoleń i ćwiczeń w odpowiedzi na potencjalne zagrożenia.
- Reagowanie – działania mające na celu udzielenie pomocy poszkodowanym, zatrzymanie rozwoju występujących zagrożeń oraz ograniczenie strat i skutków sytuacji kryzysowej.

---

[48] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski*, Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydawnictwo AON, Warszawa 2008, s. 172.

[49] J. Konieczny, *Zarządzanie w sytuacjach kryzysowych, wypadkach i katastrofach*, Wydawnictwo Poznań-Warszawa GARMOND Oficyna Wydawnicza, 2001, s. 9.

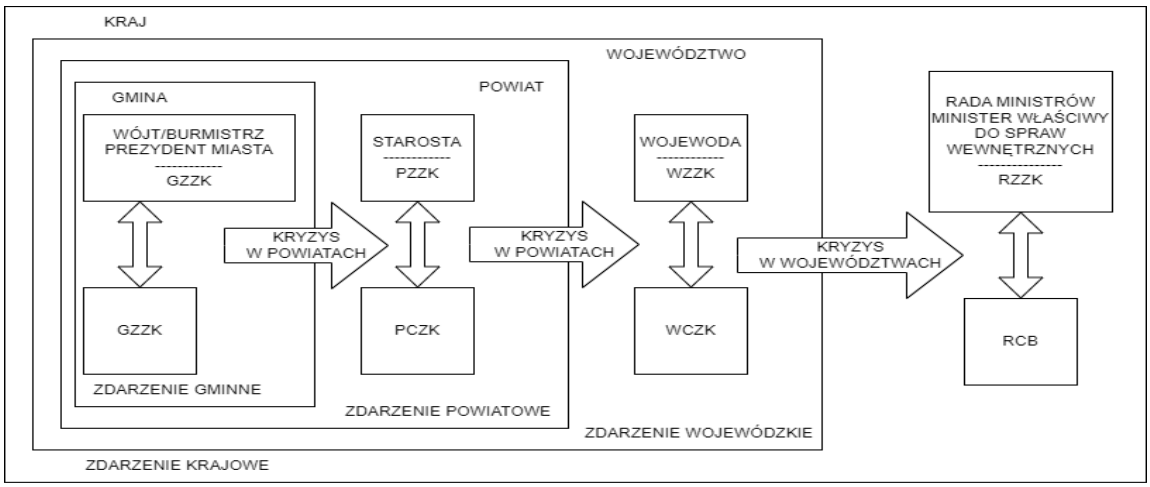
[50] https://www.gov.pl/web/rcb/obieg-informacji-i-rola-rcb-w-systemie-zarzadzania-kryzysowego (data dostępu 29.01.2023).

[51] W. Skomry, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wydawnictwo: Presscom, Wrocław 2010, s. 27–64.

- Odbudowa – realizacja zadań naprawczych związanych z przywróceniem zdolności operacyjnej i odbudową zapasów służb ratowniczych oraz przywróceniem kluczowej dla funkcjonowania danego obszaru infrastruktury energetycznej, paliwowej, telekomunikacyjnej (informacyjnej/teleinformatycznej), transportowej oraz funkcjonowania innych niezbędnych usług, (np. wodociągowych).

Zarządzanie kryzysowe to proces zapewnienia skutecznego działania wybranego podmiotu (np. państwa) w warunkach zagrożeń i kryzysów z uwzględnieniem analizy ryzyka. Istnieje bowiem wysokie ryzyko utraty ciągłości działania lub skutecznego informowania ludności. Niezbędne jest zatem podjęcie stosownych kroków mających na celu doskonalenie aktualnych rozwiązań oraz wdrożenie alternatywnych sposobów zapewniających ciągłość działania w zarządzaniu kryzysowym oraz w procesie informowania ludności. W sytuacjach kryzysowych (klęski żywiołowe, zdarzenia spowodowane przez człowieka, akty terroryzmu itp.) kluczową rolę odgrywa natychmiastowy dostęp do informacji, dzięki której możliwe jest szybkie określenie możliwości działania i skuteczne reagowanie na zaistniałą sytuację. Analizowanie danych historycznych dotyczących podobnych zdarzeń o charakterze kryzysowym oraz przeprowadzanie ćwiczeń na ich podstawie może przyczynić się do przygotowania przyszłych działań (w tym wzrostu świadomości sytuacyjnej) i umożliwienia rozszerzenia bazy informacyjnej dla kolejnego etapu planowania. Wdrożenie wspólnej platformy operacyjnej (systemu) łączącej dane krytyczne (również historyczne) z różnych systemów informacyjnych może przyczynić się do poprawy świadomości sytuacyjnej na temat zagrożeń, a także może pozytywnie wpłynąć na sposób niwelowania skutków zaistniałej sytuacji kryzysowej. Tego typu platforma powinna być dostępna w codziennych operacjach, a także w sytuacjach kryzysowych, zapewniając ciągłą gotowość do użycia na wypadek wystąpienia zagrożeń. W sytuacji kryzysowej kluczową rolę odgrywa skuteczna wymiana informacji pomiędzy organami administracji rządowej podporządkowanej Radzie Ministrów. Instytucje te odpowiadają za zarządzanie kryzysowe, dzięki któremu można skuteczniej zwalczać zagrożenia i eliminować skutki w momencie ich wystąpienia. Zgodnie z art. 11 ust. 2 pkt. 8 ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku w przypadku wystąpienia zagrożenia na szczeblu krajowym Rządowe Centrum Bezpieczeństwa pełni kluczową rolę w prawidłowej wymianie informacji pomiędzy Radą Ministrów, a ministrem odpowie-

dzialnym za kierowanie administracją rządową, wojewodą, starostą oz wójtem odgrywa Rządowe Centrum Bezpieczeństwa (RCB) (rys. 1.5)[52].



Rysunek 1.5. Model organizacji powiadamiania i reagowania kryzysowego

Źródło: opracowanie własne na podstawie ZPE (Zintegrowana platforma edukacyjna - https://zpe.gov.pl/a/kiedy-mamy-do-czynienia-z-sytuacja-kryzysowa/DeIMpPvSK)

Zgodnie z ww. ustawą RCB jest odpowiedzialne za[53]:

- utrzymanie całodobowo numerów telefonów i adresów e-mailowych służb dyżurnych,
- obsługę Rady Ministrów.

W polskim Systemie Zarządzania Kryzysowego można wyróżnić poziomy administracyjne, organy zarządzania kryzysowego, organy opiniodawczo-doradcze, oraz organy wykonawcze (tab. 1.1).

Tabela 1.1. Poziomy systemu zarządzania kryzysowego

SYSTEM ZARZĄDZANIA KRYZYSOWEGO			
Poziom administracyjny	Organ zarządzania kryzysowego	Organ opiniodawczo – doradczy	Organ wykonawczy
Krajowy	Rada Ministrów, Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa
Resortowy	Minister kierujący Działem administracji rządowej, Kierownik organu Centralnego	Zespół Zarządzania Kryzysowego (ministerstwa, urzędu centralnego)	Centrum Zarządzania Kryzysowego (ministerstwa urzędu centralnego)
Wojewódzki	Wojewoda	Wojewódzki Zespół Zarządzania Kryzysowego	Wojewódzkie Centrum Zarządzania Kryzysowego
Powiatowy	Starosta powiatu	Powiatowy Zespół Zarządzania Kryzysowego	Powiatowe Centrum Zarządzania Kryzysowego
Gminny	Wójt, Burmistrz, Prezydent miasta	Gminny Zespół Zarządzania Kryzysowego	(nie ma obowiązku utworzenia) gminne (miejskie) centra zarządzania kryzysowego

Źródło opracowanie własne na podstawie Bezpieczna https://bezpieczna.um.warszawa.pl/zarzadzanie-kryzysowe)

[52] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590).
[53] Tamże.

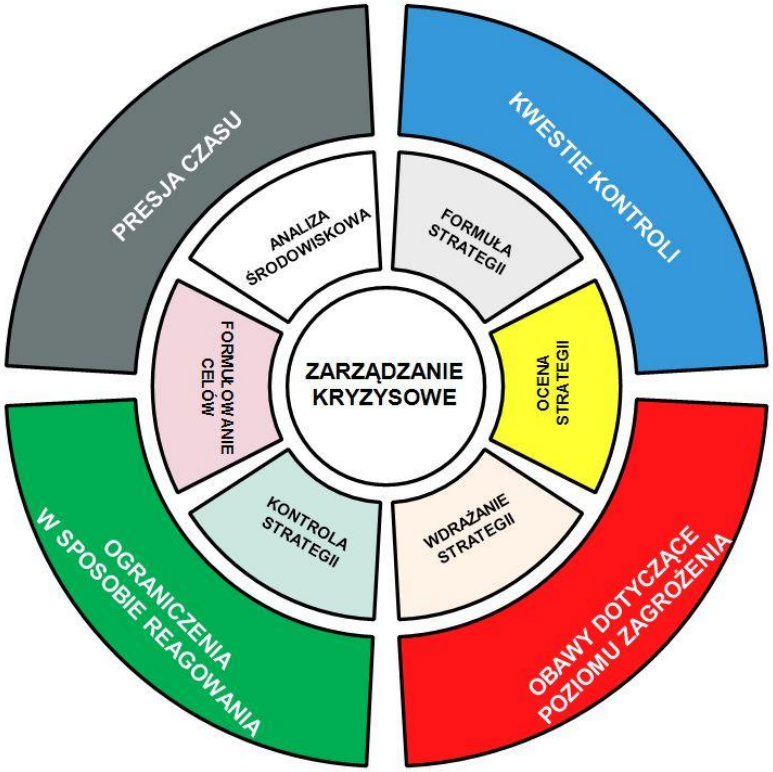
Siły i środki wykorzystywane w zarządzaniu kryzysowym planowane są na wszystkich poziomach administracji rządowej i samorządowej. Struktura zarządzania kryzysowego została zaprojektowana tak, aby zapewnić ciągłość działania, efektywność i zdolność reagowania na nowe sytuacje. Polski system zarządzania kryzysowego jest wielopoziomowy i składa się z następujących komponentów:

- organy zarządzania kryzysowego,
- organy opiniodawczo-doradcze właściwe do inicjowania i koordynowania działań z zakresu zarządzania kryzysowego,
- Centra zarządzania kryzysowego z całodobową gotowością do podjęcia działań.

Wszechobecność sytuacji kryzysowych wymaga opracowania powszechnie akceptowanego modelu zarządzania kryzysowego, który zapewnia różnym podmiotom „ramy" do rozwiązania sytuacji kryzysowej. Pomimo iż istnieją modele, które badają zarządzanie kryzysowe nie zawsze zawierają one konkretne podstawy teoretyczne.[54]. Złożoność skutecznego zarządzania kryzysowego wiąże się z faktem, że pomimo przygotowania się na wiele scenariuszy kryzysowych są lub będą sytuacje, których nie możemy kontrolować lub które są trudne do kontrolowania. Sytuacje kryzysowe mogą pojawić się w dowolnym momencie. Przygotowanie się na wypadek ich wystąpienia jest jednym z kluczowych, jeśli nie najważniejszym krokiem w fazie zapobiegania. Skuteczne zarządzanie kryzysowe zależy od trafnego planowania, które może okazać się i tak niewystarczające do uniknięcia kryzysu. Liczne incydenty pokazują, że stan przygotowania państwa i innych podmiotów na niektóre wydarzenia jest niewystarczający. Istnieje wiele czynników, które specjaliści ds. zarządzania kryzysowego muszą uwzględnić, aby zwalczyć kryzys. Uporządkowanie wszystkich niezbędnych czynników oraz przekształcenie ich w powszechnie akceptowany model stanowi wyzwanie dla praktyków i naukowców, co nie oznacza, że jest to niemożliwe do wykonania. Przykładem takiego modelu w poprawie świadomości sytuacyjnej oraz całego procesu zarządzania kryzysowego może być model zaprezentowany przez J.J. Burnett'a. Autor identyfikuje zarówno zadania, jak i czynniki, które mogą negatywnie wpłynąć na skuteczne zarządzanie kryzysowe. (rys.1.6).

---

[54] L.A. Grunig, J.E Grunig, D.M. Dozier, *Excellent public relations and effective organizations: A study of communication management in three countries*, "Lawrence Erlbaum Associates", New York, 2002, s.18.



Rysunek 1.6. Model zarządzania kryzysowego

Źródło opracowanie własne na podstawie. J. J. Burnett, A strategic approach to managing crises, Public Relations Review, 1998, Vol. 24, No 4, s.475-488S

W zaproponowanym przez J. Burnetta modelu przedstawione są cztery grupy czynników, które „hamują" zarządzanie kryzysowe: [55]

- presja czasu,
- kwestie kontroli,
- obawy dotyczące poziomu zagrożenia,
- ograniczenia w sposobie reagowania.

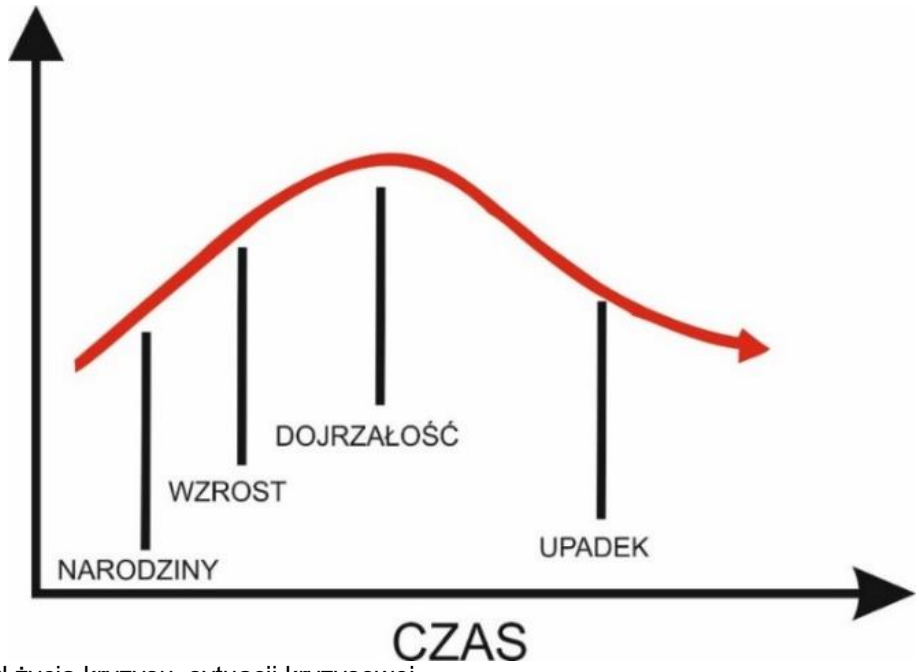
Czynniki znajdujące się na zewnętrznym pierścieniu modelu, zakłócają zdolność organizacji do koncentracji na strategicznym zarządzaniu sytuacją kryzysową. Zaprezentowany model można odnieść do całej struktury zarządzania kryzysowego nie tylko w przypadku firm, ale i całego społeczeństwa. Zgodnie z tym modelem, dopiero po uwzględnieniu tych czterech czynników można rozpatrywać proces strategicznego zarządzania sytuacją kryzysową. J.J. Burnett podzielił sześciostopniowe wewnętrzne koło modelu na trzy kategorie: identyfikację, konfrontację, rekonfigura-

[55] J. J. Burnett, *A strategic approach to managing crises,* "Public Relations Review", 1998, Vol. 24, No 4, s.475-488.

cję, przy czym: etap identyfikacji związany jest z formułowaniem celów i analizą środowiskową, której zadaniem jest przygotowanie do kryzysu, etap konfrontacji obejmuje formułowanie strategii i jej ocenę, etap rekonfiguracji obejmuje wdrożenie strategii i kontrolę strategiczną oraz dostosowanie się do sytuacji kryzysowej[56].

Według J.J. Burnett'a w czasie kryzysu zwiększa się trudność w osiąganiu dobrych wyników zarówno przez państwo jak i organizacje. Model ilustruje, wykorzystanie zadań wchodzących w skład wewnętrznego kręgu, co daje organizacji, a także zespołom zarządzania kryzysowego, możliwość kontrolowania i skutecznego zarządzania sytuacją kryzysową[57].

A. González-Herrero i C.B. Pratt prezentują sekwencyjny przebieg kryzysu przez cztery fazy: narodziny, wzrost, dojrzałość i upadek (rys. 1.7). Model ten dzieli się na możliwe do zidentyfikowania etapy i ilustruje, w jaki sposób kryzys zmienia się w czasie. Zaprezentowany model pokazuje kryzys jako nie kończący się cykl, którego skutki są odczuwalne po jego zakończeniu[58].

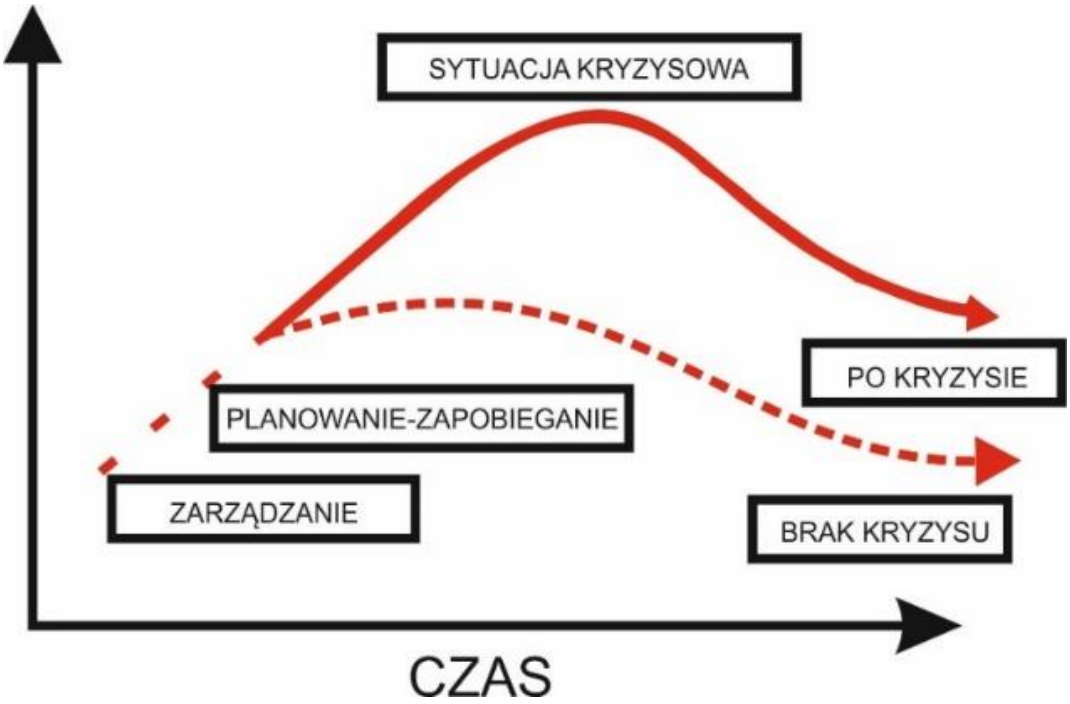


Rysunek 1.7. Cykl życia kryzysu, sytuacji kryzysowej

Źródło opracowanie własne na podstawie: A. González-Herrero, C.B. Pratt, An integrated symmetrical model for crisis-communication man-agement, "Journal of Public Relations Research", 1996, Vol.8, No.2., s. 79-105.

[56] Tamże s. 475-488.
[57] Tamże s. 475-488.
[58] A. González-Herrero, C.B. Pratt, *An integrated symmetrical model for crisis-communication management*, "Journal of Public Relations Research", 1996, Vol.8, No.2., s. 79-105.

W celu zilustrowania wpływu odpowiedniego zarządzania na rozwój sytuacji kryzysowej model ten został rozszerzony przez A. González-Herrero i C.B. Pratt. Autorzy uważają, że odpowiednie zarządzanie przed wystąpieniem kryzysu może przyczynić się do zniwelowania jego skutków lub zwalczenia go zanim zostanie rozpoczęty (rys. 1.8). W rozszerzonej wersji modelu wprowadzona została faza zarządzania przed wystąpieniem kryzysu, co okazało się dobrym rozwiązaniem, ponieważ etap ten sprzyja skutecznemu zarządzaniu kryzysem[59].



Rysunek 1.8. Wpływ zarządzania na rozwój sytuacji kryzysowej

Źródło opracowanie własne na podstawie: A. González-Herrero, C.B. Pratt, An integrated symmetrical model for crisis-communication man-agement, "Journal of Public Relations Research", 1996, Vol.8, No.2., s. 79-105.

Literatura przedmiotu związana z problematyką zarządzania kryzysowego bogata jest w modele, które mogą być stosowane, aby zminimalizować skutki kryzysu. A. González-Herrero i C.B. Pratt przedstawiają modele zarządzania kryzysowego jako sposób na identyfikowanie potencjalnych problemów i zapobiegania im**,** zanim staną się zagrożeniem. Dlatego członkowie ZZK powinni skoncentrować się na przygotowaniu do sytuacji kryzysowych zanim te wystąpią. Pomimo iż niemożliwe jest całkowite zażegnanie tego typu sytuacji to, przy odpowiednim przygotowaniu można ograniczyć ich skutki. Stosowanie procedur i wskazówek zaprezentowanych w róż-

[59] Tamże s. 79-105.

nych modelach może poprawić sytuację danego podmiotu w czasie kryzysu jak i bezpośrednio po jego wystąpieniu.

T. Szczurek uważa, że pomimo silnej presji czasu i zmieniających się warunków, zarządzanie kryzysowe musi być skuteczne. Wymaganie to realizowane jest na drodze podejmowania konkretnych decyzji, do których T. Szczurek zalicza[60]:

- dokonanie oceny aktualnej sytuacji,
- przygotowanie wstępnego planu działania oraz opracowanie planów wariantowych na wypadek pojawienia się nieprzewidzianych sytuacji,
- wyznaczenie ról i zadań oraz pełnomocnictwa do działania zespołom zarządzania kryzysowego,
- przygotowanie organów wykonawczych (RCB, CZK, WCZK, PCZK),
- przygotowanie oraz wdrożenie systemu komunikowania się umożliwiającego przepływ informacji i skuteczne rozsyłanie informacji do wszystkich osób zaangażowanych w akcję ratunkową,
- stałą ocenę podejmowanych działań i skuteczne wdrożenie działań zapobiegawczych.

Z rozważań związanych z zarządzaniem kryzysowym można wywnioskować, że system zarządzania kryzysowego pełni centralną rolę w reagowaniu na zagrożenia, którego głównym zadaniem jest działanie w sytuacji kryzysowej. System ten uruchamiany jest, gdy inne środki okazują się niewystarczające lub nieskuteczne. Mając to na uwadze, zarządzanie kryzysowe musi koncentrować się na charakterze i głównych źródłach zagrożeń życia i mienia stron dotkniętych kryzysem. W przypadku innych problemów (pośrednio związanych lub niezwiązanych z sytuacją kryzysową) ich rozwiązanie powinny podejmować instytucje i jednostki organizacyjne administracji publicznej. Dlatego SZK powinien być stale doskonalony nie tylko w zakresie regulacji prawnych, ale również podnoszenia kompetencji i wiedzy członków zespołu zarządzania kryzysowego. Współczesne zagrożenia implikują zatem potrzebę wykorzystywania odpowiednich metod i technik pozwalających na skuteczne przygotowanie społeczeństwa na istniejące i przyszłe zagrożenia. Zasadne wydaje się zatem podjęcie niezbędnych działań zmierzających do podniesienia poziomu świadomości sytuacyjnej ludności na temat zagrożeń poprzez odpowiednie ćwiczenia i treningi. Właściwy poziom świadomości sytuacyjnej w zakresie zagrożeń, ich charakteru oraz

[60] T. Szczurek, *Problemy podejmowania decyzji w sytuacjach kryzysowych,* Wydawnictwo Świadczenie na rzecz obrony realizowane w sytuacjach kryzysowych AON, Warszawa 2006, s 59.

skutków może przyczynić się do efektywnego działania całego Systemu Zarządzania Kryzysowego. Poprzez kreowanie odpowiednich nawyków i postaw budowana oraz wzmacniana jest świadomość sytuacyjna społeczeństwa na temat nowych oraz istniejących zagrożeń, co może przyczynić się do poprawy społecznej świadomości każdego obywatela, a także może usprawnić współpracę ze służbami ratowniczymi i ograniczyć ryzyko powstania chaosu, paniki i pojawiających się strat[61].

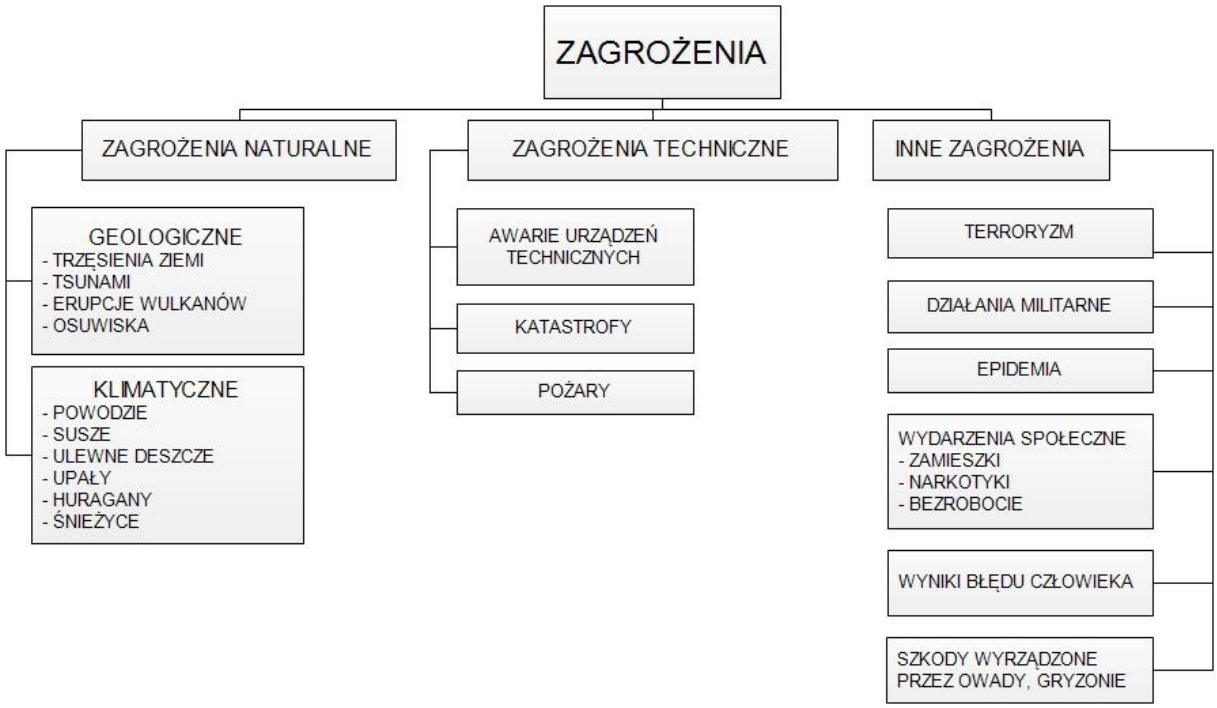
Istotne w tym zakresie jest to, aby podejmowane działania nie miały charakteru destrukcyjnego oraz by nie potęgowały takich odczuć, jak lęk czy strach. Prezentowana wiedza powinna zatem wyznaczać zarówno sposób postępowania jak i kształtować odpowiednie umiejętności, nawyki, które ułatwią radzenie sobie różnych podmiotów w przypadku zagrożeń. W celu uskutecznienia tego typu działań niezbędne jest ograniczenie stanów zamętu, paniki, strachu czy irracjonalnego zachowania. Niezbędne zatem jest zapoznanie społeczeństwa z rodzajami i klasyfikacją zagrożeń oraz możliwymi sposobami przygotowania się na wypadek ich wystąpienia.

1.5. Zagrożenia a ryzyko

Istnieje wiele definicji zagrożenia, które bywa definiowane jako wiążąca sytuacja oraz prawdopodobieństwo wystąpienia stanu niepożądanego lub niebezpiecznego[62]. S. Korycki uważa, zagrożenie za „pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, a z drugiej strony jako czynniki obiektywne powodujące stan niepewności i obaw”[63]. Według *Słownika języka polskiego* zagrożenie to „sytuacja bądź stan, w którym danej osobie coś zagraża lub czuje się ona zagrożona lub stwarza sytuację zagrożenia”[64]. Ponadto uważa się, że „zagrożenie to zdarzenie spowodowane czynnikami losowymi lub nielosowymi, które wywiera negatywny wpływ na funkcjonowanie systemu i/lub jego otoczenie”[65] (rys. 1.9). Na potrzeby rozprawy przyjęto powyższą definicję podaną przez K. Ficonia. Należy jednak rozszerzyć ją o rodzaje zagrożeń (rys. 1.9)[66], który przedstawia rodzaje zagrożeń z wyróżnieniem trzech podstawowych kategorii takich, jak katastrofy naturalne, zagrożenia technicz-

[61] https://ctif.org/news/panic-and-human-behavior-fire-emergency-situations (data dostępu 10.11.2022).
[62] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski*, Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydawnictwo AON, Warszawa 2008, s. 172.
[63] S. Korycki, *System bezpieczeństwa Polski*, Wydawnictwo AON, Warszawa, 1994, s.54.
[64] https://sjp.pwn.pl/sjp/zagro%C5%BCenie;2542384 (data dostępu 24.04.2021).
[65] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Wydawnictwo BEL Studio, Warszawa, 2007, s.76.
[66] https://epodreczniki.pl/a/zagrozenia-w-czasie-pokoju/D1EuS4od1 (data dostępu 24.04.2021).

ne oraz inne zagrożenia. Zagrożenia te mogą wywołać poważne szkody dla ludzi i mienia, niemniej jednak odpowiednia świadomość sytuacyjna na ich temat może im zapobiec lub częściowo zniwelować skutki tych zagrożeń[67].



Rysunek 1.9. Przykładowy podział zagrożeń ze względu na źródło oraz sposób powstania

Źródło: opracowanie własne na podstawie: R. Grocki, Vademecum zagrożeń, Wydawnictwo Bellona, Warszawa 2003, s. 9-10.

Zagrożenia nierozłącznie wiążą się z kategorią ryzyka. Zasadne jest zatem oszacowanie poziomu ryzyka dla zagrożenia spowodowanego przez siły natury, awarie techniczne lub działalność człowieka. Pomocnym rozwiązaniem jest ewaluacja ryzyka, która bazuje m.in. na dwuwymiarowej matrycy ryzyka, gdzie jeden wymiar odnosi się do wartości prawdopodobieństwa wystąpienia zagrożenia, a drugi do skutków jego materializacji. Każde zaistniałe zagrożenie wiąże się z oszacowanym poziomem ryzyka, dlatego należy odpowiednio reagować na jego skutki[68].

W nawiązaniu do poziomu bezpieczeństwa można stwierdzić, że bezpieczeństwo jest niejako dopełnieniem wyznaczonego poziomu ryzyka. Do zapewnienia odpowiedniego poziomu bezpieczeństwa niezbędne jest zatem systematyczne monitorowanie zagrożeń i ocena możliwości ich materializacji, co zmierza do zapewnienia świadomości sytuacyjnej na oczekiwanym poziomie poprzez obserwację zachodzą-

[67] Tamże.
[68] R. Grocki, Vademecum zagrożeń, Wydawnictwo Bellona, Warszawa 2003, s. 9-10.

cych zmian oraz ich rejestrowanie przy wykorzystaniu tradycyjnych rozwiązań oraz współczesnych technologii IT/ICT.

W celu zniwelowania ryzyka utraty bezpieczeństwa, niezbędne jest, aby korzystać ze współczesnych technologii IT/ICT z uwagi na ich niezawodność i możliwość zastępowania alternatywnymi rozwiązaniami w momencie awarii jednej z nich, co w procesie wymiany informacji może ograniczyć ryzyko utraty informacyjnej ciągłości działania[69]. Przewidywanie przyszłych katastrof i zagrożeń, analiza ich skutków oraz kompleksowa ocena ryzyka stają się ważnym wyzwaniem w skutecznym zarządzaniu kryzysowym. Dlatego też konieczne jest stałe gromadzenie danych i przetwarzanie informacji o zagrożeniach we wszystkich fazach zarządzania kryzysowego. Niezbędne jest zatem stworzenie i utrzymywanie odpowiedniej infrastruktury i oprogramowania dla przechowywania danych i monitorowania zagrożeń. Oprócz tradycyjnych rozwiązań takich, jak np. mapy zagrożeń, skutecznym rozwiązaniem mogą okazać się współczesne technologie IT/ICT, np. chmury obliczeniowe, które eliminować mogą wykluczenie informacyjne różnych podmiotów oraz mogą stanowić bazę obserwacji aktualnego stanu zagrożeń. Zagrożenia można skutecznie monitorować bowiem dzięki dostępności usług informacyjnych w cyberprzestrzeni. Niemniej jednak należy zdawać sobie sprawę z faktu, że w momencie wystąpienia zagrożenia może nastąpić utrata informacyjnej ciągłości działania. Niezbędne zatem jest tworzenie rozwiązań alternatywnych, w tym rozwiązań tradycyjnych, które mogą wydawać się przestarzałe, ale w niektórych sytuacjach kryzysowych mogą okazać się niezastąpione. Dlatego ocena prawdopodobieństwa wystąpienia zagrożenia i jego skutków wymaga wielopłaszczyznowych działań, takich jak uwzględnienie ryzyka awarii jednej z technologii oraz tego, jak ta awaria wpływa na działanie całego Systemu Zarządzania Kryzysowego.

Zagrożenia często pojawiają się w sposób nieprzewidywalny, dlatego nie zawsze można względnie trafnie oszacować prawdopodobieństwo ich wystąpienia. Niemniej jednak na każde zagrożenie można w mniejszym lub większym stopniu się przygotować, np. symulując zagrożenia lub analizując dane historyczne.

---

[69] P. Zaskórski, W. Zaskórski, J. Woźniak, *Świadomość sytuacyjna, a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, Wydawnictwo CeDeWu, Warszawa, 2021, s. 33-52.

1.6. Współczesne technologie teleinformatyczne

Technologie informacyjno-komunikacyjne (ICT) stanowią rozszerzenie technologii informatycznych (IT) odnoszących się do wszystkich technologii komunikacyjnych, w tym Internetu, sieci bezprzewodowych, telefonów komórkowych, komputerów, oprogramowania, oprogramowania pośredniczącego, wideokonferencji, sieci społecznościowych oraz inne aplikacje i usługi multimedialne umożliwiające użytkownikom: dostęp, pobieranie, przechowywanie, przesyłanie i operowanie informacjami w formie cyfrowej[70]. Współczesne technologie IT/ICT mają istotny wpływ na codzienne życie, a wręcz znaczna część społeczeństwa nie wyobraża sobie życia bez nich. Technologie te mogą stanowić jeden z najważniejszych komponentów kreowania świadomości sytuacyjnej ludności. Wykorzystanie odpowiednich narzędzi daje możliwość monitorowania i analizy oraz wieloaspektowej oceny stanu wielu obiektów i sytuacji w czasie rzeczywistym. Można zatem założyć, że narzędzia te silnie wpływają na poziom postrzegania zagrożeń i możliwość przeciwdziałania im, a także poprzez odpowiednią formę przekazu treści – rozumienia sytuacji i prognozowanie jej rozwoju. Współczesne technologie IT/ICT zrewolucjonizowały świat i codzienne życie, tworząc skuteczne narzędzia teleinformatyczne, obejmujące zarówno oprogramowanie komputerowe, jak i sprzęt (skanery, drukarki, drony, telefony, smartfony itp.). Współczesne technologie IT/ICT sprawiły, że komputery stały się szybsze, bardziej mobilne i trwalsze. Pomimo iż wpłynęło to na jakość życia, wprowadziło również nowe zagrożenia. Nieodpowiednie posługiwanie się technologiami IT/ICT może wywołać zagrożenie w świecie rzeczywistym jak i w cyberprzestrzeni, która definiowana jest jako ”cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[71]. Rozwój współczesnych technologii IT/ICT przyczynił się do opracowania i wdrożenia zupełnie nowych urządzeń takich, jak: smartfony, smartwatche, tablety, urządzenia asystenta głosowego, drony itp. Współczesne technologie IT/ICT otwierają nowe możliwości w zakresie bezpieczeństwa, mobilności i łączności. Technologie te rozszerzyły proces wymiany informacji poprzez szeroką gamę urządzeń i narzędzi do komunikowania się. Wykorzystanie przedmiotowych technologii zapewnia szybszy sposób działania i przekazywania informacji niż ich

[70] http://aims.fao.org/information-and-communication-technologies-ict (data dostępu: 01.03.2021).
[71] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (data dostępu 23.01.2023).

tradycyjne odpowiedniki takie jak np. telefon stacjonarny, mapy w wersji papierowej, listy itp. Przykładowo wykorzystanie smartfona zamiast telefonu stacjonarnego może znacznie przyśpieszyć kontakt ze służbami ratowniczymi w przypadku znalezienia się w sytuacji kryzysowej ze względu na sposób komunikacji, jak i prostotę formy przekazywania informacji.

Wykorzystanie współczesnych technologii IT/ICT zwykle wymaga współdziałania na platformie Internetu w celu rozszerzenia ich funkcjonalności. Wyjątek stanowią połączenia telefonii komórkowej oraz wysyłanie wiadomości tekstowych typu SMS. Rozszerzenie funkcji współczesnych technologii IT/ICT o dostęp do Internetu umożliwia synchronizację przedmiotów codziennego użytku np. za pośrednictwem sieci Wi-Fi. Omówiona koncepcja podłączenia urządzeń do sieci internetowej funkcjonuje pod nazwę Internet Rzeczy (IoT – *Intenret of Things*). Taka synchronizacja sprawia, że zwykłe funkcje urządzeń (w tym np. sensorów monitorujących sytuacje zagrożenia) są dostępne zdalnie i zautomatyzowane za pośrednictwem danych udostępnianych w sieci *World Wide Web* (WWW)[72]. Może to być ważny atrybut procesu kształtowania świadomości sytuacyjnej.

Ogólnie można stwierdzić, że zastosowanie technologii kompatybilnych z Internetem Rzeczy może przyczynić się do poprawy bezpieczeństwa w każdym systemie wspieranym przez tę technologię, która coraz częściej wykorzystywana jest do monitorowania bezpieczeństwa różnych obiektów (np. domów, miejsc pracy, miast itp.) Wraz z pojawieniem się współczesnych technologii IT/ICT, a w tym zintegrowanych systemów informatycznych zarządzania, Internetu rzeczy (IoT), Internetu wszystkiego (IoE), systemów klasy *Big-Data* itp. umożliwiających analizę i obiektywizację oceny w czasie rzeczywistym oraz planowanie zasobów organizacji podnosi sprawność informacyjno-decyzyjna organizacji i pojedynczego obywatela. Dotyczy to zarówno wykorzystania systemów klasy ERP, przetwarzanie transakcji online (OLTP), przetwarzanie informacji z wykorzystaniem wielowymiarowej bazy danych (OLAP) itp., które zmieniły sposób komunikowania się w sytuacjach kryzysowych. Tego typu rozwiązania wykorzystywane w zakresie zarządzania kryzysowego odgrywać mogą i częściowo już odgrywają coraz większą rolę w planowaniu przedsięwzięć zmierzających do przeciwdziałania zagrożeniom, niwelowaniu ich skutków oraz do informowania ludności o zagrożeniach, co może ułatwiać także wszelkiego rodzaju działania

[72] *World Wide Web - powszechnie nazywane WWW, W3 lub Sieć Web - jest połączonym systemem publicznych stron internetowych dostępnych przez Internet.*

ratownicze. Wykorzystanie nowych strategii technologicznych w zespołach zarządzania kryzysowego pozwala zaoszczędzić czas, a co za tym idzie środki finansowe, np. poprzez konsolidację serwerów lub monitorowanie zagrożeń za pomocą technologii teleinformatycznych (w tym także drony, kamery itp.). Technologie te, oprócz funkcji związanych z monitorowaniem zagrożeń znajdują też coraz częściej zastosowanie w procesie wymiany informacji między różnymi podmiotami w czasie rzeczywistym, a także w zakresie udzielania pomocy wszędzie tam, gdzie niemożliwe jest dotarcie przez człowieka. Zasadne zatem wydaje się wdrożenie współczesnych technologii w celu zapewnienia informacyjnej ciągłości działania w momencie wystąpienia sytuacji kryzysowej. Utrata tej ciągłości może wywołać negatywne skutki zarówno w procesach decyzyjnych, jak i w procesie reagowania kryzysowego. Współczesne technologie są dobrą alternatywą dla tradycyjnych rozwiązań i mogą stanowić ich skuteczne uzupełnienie. Wykorzystanie chmury obliczeniowej może przyczynić się do poprawy poziomu bezpieczeństwa oraz zwiększa możliwość zapewnienia informacyjnej ciągłości działania, a przez to do kreowania właściwego poziomu świadomości sytuacyjnej zarówno zarządzających, jak i odbiorców informacji, czyli nawet pojedynczych użytkowników (obywateli). Do zapewnienia ciągłości działania informacji zalecane jest stosowanie modeli biznesowych przetwarzania danych bieżących (OLTP) oraz zasobów analitycznych (historycznych, statystycznych, OLAP w postaci uporządkowanej, tabelarycznej) w różnych formatach (np. *Big Data*, systemy gromadzące bardzo duże objętości danych wyrażane w petabajtach i zetabajatach z możliwością ich wieloaspektowej analizy), ze szczególnym uwzględnieniem modeli odkrywania i generowania wiedzy (DM), dzięki którym mogą być wspierane procesy kreowania świadomości sytuacyjnej z zachowaniem informacyjnej ciągłości działania. Połączenie wymienionych wyżej technologii z konsolidacją wspólnych zasobów informacyjnych (serwerów) może zwiększyć skuteczność i elastyczność funkcjonowania systemów zarządzania kryzysowego poprzez istotne usprawnienie procesu przepływu informacji[73].

Wykorzystanie konsolidacji serwerów baz danych i integracja ich z nowoczesnymi technologiami IT/ICT, takimi jak platformy wspierające kształtowanie świadomości

[73] P. Zaskórski, W. Zaskórski, J. Woźniak, *Świadomość sytuacyjna, a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, Wydawnictwo CeDeWu, Warszawa 2021, s. 240-241.

sytuacyjnej, a w tym *small data*[74], przetwarzanie w chmurze oraz systemy informacji geoprzestrzennej może przyczynić się do zwiększenia nie tylko świadomości sytuacyjnej poprzez proces wspierania postrzegania i rozumienia zagrożeń, ale także może wpłynąć na efektywniejsze zarządzanie w sytuacjach kryzysowych. Wraz z ewolucją nowoczesnych technologii IT/ICT pojawiają się nowe zagrożenia, nowe kategorie ryzyka oraz sytuacje kryzysowe, które mogą zakłócić działanie całej infrastruktury krytycznej. Technologie te mogą odgrywać kluczową rolę w całym zarządzaniu kryzysowym jak i w procesie informowania ludności o zagrożeniach. Niemniej jednak istotne jest przygotowanie alternatywnych rozwiązań, w tym także tych tradycyjnych – na wypadek, gdyby któraś z technologii uległa awarii bądź trwałemu uszkodzeniu na skutek wystąpienia zagrożenia.

1.7. Podsumowanie rozdziału pierwszego

Rozdział ten został poświęcony identyfikacji dziedziny problemu, a w tym ustaleniu oraz interpretacji podstawowych pojęć związanych z celem, zakresem i treścią rozprawy oraz podejmowanych w niej badań. Skuteczne zarządzanie kryzysowe warunkowane jest bowiem odpowiednim poziomem świadomości sytuacyjnej, a w tym spójnym, wiarygodnym i kompleksowym monitorowaniem oraz identyfikowaniem zagrożeń i zapewnieniem oczekiwanego poziomu bezpieczeństwa. Właściwe przygotowanie społeczeństwa, jak i każdego obywatela, wymaga wdrożenia adekwatnych do zagrożeń procedur działania, którą będą zmierzały do kształtowania świadomości sytuacyjnej ludności i Zespołów Zarządzania Kryzysowego. W rozdziale przedstawiono zatem kategorię bezpieczeństwa i ryzyka, które nierozłącznie wiążą się z zagrożeniami.

Zagrożenia mogą pojawić się w sposób nieoczekiwany i są trudno przewidywalne w swoich skutkach. W przypadku zagrożeń naturalnych, technicznych i innych niezbędne jest odpowiednie przygotowanie się na ich wystąpienie. Każde zagrożenie charakteryzuje się tym, że w momencie jego materializacji kluczową rolę odgrywa czas i zwykle jak najszybsze przeciwdziałanie. Niemniej jednak sama wiedza na temat zagrożeń jest niewystarczająca. Niezbędne jest zatem wdrożenie odpowiednich zasad działania, narzędzi i platform wspierających świadomość sytuacyjną w celu ograniczenia lub złagodzenia skutków zagrożeń. Stąd znaczącą rolę przypisuje się narzędziom teleinformatycznym, które umożliwiają zarówno szybkie przetwarzania

[74] *Small data* to dane, które są wystarczająco „małe”, aby zrozumieć je przez człowieka. Są to dane w objętości i formacie, które czynią je dostępnymi, informacyjnymi i praktycznymi.

dużych zasobów danych, jak i szybkie informowanie poszczególnych interesariuszy Systemu Zarządzania Kryzysowego (szczególnie decydentów).

Warto jednak podkreślić, że nie można ograniczyć się wyłącznie do jednej technologii, dlatego też konieczne jest stałe udoskonalanie istniejących rozwiązań – zarówno tradycyjnych, jak i nowatorskich. Każda wykorzystywana w tym celu technologia powinna być zrozumiała dla osób z niej korzystających. Z punktu widzenia Zespołów Zarządzania Kryzysowego jak i pojedynczego obywatela istotna jest ich użyteczność i funkcjonalność w konkretnych sytuacjach. W przypadku ZZK wartością użytkową są wykorzystywane narzędzia informatyczne, nad którymi kontrolę sprawuje administrator systemu, który odpowiada za – de facto - informacyjną ciągłość działania Systemu Zarządzania Kryzysowego, która determinuje organizacyjno-funkcjonalną ciągłość działania całego systemu. Dla członków ZZK ważne jest, aby interfejs użytkownika systemu i wszystkie jego elementy zawierały proste procedury (ergonomia), zrozumiałe dla każdej osoby, która z niego korzysta.

W przypadku obywateli kluczowe znaczenie odgrywa informacja o zagrożeniu, którą powinni otrzymywać zgodnie z przyjętym scenariuszem w najskuteczniejszy sposób i aby informacja dotarła w formie komunikatywnej za pomocą dostępnego środka. Tradycyjne środki komunikowania się, które jak wielokrotnie wspomniano uzupełniają współczesne technologie IT/ICT i powinny pełnić redundantne funkcje, jeśli któraś z nich zawiedzie. Tradycyjne środki komunikowania się to alternatywa dla współczesnych rozwiązań, które umożliwiają przekazywanie informacji osobom preferującym klasyczne rozwiązania. Technologie te mogą ze sobą współpracować i być rozwijane jednocześnie ze względu na silne powiązania między nimi.

W rozdziale pierwszym omówiono możliwości wykorzystania tradycyjnych i współczesnych technologii IT/ICT, w odniesieniu do funkcjonowania Zespołów Zarządzania Kryzysowego oraz obywateli. Dlatego też obszar badawczy został sprofilowany dla tych dwóch komponentów, ponieważ z punktu widzenia obywateli, jak i ZZK kreowanie świadomości na temat zagrożeń powinno prowadzić do zapobiegania im, zmniejszania skutków lub całkowitego ich wyeliminowania.

ROZDZIAŁ II
METODYCZNE PODSTAWY BADAŃ

2.1. Cel badań

Głównym celem rozprawy jest identyfikacja luk (niekompletności i niespójności) w realizowanych współcześnie procesach informowania ludności w kontekście zapewniania pożądanego poziomu świadomości sytuacyjnej w sytuacjach kryzysowych. Realizacja tego celu będzie silnie połączona z analizą możliwości implementacji współczesnych technologii IT/ICT oraz zakresu wykorzystania tych technologii w celu podniesienia efektywności, niezawodności, elastyczności oraz skuteczności przepływów informacyjnych i zwiększania stanu świadomości sytuacyjnej ludności w sytuacjach kryzysowych. Przedstawione rozwiązania poddane zostaną ocenie z uwzględnieniem kryteriów użyteczności, funkcjonalności i skuteczności wykorzystania współczesnych technologii IT/ICT w procesie informowania ludności w celu osiągnięcia pożądanego poziomu świadomości sytuacyjnej.

W rozprawie w celu głównym wyodrębniono aspekt poznawczy i utylitarny. Celem poznawczym jest identyfikacja luk w istniejącym systemie informowania ludności o zagrożeniach w powiązaniu z oceną ryzyka obniżania poziomu świadomości sytuacyjnej oraz możliwości jego ograniczania dzięki wykorzystaniu środowiska współczesnych technologii informacyjnych (platform IT).

Celem utylitarnym jest opracowanie i ocena koncepcji zapewniania pożądanego poziomu świadomości sytuacyjnej w Systemie Zarządzania Kryzysowego z wykorzystaniem środowiska współczesnych technologii IT/ICT informatycznych wraz z oceną ich użyteczności w zarządzaniu kryzysowym.

2.2. Przedmiot badań i problem badawczy

Przedmiotem rozprawy jest kształtowanie świadomości sytuacyjnej Zespołów Zarządzania Kryzysowego oraz ludności z wykorzystaniem wybranych platform IT/ICT. Traktując świadomość sytuacyjną jako jeden z ważniejszych elementów w procesie informowania ludności o zagrożeniach zamierza się wskazać braki w aktualnie wykorzystywanych tradycyjnych i współczesnych technologiach stosowanych w zakresie zarządzania kryzysowego i kreowania świadomości sytuacyjnej. Na bazie wyników tej analizy opracowana zostanie koncepcja wykorzystania tradycyjnych i nowoczesnych technologii ze szczególnym uwzględnieniem procesu kreowania świadomości sytuacyjnej obywateli i ZZK.

Zapewnienie świadomości sytuacyjnej może wiązać się bezpośrednio z:

- Korzystaniem z prostych i funkcjonalnych narzędzi wpływających na zarządzanie kryzysowe.
- Prostym i zrozumiałym przekazem informacji.
- Stosowaniem właściwych rozwiązań tradycyjnych i współczesnych technologii IT/ICT w procesie informowania ludności na bazie zdywersyfikowanych źródeł danych o zagrożeniach.
- Zrozumieniem wpływu działań i zdarzeń na otoczenie.
- Procesem podejmowania decyzji w sytuacjach kryzysowych.
- Szybkim i skutecznym reakcją na klęski żywiołowe lub katastrofy.
- Zapobieganiem zagrożeniom lub niwelowaniem wpływu ich skutków na otoczenie.
- Gromadzeniem informacji na temat zagrożeń oraz ich weryfikacją.

Istotne wydaje się zatem dokonanie analizy aktualnie wykorzystywanych tradycyjnych i współczesnych technologii IT/ICT w celu zapewnienia świadomości sytuacyjnej ZZK i ludności na temat zagrożeń oraz w celu zwiększenia poczucia bezpieczeństwa poprzez odpowiednie przygotowanie społeczeństwa na materializację tych zagrożeń.

Główny problem badawczy koncentruje się wokół odpowiedzi na pytanie:

1. Jak zdefiniować poziom świadomości sytuacyjnej na potrzeby systemu informowania ludności w sytuacjach kryzysowych i jak zapewnić oczekiwany (pożądany) jego poziom?

Dla tak określonego głównego problemu badawczego sformułowane zostało pięć **szczegółowych problemów badawczych**:

1) W czym wyraża się istota i jakie mogą być systemowe determinanty świadomości sytuacyjnej ludności o zagrożeniach i sytuacjach kryzysowych?
2) Jaki jest aktualny poziom i jakie są determinanty świadomości sytuacyjnej (w tym wykorzystywane dotychczas technologie ICT) ludności o zagrożeniach i sytuacjach kryzysowych w istniejącym systemie zarządzania kryzysowego RP?
3) Czy i jak współczesne technologie IT/ ICT mogą wpływać na skuteczności wydajność procesu informowania ludności i zwiększenia jej świadomości sytuacyjnej?

4) Czy i dlaczego należy wprowadzać współczesne technologie w celu zwiększenia świadomości sytuacyjnej ludności i jak skutecznie zwiększyć tę świadomość poprzez wprowadzenie współczesnych technologii IT/ICT w kontekście eliminacji lub dublowania tradycyjnych środków przekazu?
5) Jaki może być poziom implementacyjności proponowanej koncepcji oraz użyteczności i funkcjonalności przewidywanych rozwiązań technologicznych?

Odpowiedź na powyższe pytania pozwoli na zbadanie możliwości wzrostu poziomu świadomości sytuacyjnej obywateli oraz zespołów zarządzania kryzysowego, co może przyczynić się do skuteczniejszego przygotowania się na zagrożenia oraz udoskonalenia procesu zwalczania skutków zaistniałych sytuacji kryzysowych. Rozwiązanie wyspecyfikowanych wyżej problemów badawczych jest ściśle zorientowane na realizację założonych celów rozprawy. Problemy badawcze dotyczą kreowania i zapewniania pożądanego poziomu świadomości sytuacyjnej ludności oraz zespołów zarządzania kryzysowego. Są to problemy ważne z naukowego i praktycznego punktu widzenia, ponieważ wysoki poziom świadomości sytuacyjnej może ograniczać (nawet minimalizować) ryzyko wystąpienia zagrożenia lub wyeliminować jego skutki. Rozważane problemy są aktualne i ważne, a także bardzo mocno osadzone w rzeczywistości.

2.3. Hipotezy badawcze

Hipoteza główna jest następująca: ***System informowania ludności posiada istotne luki, co ujemnie wpływa na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów, które można eliminować poprzez wykorzystanie nowoczesnych rozwiązań teleinformatycznych (IT/ICT*).**

Hipoteza główna została zdekomponowana na pięć hipotez szczegółowych:

1) ***Świadomość sytuacyjna ludności o zagrożeniach i ryzyku utraty bezpieczeństwa w warunkach materializacji zagrożeń i kryzysów kształtuje się na niskim poziomie.***
2) ***W funkcjonującym systemie informowania ludności o zagrożeniach poziom świadomości sytuacyjnej ludności nie jest determinowany złożonością tego systemu.***
3) ***Skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej a sprawnością systemu informowania w warunkach zagrożeń i kryzysów.***

4) ***Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów.***
5) ***Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja.***

W celu weryfikacji sformułowanych hipotez niezbędne jest wykorzystanie zróżnicowanych metod i narzędzi badawczych.

2.4. Metody i narzędzia badawcze oraz źródła danych

W realizacji procesu badawczego i uzyskania wyników prezentowanych w rozprawie zastosowano metody badawcze teoretyczne i empiryczne. Sposób użycia poszczególnych metod badawczych uszczegółowiono w tabeli 2.1.

Tabela 2.1. Wykorzystane metody badawcze teoretyczne i empiryczne

MERYTORYCZNY OBSZAR BADAŃ	METODY BADAWCZE
Świadomość sytuacyjna w aktualnym systemie informowania ludności w sytuacjach kryzysowych. Analiza aktualnych rozwiązań oraz ocena poziomu świadomości sytuacyjnej ludności.	Kwerenda literatury przedmiotu
Ryzyko utraty oraz poziomy świadomości sytuacyjnej.	studium przypadku
Aktualny poziom świadomości sytuacyjnej ludności.	Badania ankietowe CAWI

Źródło: opracowanie własne.

W pierwszej kolejności dokonano przeglądu literatury krajowej i zagranicznej z zakresu zarządzania kryzysowego i kształtowania świadomości sytuacyjnej. Analiza literatury oraz aktualnych rozwiązań była podstawą doprecyzowania założeń badawczych i prac nad koncepcją, która może przyczynić się do udoskonalenia istniejących narzędzi i metod działania w zakresie kształtowania świadomości sytuacyjnej obywateli oraz osób funkcyjnych w SZK. Za pomocą wywiadów eksperckich i analizy studiów przypadków zweryfikowane zostaną przyjęte hipotezy oraz oceniona zostanie trafność, aktualność i rozwojowość docelowych rozwiązań związanych z wykorzystaniem współczesnych technologii IT/ICT w zapewnieniu świadomości sytuacyjnej. Metoda ilościowa zostanie wykorzystana w statystycznym opracowaniu wyników badań w celu oszacowania i oceny poziomu świadomości sytuacyjnej członków ZZK i ludności na tle wyników identyfikacji istniejących luk.

W części teoretycznej pracy rozważania mają charakter identyfikacji zjawisk i sytuacji związanych z zagrożeniami, ryzykiem i bezpieczeństwem oraz dotyczą zarządzania kryzysowego i istoty świadomości sytuacyjnej. Głównymi źródłami są za-

równo polska, jak i zagraniczna literatura przedmiotu z zakresu bezpieczeństwa, zarządzania kryzysowego, świadomości sytuacyjnej, tradycyjnych i współczesnych technologii IT/ICT, a także raporty i opracowania publikowane w prasie i na portalach internetowych. W części empirycznej praca bazuje na badaniach ankietowych skierowanych do obywateli i członków ZZK oraz na wywiadzie eksperckim. W pracy wyszczególniono zakres przedm*iot*owy, podmiotowy, przestrzenny i czasowy:

a) Zakres przedmiotowy

Zakres przedm*iot*owy jest ściśle związany z szeroko pojętym bezpieczeństwem oraz sytuacjami kryzysowymi i zagrożeniami, które bezpośrednio wpływają na funkcjonowanie państwa, a w tym także negatywnie wpływają na działalność firm i pojedynczych obywateli. Przedmiotem badania jest:

- oszacowanie poziomu świadomości sytuacyjnej członków Zespołów Zarządzania Kryzysowego,
- ocena przydatności tradycyjnych i współczesnych technologii IT/ICT w zarządzaniu kryzysowym,
- złożoność, wydajność i determinanty systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych.

Badanie skierowane jest do członków Zespołów Zarządzania Kryzysowego oraz do obywateli o zróżnicowanych przedziałach wiekowych. W badaniu ankietowym brane były pod uwagę takie cechy jak : płeć, wiek, wykształcenie, miejsce zamieszkania. Przeprowadzone badanie ankietowe dostarczają między innymi informacji o: rzeczywistym poziomie świadomości sytuacyjnej obywateli oraz członków ZZK; preferencjach obywateli związanych z technikami komunikowania się w czasie zagrożeń i kryzysów; możliwych do wykorzystania współczesnych technologiach IT/ICT niezbędnych do usprawniania Systemu Zarządzania Kryzysowego; wydajności i złożoności obecnie funkcjonującego Systemu Zarządzania Kryzysowego.

b) Zakres podmiotowy

Badania ograniczone są do dwóch typów podmiotów – obywateli oraz członków ZZK ze wszystkich województw. Badanie zostało przeprowadzone na losowej, reprezentatywnej próbie obywateli ZZK oraz członków wszystkich województw i obejmowało 112 osób w wieku 18 lat i więcej, o różnym wykształceniu i mieszkających w różnych regionach kraju.

c) Zakres przestrzenny

Obszarem badań jest terytorium państwa polskiego, a pytania ankietowe skierowane są do obywateli a w tym w szczególności do osób funkcyjnych w SZK RP (członków ZZK) w we wszystkich województwach.

d) Zakres czasowy

Badania i opracowanie wyników obejmuje lata 2019-2023, czyli czas tworzenia rozprawy doktorskiej.

Rozwój współczesnych technologii spowodował, że powszechnie korzysta się z urządzeń elektronicznych (urządzenia mobilne, drony, kamery itp.). Stąd upatruje się we współczesnych technologiach IT/ICT możliwości kreowania świadomości sytuacyjnej poprzez szersze wykorzystanie innych rozwiązań i narzędzi w sytuacjach kryzysowych. Zakłada się więc, że ważny staje się problem:

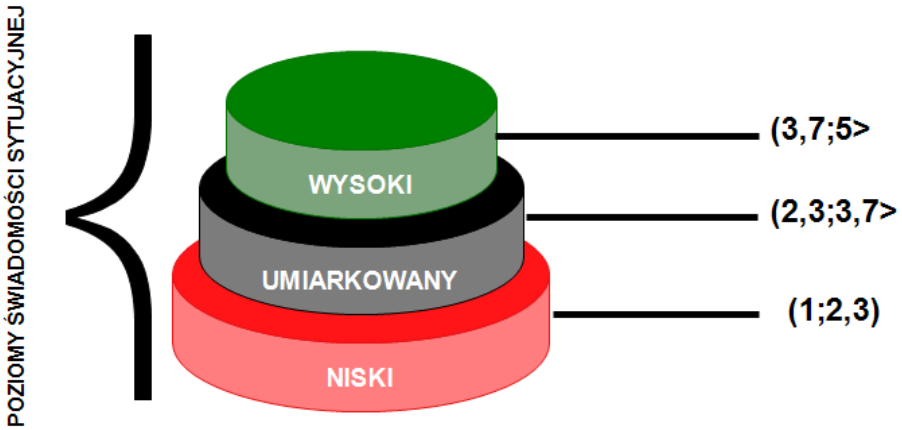
W jaki sposób można wykorzystać współczesne technologie IT/ICT w procesie informowania ludności, aby zwiększyć ich świadomość sytuacyjną?

W dalszej części pracy przyjęto zatem, że rozwiązanie tego problemu może istotnie usprawnić proces funkcjonowania poszczególnych ogniw SZK zarówno w skali lokalnej, jak i ogólnokrajowej. W tym celu przeprowadzono badania ankietowe, których celem było zbadania poziomu świadomości sytuacyjnej obywateli oraz członków ZZK. Ponadto oceniono złożoność i wydajność funkcjonującego w Polsce Systemu Zarządzania Kryzysowego SZK. Pytania cząstkowe oceniane były w 5-stopniowej skali. Na potrzeby badania wyróżnione zostały 3 poziomy świadomości sytuacyjnej, ponieważ skoncentrowano się na wartościach najniższych, umiarkowanych i najwyższych zmiennych. Nowe poziomy są innymi niż te w 5-stopniowej skali. Zakresy wartości dla nowych zmiennych są takie same jak dla cząstkowych (1-5), ale nie powoduje to konieczności ścisłego przestrzegania 5-stopniowej skali. Do wyszczególnienia 3 poziomów dla nowych zmiennych wykorzystano analizę skupień metodą k-średnich, ponieważ wcześniej przyjęto 3 poziomy. Wprowadzenie 5 -stopniowej skali prowadziłoby do nadmiernej „fragmentaryzacji" analizy i zatarcia istotnych różnic pomiędzy poziomami. Ocena czynników w 5–stopniowej skali tworzących nową zmienną (określony wskaźnik kompozytowy np. PŚSL – Poziom Świadomości Sytuacyjnej Ludności)[75], a skala interpretacji wartości nowej zmiennej dają

[75] Wyprowadzenie wskaźników kompozytowych przedstawiono w dalszych rozdziałach.

inną perspektywę, ponieważ czynniki szczegółowe dotyczyły znaczenia danego zjawiska bądź poziomu jego spełnienia przez respondenta, natomiast nowa zmienna odwołuje się do złożoności zjawiska jako determinanty opisywanej przez nową zmienną.

Zatem na potrzeby badań opracowano trójpoziomowy schemat świadomości sytuacyjnej ludności na temat zagrożeń (rys. 2.1). Jako pierwowzór utworzonego schematu posłużył model zaprezentowany przez J. Coopera, przy czym model ten zmodyfikowano i przyjęto tylko 3 poziomy świadomości sytuacyjnej określające poziom przygotowania do postrzegania zagrożeń jako: wysoki (zadowalający), umiarkowany (akceptowalny) i niski (niedostateczny).



Rysunek 2.1. 3-poziomowy schemat świadomości sytuacyjnej na temat zagrożeń

Źródło: opracowanie własne na postawie modelu świadomości sytuacyjnej J. Coopera

W dalszej części rozdziału scharakteryzowano wykorzystywane ilościowe metody badawcze i określono, z którymi hipotezami i z którymi pytaniami ankietowymi te metody się wiążą i tak hipotezę:

[H.1] Świadomość sytuacyjna ludności o zagrożeniach i ryzyku utraty bezpieczeństwa w warunkach materializacji zagrożeń i kryzysów kształtuje się na niskim poziomie zostanie zweryfikowana za pomocą pytania nr 1 – ankieta skierowana do obywateli (zał. 2), a do opracowania wyników posłużyła:

- **Analiza czynnikowa** (metodą głównych składowych PCA, ponadto opracowano wskaźnik kompozytowy PŚSL – poziom świadomości sytuacyjnej ludności, oszacowano wartości średniej dla próby badawczej).
- **Analiza skupień** (metodą *k*-średnich dla znormalizowanej zmiennej PŚSL, ponadto wyznaczono 3 skupienia dla respondentów/obywateli: o niskim, śred-

nim i wysokim poziomie świadomości sytuacyjnej w warunkach zagrożeń i kryzysów).

[H.2] W funkcjonującym systemie informowania ludności o zagrożeniach poziom świadomości sytuacyjnej ludności nie jest determinowany złożonością tego systemu zostanie zweryfikowana za pomocą pytania nr 2 – ankieta skierowana do obywateli (zał. 2) oraz pytania nr 1 – ankieta skierowana do ZZK (zał. 3), a do opracowania wyników posłużyła:

- **Analiza czynnikowa** (metodą głównych składowych PCA, rotacja Varimax, ponadto opracowano wskaźnik kompozytowy ZSIL – złożoność systemu informowania ludności, oszacowano wartości średniej dla próby badawczej). Analizie podlegały oceny obywateli nt. złożoności systemu informowania ludności.
- **Analiza skupień** (metodą k-średnich dla znormalizowanej zmiennej ZSIL – Złożoność Systemu Informowania Ludności, ponadto wyznaczono 3 skupienia: o niskim, średnim i wysokim poziomie złożoności systemu informowania ludności. Analizie podlegają oceny obywateli nt. złożoności systemu informowania ludności.
- **Korelacja rho-Spearmana** (pomiędzy zmiennymi ZSIL oraz PŚSL)
- **Analiza rozkładów odpowiedzi członków ZZK** (nt. złożoności i rodzaju działań podejmowanych w ramach informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń).

[H.3] Skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej, a sprawnością systemu informowania w warunkach zagrożeń i kryzysów zostanie zweryfikowana za pomocą pytania nr 3 – ankieta skierowana do obywateli (zał.2) oraz pytania nr 2 - ankieta skierowana do ZZK (zał. 3) a do opracowania wyników posłużyła:

- **Analiza czynnikowa** (metodą głównych składowych PCA, rotacja Varimax, ponadto opracowano wskaźnik kompozytowy WSIL – Wydajność Systemu Informowania Ludności, oszacowanie wartości średniej dla próby badawczej). Analizie podlegają oceny obywateli nt. wydajności systemu informowania ludności.

- **Analiza skupień** (metodą *k*-średnich dla znormalizowanej zmiennej WSIL, ponadto wyznaczono 3 skupienia: o niskim, średnim i wysokim poziomie wydajności systemu informowania ludności). Analizie podlegają oceny obywateli nt. złożoności systemu informowania ludności
- **Korelacja rho-Spearmana** (pomiędzy zmiennymi WSIL oraz PŚSL)
- **Analiza rozkładów odpowiedzi członków ZZK** (nt. wydajności działań podejmowanych w ramach informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń).

[H.4] Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów zostanie zweryfikowana za pomocą pytań 4-6 – ankieta skierowana do obywateli (zał.2) oraz pytań 3-5 – ankieta skierowana do ZZK (zał. 3), a do opracowania wyników posłużyła:

- **Analiza rozkładów odpowiedzi obywateli i członków ZZK** (nt. atrybutów ICT oraz użyteczności tradycyjnych środków komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów)
- **Korelacja rho-Spearmana** (pomiędzy średnim użytecznością ICT w informowaniu ludności oraz PŚSL).
- **Korelacja rho-Spearmana** (pomiędzy średnią użytecznością tradycyjnych środków komunikowania w informowaniu ludności oraz PŚSL).Obie wartości korelacji zostały ze sobą porównane.

[H.5] Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja zostanie zweryfikowana za pomocą pytania nr 6 – ankieta skierowana do obywateli (zał.2) oraz pytań 6-7 – ankieta skierowana do ZZK (zał. 3), a do opracowania wyników posłużyła:

- **Analiza rozkładów odpowiedzi członków ZZK** (nt. potencjalnego wpływu zastosowania ICT w systemach informowania ludności na poziom świadomości sytuacyjnej ludności).
- **Analiza czynnikowa** (metodą głównych składowych PCA, rotacja Varimax, ponadto opracowano wskaźnik kompozytowy ZICT – złożoność zastosowania

ICT w informowaniu ludności, oszacowanie wartości średniej dla próby badawczej). Analizie podlegają oceny obywateli nt. złożoności wykorzystania ICT przez administrację.

- **Analiza skupień** (metodą *k*-średnich dla znormalizowanej zmiennej ZICT, ponadto wyznaczano 3 skupienia: o niskim, średnim i wysokim poziomie złożoności wykorzystania ICT. Analizie podlegają oceny obywateli nt. złożoności wykorzystania ICT przez administrację.
- **Korelacja rho-Spearmana** (pomiędzy zmiennymi ZICT oraz PŚSL).

Wskaźniki kompozytowe, opracowano przy wykorzystaniu metody analizy czynnikowej PCA i wyrażono je wzorami:

- PŚSL – poziom świadomości sytuacyjnej ludności, oszacowanie wartości średniej dla próby badawczej, który przyjmuje postać średniej arytmetycznej (wzór 2.1) – pyt.1 ankieta skierowana do obywateli (zał.2).

$$\text{PŚSL} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.1)$$

- ZSIL – złożoność systemu informowania ludności, oszacowanie wartości średniej dla próby badawczej) – analizie podlegają oceny obywateli nt. złożoności systemu informowania ludności, która przyjmuje postać średniej arytmetycznej (wzór 2.2) – pyt. 2 ankieta skierowana do obywateli (zał.2) oraz pyt.1 ankieta skierowana do ZZK (zał.3).

$$\text{ZSIL} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.2)$$

- WSIL – wydajność systemu informowania ludności, oszacowanie wartości średniej dla próby badawczej) – analizie podlegają oceny obywateli nt. wydajności systemu informowania ludności, który przyjmuje postać średniej arytmetycznej (wzór 2.3) – pyt. 3 ankieta skierowana do obywateli (zał.2) oraz pyt. 2 ankieta skierowana do ZZK (zał.3).

$$\text{WSIL} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.3)$$

- ZICT – złożoność procesu wykorzystania ICT w informowaniu ludności, oszacowanie wartości średniej dla próby badawczej) – analizie podlegają oceny obywateli nt. złożoności procesu wykorzystania ICT przez administrację, który przyjmuje postać średniej ważonej wyrażonej wzorem 2.4 – pyt. 6 ankieta skierowana do obywateli (zał.2) oraz pyt. 6-7 ankieta skierowana do ZZK (zał.3).

$$ZICT^{76} = \frac{W1(C4+C5+C9+C10+C11+C13+C14)}{7} + \frac{(W1(C4+C5+C9+C10+C11+C13+C14)\ )}{5} + \frac{(W3(C1+C12)}{2} \quad (2.4)$$

Podsumowując, jako metodę analizy danych w pracy wykorzystano metody ilościowe: analizę czynnikową, analizę skupień, korelację rho-Spearmana, analizę rozkładu odpowiedzi członków ZZK. Za pomocą wybranych metod można ocenić poziom świadomości sytuacyjnej obywateli i Zespołów Zarządzania Kryzysowego, a także skuteczność SZK oraz przydatność tradycyjnych i współczesnych technologii IT/ICT w informowaniu ludności o zagrożeniach. oraz w działaniach zmierzających do wyeliminowania lub częściowego złagodzenia zagrożenia.

W celu określenia potencjału wykorzystania technologii IT/ICT zastosowano też analizę SWOT-TOWS. W analizie zidentyfikowano mocne strony, słabe strony, szanse oraz zagrożenia określonych technologii IT/ICT. Ze względu na znaczenie wskazanych w analizie czynników przyjęto 5-stopniową skalę, gdzie: „1" oznacza bardzo małe znaczenie, „2" oznacza małe znaczenie, „3" oznacza średnie znaczenie „„4" oznacza duże znaczenie, a „5" oznacza bardzo duże znacz nie technologii IT/ICT.

W analizie SWOT-TOWS zrezygnowano ze zwyczajowego podejścia podkreślania najważniejszych cech technologicznych, uznając, że każda cecha odgrywa ważną rolę w efektywnym zastosowaniu technologii. Ponadto, w celu przeprowadzenia analizy SWOT-TOWS zdekomponowane zostały pytania pomocnicze:

I. SWOT:

- Czy mocna strona ……... pozwoli wykorzystać szanse?
- Czy mocna strona ……zniweluje zagrożenia?
- Czy słaba strona …… ogranicza wykorzystanie szansy?
- Czy słaba strona ……wpływa na możliwość wystąpienia zagrożenia?

II. TOWS:

- Czy szanse …… wpływają na mocne strony?
- Czy zagrożenia …… wpływają na mocne strony ?
- Czy szanse ……wpływają na słabe strony?
- Czy zagrożenia ……wpływają na słabe strony?

W tabelach (załącznik Analiza SWOT/TOWS - tabele) zaprezentowano wyniki analizy ośmiu układów macierzowych (SWOT-TOWS), określono liczbę interakcji między czynnikami oraz rangę cech z przedziału od 0 do 5. Ponadto w tabelach przyjęto wartości 1 oraz 0, gdzie jeden oznacza zależność między poszczególnymi czyn-

[76] Złożoność procesu wykorzystania ICT w informowaniu ludności.

nikami, 0 oznacza brak zależności między czynnikami. Po określeniu zależności obliczona została suma interakcji oraz suma iloczynów dla poszczególnych par czynników. Do kolumny i wiersza opisanego jako waga przypisano wagi dla każdej z cech. Sumę interakcji należy interpretować jako sumę występujących zależności, iloczyn wag i interakcji oznacza pomnożone wagi oraz interakcje. Ponadto określone zostały rangi od 1 do 5, gdzie 1 oznacza najwyższy iloczyn wag i interakcji, a 5 oznacza najniższy. Poprzez rangi określone została moc cechy.

W rozprawie w celu oceny przydatności współczesnych i tradycyjnych technologii zastosowano również metodę QFD[77]. Aktualnemu rozwiązaniu przypisane zostały wagi od 1 do 5, które następnie zostało porównane z koncepcją udoskonalenia wykorzystywanych rozwiązań. Na podstawie przypisanych zależności ● – 9, ○ – 3 oraz ▽ – 1 określono stopień zależności oraz kierunek doskonalenia. Następnie do każdej z technologii został przypisany poziom świadomości sytuacyjnej (postrzeganie, zrozumienie, prognozowanie) w celu określenia, na którym poziomie możliwe jest wykorzystanie technologii.

2.5. Podsumowanie rozdziału drugiego

W rozprawie zamierza się zbadać użyteczność i funkcjonalność tradycyjnych i współczesnych technologii IT/ICT w kształtowaniu świadomości sytuacyjnej obywateli oraz osób funkcyjnych (członków ZZK) w sytuacjach kryzysowych. W tym celu należało zbadać ich przydatność w aspekcie:

- funkcjonalno-organizacyjnym,
- technologiczno-organizacyjnym,
- informacyjnym.

Założono, że badania te mogą dostarczyć odpowiedzi na pytanie, które z obecnych rozwiązań wymagają udoskonalenia oraz które tradycyjne oraz współczesne technologie IT/ICT należy wykorzystać do kreowania wzrostu świadomości sytuacyjnej na temat zagrożeń. Na podstawie analizy obecnych rozwiązań oceniany jest poziom świadomości sytuacyjnej ZZK i obywateli w sytuacjach kryzysowych.

Sytuacje kryzysowe oraz zagrożenia będące ich następstwem lub przyczyną wymagają stałego nadzoru, monitorowania oraz przewidywania i niwelowania ich skutków. Zapewnienie odpowiedniej świadomości sytuacyjnej w systemie bezpieczeństwa państwa i jego obywateli jest wyzwaniem dla rządzących. Można tu zau-

[77] QFD – Dom jakości (House of Quality) to szeroka forma diagramu tabelarycznego, która jest szczególnie przydatna w fazie projektowania produktu.

ważyć, że jednym z głównych elementów SZK są zasoby informacyjne i dobór odpowiednich technologii umożliwiających efektywne przekazywanie informacji pomiędzy ZZK oraz służbami ratowniczymi, a także dobór niezbędnych narzędzi umożliwiających informowanie ludności o zagrożeniach i realizację sprawnego procesu informacyjno-decyzyjnego. Analizując istniejące rozwiązania, wskazuje się na niedociągnięcia i możliwe sposoby ich poprawy w sytuacjach takich jak np.:

- zagrożenia naturalne,
- zagrożenia związane z gospodarczą działalnością człowieka,
- katastrofy i awarie techniczne,
- zagrożenia terrorystyczne.

W przypadku wyżej wymienionych zagrożeń szczególnie ważne staje się zapewnienie skutecznego przepływu informacji oraz kreowanie świadomości sytuacyjnej na temat tego, co się wydarzało i jak radzić sobie z zaistniałą sytuacją. Dlatego też podjęto w pracy próbę sformułowania propozycji rozwiązań doskonalących procesy kreowania świadomości sytuacyjnej ludności w momencie wystąpienia sytuacji kryzysowej oraz w trakcie jej trwania.

Celem przeprowadzenia badań i analizy zastosowanych rozwiązań jest zwiększenie świadomości sytuacyjnej poprzez wzbogacenie narzędzi tradycyjnych i szersze wykorzystanie nowoczesnych technologii IT/ICT, które mogą przyczynić się do ograniczenia skutków zagrożeń oraz zwiększenia świadomości sytuacyjnej obywateli i członków ZZK. W tym celu zdefiniowano hipotezy badawcze, w tym główną hipotezę, że: System informowania ludności posiada istotne luki, co ujemnie wpływa na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów, które można eliminować poprzez wykorzystanie nowoczesnych rozwiązań teleinformatycznych (ICT) oraz 5 hipotez szczegółowych. Hipotezy zostały zweryfikowane na podstawie: kwerendy literatury; aktów normatywnych; analizy aktualnych rozwiązań w zakresie informowania ludności o zagrożeniach oraz analiz wynikających z ocen ankietowych badań obywateli i członków ZZK a także z wywiadów eksperckich. Obszar badań wyznaczony został poprzez badanie poziomu użyteczności tradycyjnych i współczesnych technologii w procesie kreowania świadomości sytuacyjnej na temat zagrożeń oraz w celu zmniejszenia skutków tych zagrożeń.

ROZDZIAŁ III
UWARUNKOWANIA ZAPEWNIANIA ŚWIADOMOŚCI SYTUACYJNEJ W SYTUACJACH KRYZYSOWYCH

3.1. Zagrożenia i ryzyko utraty bezpieczeństwa dla ludności

Zagrożenia są związane z odczuwalnym przez każdy podmiot poziomem bezpieczeństwa. Rodzaj i charakter zagrożeń zmieniał się wraz z rozwojem technologii i oprócz sił natury pojawiały się inne typy zagrożeń. Przykładowo wraz z rozwojem technologii teleinformatycznych mamy do czynienia z nowymi zagrożeniami. W każdym jednak przypadku zagrożenia można zdefiniować jako czynniki wpływające na poziom bezpieczeństwa i reprezentujące sytuację, w której wartości dla danej strony są trudne do osiągnięcia lub ulegają całkowitemu zniszczeniu [78]. Szczególne poczucie zagrożenia pojawia się u człowieka w momencie uświadomienia skutków materializacji bezpośredniego zagrożenia dla życia, zdrowia lub mienia.

Na skutek wystąpienia zagrożenia pojawia się potrzeba szukania informacji i rozwiązań dotyczących radzenia sobie z zaistniałą sytuacją. Tego typu podejście może wynikać z braku odpowiednich technik i narzędzi ułatwiających kształtowanie świadomości sytuacyjnej każdego podmiotu i całej populacji (ludności) i przygotowywania ich na sytuacje, które są nieprzewidywalne w swoich skutkach[79].

W momencie pojawienia się zagrożenia, istnieje konieczność wyboru określonych reguł postępowania spośród możliwych dostępnych systemów, sposobów i technologii teleinformatycznych niezbędnych w procesie kształtowania świadomości sytuacyjnej informowania ludności. Rozwój cywilizacji powoduje, że zagrożenia występują z różną częstotliwością. Jak wcześniej już wspomniano zagrożenia mogą wynikać z[80]:

- sił natury,
- działalności człowieka,
- awarii technicznych,
- zagrożeń terrorystycznych.

---

[78] W. Fehler., *Zagrożenie – kluczowa kategoria teorii bezpieczeństwa*, w: K. Jałoszyński, B. Wiśniewski, T. Wojtuszek (red.), *Współczesne postrzeganie bezpieczeństwa*, Wyższa Szkoła Administracji, BielskoBiała 2007, s. 34.

[79] J. Piwowarski, A. Zachuta, *Pojęcie bezpieczeństwa w naukach społeczno-prawnych*, Wydawnictwo Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2013, s. 6.

[80] R. Jakubczak, *Obrona narodowa w tworzeniu bezpieczeństwa III RP,* Dom Wydawniczy BELLONA, Warszawa 2003, załącznik 33 wg. K. Przeworskiego.

Niektóre zagrożenia mogą prowadzić do stanu klęski żywiołowej. W polskiej konstytucji stan ten wyróżniony jest jako osobna kategoria stanu nadzwyczajnego. Stan ten może zostać wprowadzony przez Radę Ministrów, która działa z inicjatywy własnej lub na podstawie wniosku właściwego wojewody, o czym mówi art. 5 ust. 1 ustawy o stanie klęski żywiołowej[81]. Konstytucja RP w art. 232[82] reguluje możliwości wprowadzenia stanu klęski żywiołowej w celu zapobieganiu skutkom katastrof naturalnych oraz awarii technicznych. Stan klęski żywiołowej może zostać ogłoszony na skutek wystąpienia w/w zagrożeń w celu podjęcia szczególnego działania i wymuszenia pożądanych zachowań wśród ludności oraz usuwania powstałych skutków w trybie nadzwyczajnym.

W przeciwieństwie do takich stanów jak wojenny lub wyjątkowy – stan klęski żywiołowej nie podlega kontroli parlamentarnej, co oznacza, że sejm nie może uchylić tego stanu większością głosów. Stan klęski żywiołowej wprowadzany jest na 30 dni i może być przedłużony za zgodą sejmu na czas określony. Konstytucja RP nie określa okresu, w ciągu którego można przedłużyć stan klęski żywiołowej[83].

Pojęcie klęski żywiołowej zostało po raz pierwszy użyte w dekrecie z dnia 23 kwietnia 1953 o świadczeniach mających na celu zwalczanie klęsk żywiołowych[84]. Klęska żywiołowa to zdarzenie zagrażające: życiu lub zdrowiu, bezpieczeństwu i mieniu dużej liczby osób. Taka sytuacja może spowodować poważne zakłócenia w funkcjonowaniu gospodarki kraju. Powszechnie stosowaną definicją stanu klęski żywiołowej jest definicja zatwierdzona w ustawie o stanie klęski żywiołowej z dnia 18 kwietnia 2002 r. Według ustawy klęskę żywiołową określa się jako „katastrofę naturalną lub awarię techniczną, której skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem”[85]. Z definicją klęski żywiołowej powiązany jest stan klęski żywiołowej, a w ustawie określono, w jakich przypadkach może zostać wprowadzony. Zgodnie z ustawą stan klęski żywiołowej ustanawia się w celu zapobieżenia klęskom żywiołowym lub awariom technicznym

[81] USTAWA z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej.
[82] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., (Dz. U. 1997, Nr 78, poz. 483 ze zm.).
[83] Tamże.
[84] Dekret z dnia 23 kwietnia 1953 r. o świadczeniach w celu zwalczania klęsk żywiołowych.
[85] USTAWA z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej.

oraz ograniczeniu ich skutków.[86]. Ponadto, ustawa ta definiuje klęskę naturalną, jako zdarzenie spowodowane siłami natury. Ingerencja człowieka w środowisko naturalne spowodowała, że zmiany klimatyczne stały się jeszcze bardziej widoczne, co spowodowało zanieczyszczenie, skażenia, zatrucie wody czy kwaśne deszcze. Do najniebezpieczniejszych katastrof spowodowanych przez człowieka należą katastrofy ekologiczne, które mogą przybierać różne formy i powodować zanieczyszczenie wody i powietrza. W przypadku katastrofy ekologicznej szkody mogą być nieodwracalne i doprowadzić do zagłady ludzkości, ponieważ „degradacja przyrody, jest pośrednio degradacją człowieka, a więc działaniem ograniczającym jego bezpieczeństwo”[87].

Kluczową rolę w reagowaniu na zagrożenia poprzedzające klęski żywiołowe i w przygotowaniu się na nie odgrywa System Zarządzania Kryzysowego, a w szczególności obieg informacji, jej weryfikacja oraz kształtowanie świadomości sytuacyjnej zespołów zarządzania kryzysowego i całego społeczeństwa połączone z koniecznością wypełniania poleceń służb ratowniczych i organów zarządczych. Do rozwijania świadomości sytuacyjnej niezbędna jest przede wszystkim pełna identyfikacja istniejących zagrożeń z uwzględnieniem ewaluacji ich charakterystyk, co ma istotny wpływ na poziom świadomości sytuacyjnej każdego podmiotu indywidualnego lub grupowego. Do osiągnięcia pożądanego stanu świadomości sytuacyjnej niezbędne jest podjęcie kroków zmierzających do uświadamiania obywateli o istniejących zagrożeniach przekazując im nie tylko informację o zbliżającym się zagrożeniu, ale również o miejscu jego materializacji, zakresie i czasie trwania, a także o sposobie ochrony i zachowania w momencie jego wystąpienia oraz zakresu działań, jakie należy podjąć, by zmniejszyć ich skutki. Przekazywanie tego typu wiedzy z wykorzystaniem możliwych technologii może sprzyjać zmniejszeniu szkód oraz ograniczeniu ryzyka wywołania innego zagrożenia, które może powstać równolegle na skutek przepływu nieaktualnych, często niewiarygodnych danych, w tym nawet celowej dezinformacji. Istnieje zatem potrzeba wzmacniania potencjału systemów informacyjnych (w tym teleinformatycznych) w celu podniesienia ich skuteczności w kształtowaniu świadomości sytuacyjnej.

---

[86] Tamże.
[87] K. Kołodziejczyk, *Personalny wymiar bezpieczeństwa*, „Periodyk Naukowy Akademii Polonijnej”, 2010, Nr 1, s. 99.

3.2. Identyfikacja zagrożeń

Współczesne zagrożenia dla Polski, poza typowymi zagrożeniami wywołanymi przez katastrofy naturalne, awarie techniczne oraz na skutek działalności człowieka wynikają z położenia geograficznego, stanu gospodarki i funkcjonowania w Pakcie Północnoatlantyckim oraz Unii Europejskiej, a także z polityki wewnętrznej i zagranicznej. Nie sposób wymienić i scharakteryzować wszystkie zagrożenia ze względu na fakt, że w każdej chwili mogą pojawić się nowe zagrożenie, które mogą wywołać nieprzewidziane konsekwencje. Warto jednak przygotować się na te zagrożenia, które są nam znane poprzez analizę danych historycznych prowadzenie szkoleń, symulowanie zagrożeń i wdrażanie odpowiednich procedur i działań zmierzających do zmniejszenia ryzyka ich wystąpienia.

Katastrofy naturalne

Do najczęstszych katastrof naturalnych w Polsce zalicza się pożary, susze, powodzie, wyładowania atmosferyczne i silne wiatry (tab. 3.1)[88].

Tabela 3.1. Najczęściej występujące katastrofy naturalne w Polsce wg źródeł ich wystąpienia

Powodzie	- Powodzie opadowe, - powodzie rzeczne, - powodzie od strony morza, - powodzie wywołane innymi czynnikami, - powodzie wód gruntowych, - powodzie hydrotechniczne, - powodzie wywołane na skutek działalności człowieka.
Pożary	- Wyładowania atmosferyczne, - zaniedbania, - podpalenia, - wypadki komunikacyjne.
Susze	- Atmosferyczne, - hydrologiczne, - rolnicze, - hydrogeologiczne.
Wyładowania atmosferyczne	- Wewnątrz chmurowe, - między chmurowe,
Silne wiatry	- Stałe, - sezonowe, - zmienne (lokalne),

Źródło: Opracowanie własne na podstawie: R. Grocki, Vademecum zagrożeń, Bellona, Warszawa 2003, s.10

Zagrożenie powodziami

Powodzie są dość często spotykanym zagrożeniem spowodowanym intensywnymi opadami deszczu, gwałtownym topnieniem śniegu, w efekcie czego nastę-

[88] R. Grocki, Vademecum zagrożeń, Wydawnictwo Bellona, Warszawa 2003, s. 9-10.

puje ekstremalny przypadek wezbrania (podniesienia stanu wody w rzece), który staje się przyczyną zniszczenia środowiska, mienia oraz infrastruktury, mogący spowodować śmierć ludzi i zwierząt[89]. Powodzie można sklasyfikować ze względu na źródło[90]:

- powodzie opadowe – powstałe na skutek zalania terenu wodami pochodzącymi z deszczu oraz topnienia śniegu,
- powodzie rzeczne – powstałe na skutek wezbrania wód rzecznych, strumieni potoków kanałów jezior, a także na skutek topnienia śniegu,
- powodzie od strony morza – powstałe na skutek zalania terenu przez wody morskie,
- powodzie o nieznanej genezie,
- powodzie wywołane innymi czynnikami,
- powodzie wód gruntowych – powstałe na skutek podnoszenia się poziomu wód powyżej gruntu,
- powodzie hydrotechniczne – powstałe na skutek zalania terenu przez wody na skutek awarii budowli piętrzących,
- powodzie wywołane na skutek działalności człowieka.

Według poradników na temat powodzi umieszczonych na stronie Rządowego Centrum Bezpieczeństwa, powodzią nazywa się zalanie przez wodę terenów nadbrzeżnych, wzdłuż koryta rzeki lub brzegu morza, na skutek wezbrania wód. Powódź jest jedną z groźniejszych i tragicznych w skutkach klęsk żywiołowych[91]. Może spowodować powszechne zniszczenia, powodujące utratę życia i szkody w mieniu osobistym i krytycznej infrastrukturze. Osoby, które mieszkają na terenach zalewowych, w budynkach nieodpornych na ten rodzaj kataklizmu lub nie mają systemów ostrzegawczych – powinny uzyskać odpowiedni poziom świadomości na temat zagrożenia powodziowego, jego skutków i modelu zachowań w całym procesie narastania i przebiegu zagrożenia.

Warto pamiętać o tym, że wskutek powodzi zniszczeniu ulega nie tylko infrastruktura taka, jak mosty drogi, domy mieszkania, ale tzw. infrastruktura krytyczna

---

[89] E. Bajkiewicz – Grabowska, Z. Mikulski, *Hydrologia ogólna*, Wydawnictwo PWN, Warszawa 2007, s. 177.

[90] Zaktualizowana metodyka Wstępnej oceny ryzyka powodziowego, czerwiec 2018 r.- https://www.wody.gov.pl/WORP/zal_1_metodyka_04122018.pdf (data dostępu 03.07.2021)

[91] https://www.gov.pl/attachment/4153fe60-a576-487f-96dd-2e863512e1d2 (data dostępu: 03.07.2021).

implikująca ciągłość działania określonych instytucji państwa lub nawet całego państwa[92]. Zagrożenia tej klasy mogą wywołać bezrobocie, a także negatywne skutki dla zdrowia i mienia. Dlatego każdy obywatel powinien mieć świadomość takiego zagrożenia w wymiarze uniwersalnym i stosownie do miejsca swojego pobytu umieć na różne sposoby chronić swoją własność i przygotowywać się do działań pożądanych w takich warunkach.

Zagrożenia pożarowe

Pożar to niekontrolowane rozprzestrzenianie się ognia, stwarzające zagrożenie dla ludzi oraz obiektów objętych pożarem. Może powstać na skutek sił natury, ale również działań człowieka. Pożary można sklasyfikować ze względu na wielkość, wyróżniając pożary małe, średnie, duże i bardzo duże, a także ze względu na źródło ich powstawania, wyróżniając pożary powstające na skutek[93]:

- wyładowania atmosferycznego,
- zaniedbań,
- podpaleń,
- wypadków komunikacyjnych.

Pożary mogą występować w lasach, na łąkach, zabudowach mieszkalnych itp. Na skutek silnych porywów wiatru mogą się szybko rozprzestrzeniać. W momencie gdy pożary zbliżają się lub występują w pobliżu miast, często wymagana jest ewakuacja zapobiegawcza, ponieważ kierunek, z jakim mogą się rozprzestrzeniać pożary, jest nieprzewidywalny. Jak już sygnalizowano najczęstszymi przyczynami pożarów są uderzenia piorunów, iskry podczas suszy, pożary wywołane przez człowieka wynikające z celowego podpalenia lub wypadków. Efektem ubocznym pożarów, które zagrażają również obszarom zamieszkałym, jest dym. Pożary tworzą duże ilości dymu, który może rozprzestrzeniać się przez wiatr i stwarzać zagrożenie dla zdrowia, a przede wszystkim dla układu oddechowego. Coraz więcej osób buduje swoje domy w lasach, na obszarach wiejskich, na odległych terenach górskich lub w ich pobliżu. Ochrona struktur na terenie dzikiej przyrody przysparza spore problemy i może rozciągnąć zasoby gaśnicze do granic możliwości np. utrudnione gaszenie pożarów ze względu na ukształtowanie terenu.

---

[92] T. Kowalczyk, *Przeobrażenia struktury przestrzennej osadnictwa i zmiany hydrotechniczne w dolinie Wisły wywołane powodzią zimową 1982 roku w województwie płockim*, „Notatki Płockie" 1983, nr 1/114, s. 44–55.

[93] S. Tomasz, *Badania przyczyn pożarów.* Wydawnictwo Elamed, Katowice 2008, s. 17.

W zależności od panujących warunków atmosferycznych i ilości wody w środowisku, pożary mogą szybko wymknąć się spod kontroli i spowodować rozległe zniszczenia mienia i utratę życia[94]. Duży pożar może pozostawić po sobie duże ilości spalonej i jałowej ziemi, a obszary te często nie wracają do stanu sprzed pożaru. Zachorowalność i śmiertelność związana z pożarem obejmuje oparzenia, urazy, powikłania oddechowe i skutki sercowo-naczyniowe związane ze stresem.

Zachowania ludzkie mogą być także źródłem zagrożeń, np. palenie w zalesionych obszarach lub niewłaściwe gaszenie ognisk, może być przyczyną wielu pożarów lasów. Inną przyczyną pożarów lasów są wyładowania atmosferyczne. Warto w tym miejscu także zauważyć, że ten rodzaj zagrożeń może niszczyć znacznie zasoby i obiekty infrastruktury krytycznej państwa. Stąd potrzebna jest świadomość całego społeczeństwa o tej klasie zagrożeń i wiedza o możliwościach i skutkach materializacji tych zagrożeń w wymiarze lokalnym. Szczególna zatem rolę przypisuje się współczesnym technologiom informacyjnym i platformom usług IT/ICT.

Zagrożenie suszą

Susza jest to stan niezwykle suchego klimatu w określonym regionie geograficznym z powodu braku opadów. Susza to naturalna powtarzająca się cecha klimatu, która może wystąpić we wszystkich strefach klimatycznych, niemniej jednak jej cechy i skutki w zależności od rejonu występowania mogą być inne. Wyróżnia się następujące typy suszy[95]:

- atmosferyczna – występująca na skutek deficytu opadów,
- hydrogeologiczna – powstająca na skutek długotrwałego obniżenia wód powierzchniowych,
- hydrologiczna – powstająca na skutek obniżenia ilości wody w rzekach i jeziorach,
- rolnicza – powstająca na skutek braku odpowiedniego poziomu wilgotności gleby.

Susza jest klęską żywiołową niebezpieczną dla ludzi, ponieważ powoduje niedobór wody, szkody w uprawach i zwiększoną śmiertelność zwierząt gospodarskich oraz flory i fauny dzikiej. Na obszarach podatnych na suszę można podjąć środki zapobiegawcze takie, jak budowa zbiorników retencyjnych lub systemów zbierania wo-

[94] .R. Krynojewski, S. Mazur, *Podstawy wiedzy o zarządzaniu*, [w:] F.R. Krynojewski, S. Mazur, G. Mikrut, P. Tchorzewski, *Zarządzanie kryzysowe, obrona cywilna kraju, ochrona informacji niejawnych*, Akademia Wychowania Fizycznego, Katowice 2003, s. 66.
[95] https://www.disaster-survival-resources.com/drought.html (data dostępu: 02.07.2021).

dy opadowej. Efektem suszy jest poważne zachwianie równowagi wodnej, co skutkuje deficytem wody, uszkodzeniami oraz zniszczeniami upraw, zachwianiem równowagi wód podziemnych oraz utraty wilgoci[96].

W Polsce susze odnotowywane są raz na 4 – 7 lat[97], a najczęściej towarzyszącym im zjawiskiem są wysokie upały. Swoim działaniem mogą wywołać straty w rolnictwie i pożary. Susza to zagrożenie, które w przypadku braku wcześniejszego przeciwdziałania takiego jak np. budowa zbiorników retencyjnych może wywołać bardzo duże starty gospodarcze zarówno dla całego społeczeństwa jak i pojedynczego obywatela. Materializacja tego zagrożenia to także możliwość naruszenia ciągłości działania określonych podmiotów a przede wszystkim naruszenia bezpieczeństwa społeczno-ekonomicznego państwa lub w szczególności regionów dotkniętych takim kataklizmem. Stąd tak ważną rolę przypisuje się aktualnej, wieloprzekrojowej informacji i wiedzy. Szczególnego znaczenia nabierają więc różne alternatywne formy docierania aktualnej i tematycznie zorientowanej informacji do każdego obywatela objętego takim zagrożeniem.

Zagrożenie wyładowaniami atmosferycznymi

Wyładowania atmosferyczne są groźnymi zjawiskami powodującymi okresowe zagrożenia. Burza charakteryzuje się zakłóceniami i wyładowaniami atmosferycznymi (burza z piorunami), intensywnymi opadami deszczu, ulewnym marznącym deszczem (burza lodowa), silnymi wiatrami (cyklon tropikalny, wichura) lub wiatrem przenoszącym część substancji przez atmosferę, np. burza pyłowa[98]. Niezależnie od rodzaju burzy, każde tego typu zjawisko jest niebezpieczne. Burzy towarzyszą błyskawice, które zabijają więcej ludzi każdego roku niż tornada. Ulewny deszcz z burzami może prowadzić do powodzi błyskawicznych. Silne wiatry, grad i tornada są również zagrożeniami związanymi z niektórymi burzami. Burze z piorunami mogą wystąpić pojedynczo, w klastrach lub w liniach. Pioruny są głównym zagrożeniem podczas burzy. Osoby porażone piorunem często zgłaszają różne długoterminowe, wyniszczające objawy, w tym utratę pamięci, deficyty uwagi, zaburzenia snu, drętwienie,

[96] http://rcb.gov.pl/wp-content/uploads/RCB-Zagro%C5%BCenia-okresowe-w-Polsce-aktualizacja.pdf (data dostępu 10.07.2021).
[97] H. Marek, *Współczesne zagrożenia naturalne Polski w świadomości społeczeństwa, na przykładzie reprezentatywnej grupy mieszkańców miasta Rybnika i powiatu rybnickiego (woj. śląskie)*, s. 37, dostęp w Internecie na *www.seminarium.21/edu.pl/*ks/5/0004%20MAREK.pdf. (data dostępu 10.07.2021).
[98] A. Żebrowski, *Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2012, s. 40-41.

zawroty głowy, sztywność stawów, drażliwość, zmęczenie, osłabienie, skurcze mięśni, depresję[99]. I znowu dla tego typu zagrożeń ważną przesłanką staje się świadomość każdego obywatela na temat zachowania w przypadku zaistnienia tego zdarzenia oraz sposobu przeciwdziałania skutkom a wcześniej zapobiegania (ochrony) przed ich wystąpieniem. Ważna rolę odgrywać tu mogą nie tylko tradycyjne środki powiadamiania. Szybkość i trafność działań może być ważnym atrybutem skuteczności działań dzięki wykorzystywaniu współczesnych usług IT/ICT.

Zagrożenie silnymi wiatrami

Wiatr to naturalny ruch powietrza lub innych gazów względem powierzchni planety. Wiatry występują w kilku skalach, od trwających kilkadziesiąt minut burz spowodowanych globalnym ociepleniem i lokalnych wiatrów trwających kilka godzin, po wiatry globalne wynikające z różnic w absorpcji energii słonecznej pomiędzy strefami klimatycznymi Ziemi[100].

Wiatry są ogólnie klasyfikowane zgodnie z ich zasięgiem przestrzennym, prędkością i kierunkiem, siłami, które je wytwarzają, obszarami ich występowania i ich skutkami [101].

Silne wiatry wywołują swoim dzianiem poważne zagrożenie, a prawdopodobieństwo ich wystąpienia w Polsce jest coraz większe. Wiatr wiejący z duża prędkością może stanowić poważne zagrożenie dla ludzi, zwierząt, budynków oraz infrastruktury krytycznej. Mając na uwadze charakter negatywnych skutków powstałych w wyniku porywistych wiatrów trudno mówić o skutecznej ochronie. Podejmowane zapobiegawczych działań powinno zmierzać do minimalizowania skutków poprzez wykrywanie zagrożeń oraz ostrzeganie i informowanie ludności o zagrożeniu. Niemniej jednak należy sobie zdawać sprawę z tego, że w przypadku wystąpienia tego zagrożenia mogą być liczne ofiary w ludziach i ich mieniu[102].

Awarie techniczne

Oprócz katastrof naturalnych istotnym źródłem zagrożeń mogą być awarie techniczne, poprzez które należy rozumieć gwałtowane oraz nieprzewidziane uszkodze-

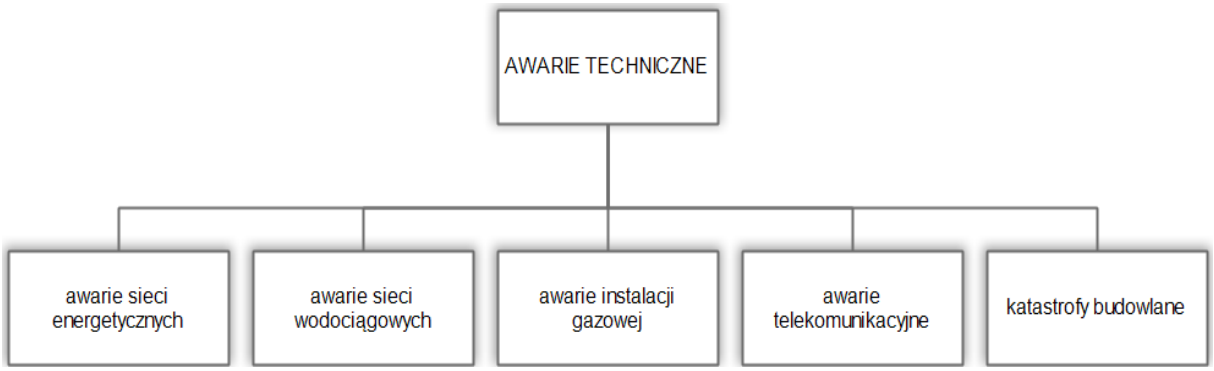
[99] https://www.gov.pl/web/kmpsp-jeleniagora/burze-zagrozenia-atmosferyczne (data dostępu 10.07.2021).
[100] G. Sobolewski, *Zagrożenia kryzysowe*, Wydawnictwo AON, Warszawa 2011, s. 38-40.
[101] E. Wołoszyn, *Meteorologia i klimatologia w zarysie*, Wydawnictwo Politechniki Gdańskiej, 2009, s.125-136.
[102] Tamże s. 125-136.

nia lub zniszczenia obiektu lub systemu, urządzeń technicznych – w efekcie czego następuje przerwa w ich użytkowaniu i utrata ich własności[103].

Awaria techniczna (rys. 3.1) jest zdarzeniem spowodowanym nieprawidłowym działaniem struktury technologicznej i/lub błędem ludzkim w kontrolowaniu lub obsłudze struktury technologicznej. Katastrofy te można uznać za katastrofę stworzoną przez człowieka, co oznacza, że istnieje cecha "identyfikowalnej przyczyny[104].

Skutki katastrofy nie tylko dla rodzin i jednostek, ale także dla całych społeczności i państwa mogą być długotrwałe. Wszystkie rodzaje klęsk są katastrofalne w skutkach, ale awarie techniczne wydają się być trudne do przewidzenia. Awaria techniczna jest nagła, niespodziewana i nieprzewidywalna, ale można się na nią przygotować. Wdrożenie odpowiednich scenariuszy działań, przewidywane potencjalnych możliwych usterek, które mogą wywołać awarie techniczne, może przyczynić się do zmniejszenia skutków zagrożenia.

W art. 3 ust. 3 ustawy o stanie klęski żywiołowej katastrofa techniczna definiowana jest jako gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości[105].



Rysunek 3.1. Rodzaje awarii technicznych

Źródło opracowanie własne na podstawie Planu Zarządzania Kryzysowego Województwa Pomorskiego

[103] https://soinso.uj.edu.pl/klasyfikacja-zagrozen (data dostępu 13.07.2021).
[104] R. Goldsteen, J.K. Schorr,. *The long-term impact of a man-made disaster: An examination of a small town in the aftermath of the Three Mile Island Nuclear Reactor Accident, Disasters*, **"**Department of Sociology Stetson University DeLand", Florida, U.S.A, 1982, Vol. 6, No. 1, s. 50–59.
[105] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej. (Dz. U. z 2002 r. Nr 62, poz. 558).

Awarie sieci energetycznej

Awaria techniczna to nagła i poważna awaria systemu elektroenergetycznego, która powoduje dłuższą przerwę w dostawie energii . Wyróżnia się następujące rodzaje awarii sieci energetycznej [106]:

Awaria techniczna to nagła i poważna awaria systemu elektroenergetycznego, która powoduje dłuższą przerwę w dostawie energii[107]. Wyróżnia się następujące rodzaje awarii sieci energetycznej[108]:

- *blackout* – rozległa awaria napięcia występująca na dużym obszarze powstająca na skutek wyłączenia wszystkich urządzeń nie posiadających awaryjnego zasilania,
- *rolling blackout* – to czasowe zaplanowane wyłączenie zasilania poszczególnych obiektów ze względu na brak mocy wytwórczych. Dotyczy to przeważnie zakładów przemysłowych np. wyłączenia w określonych godzinach zasilania na danym obszarze dzielnic, miast lub wsi,
- *brownout* – występuje na skutek obniżenia parametrów jakościowych prądu. W efekcie czego następuje spadek napięcia w sieci oraz spadek częstotliwości prądu. Obniżenie napięcia powoduje m.in. zmniejszenie mocy elektrycznej źródeł ciepła takich jak np. grzejniki elektryczne.

Awarie sieci energetycznych mogą powstać na skutek wyładowań atmosferycznych, np. podczas burzy. Również takie zjawiska atmosferyczne jak śnieg i wichury mogą skutkować uszkodzeniem instalacji energetycznych[109].

Awaria sieci wodociągowej

Awaria sieci wodociągowej może powstać na skutek uszkodzenia przewodu lub uzbrojenia, powodując całkowity lub częściowy brak dostępu wody. Powodem wystąpienia awarii wodociągowej może być brak szczelności i przepustowości oraz mechaniczne uszkodzenie sieci wodociągowej. Może ona powstać również na skutek błędu ludzkiego poprzez niewłaściwy dobór materiałów, błędne położenie instalacji, ułożenie instalacji na gruntach nadmiernie nawodnionych lub osiadających, a także

[106] https://www.techsterowniki.pl/blog/jak-zabezpieczyc-swoj-dom-przed-blackoutem (dostęp 2019-10-04).
[107] Obserwatorium Językowe Uniwersytetu Warszawskiego [dostęp 2019-10-04].
[108] https://www.techsterowniki.pl/blog/jak-zabezpieczyc-swoj-dom-przed-blackoutem (dostęp 2019-10-04).
[109] Biuro Bezpieczeństwa i Zarządzania Kryzysowego: Awaria Techniczna. (data dostępu 03.08.2021)

na skutek niezastosowania odpowiedniego zagęszczenia okalającego rury. Wyróżnia się dwa rodzaje awarii w sieci wodociągowej[110]:

- nagły – charakteryzujący się dużym wypływem wody
- stopniowy – charakteryzujący się niewielkim wypływem wody w początkowej fazie. Wypływ może się pojawiać na powierzchni terenu lub nie, co zdarza się znacznie częściej.

Awarie w sieci wodociągowej to niechciane i nieuniknione problemy w eksploatacji, dlatego też niezbędne jest wyposażenie przedsiębiorstw na danym terenie w sprzęt do wykrywania i usuwania tego typu usterek[111].

Awarie instalacji gazowej

Awarie instalacji gazowej mogą być przyczyną wypadków. Ulatniający się gaz może spowodować wybuch, jeśli zgromadzi się w dużych ilościach[112].

Do najczęstszych przyczyn awarii sieci gazowej zalicza się[113]:

- niewłaściwie wykonany projekt, np. błędne wykonanie obliczeń hydraulicznych lub wytrzymałościowych,
- awarię elementów peryferyjnych wspomagających pracę sieci,
- awarie mechaniczne spowodowane korozją lub oddziaływaniami zewnętrznymi,
- awarię połączeń rozłącznych i nierozłącznych,
- awarię systemów kontroli,
- awarię systemów bezpieczeństwa,
- odchylenia od normalnych warunków pracy,
- błędy ludzkie i organizacyjne,
- zakłócenia z zewnątrz,
- czynniki przyrodnicze,
- terroryzm,
- sabotaż.

[110] https://www.teraz-srodowisko.pl/aktualnosci/wiekszosc-awarii-sieci-wodociagowych-ma-miejsce-przy-przylaczach-4827.html (data dostępu 03.08.2021).
[111] https://inzynierbudownictwa.pl/awarie-w-systemie-dystrybucji-wody-cz-i/ (data dostępu 03.08.2021)
[112] Biuro Bezpieczeństwa i Zarządzania Kryzysowego: Awaria Techniczna.
[113] https://asystentbhp.pl/przyczyny-awarii-sieci-gazowych/ (data dostępu 03.08.2021)

Zgodnie z art. 62 ust. 1 ustawy Prawo budowlane – na właścicielach i zarządcach obiektów budowlanych spoczywa obowiązek zapewnienia co najmniej raz w roku kontroli stanu technicznego użytkowanego obiektu budowlanego. W szczególności sprawdzenie stanu technicznego przewodów kominowych, dymowych, spalinowych i wentylacyjnych oraz instalacji gazowych[114].

W przypadku stwierdzenia uszkodzeń lub braków właściciel, zarządca lub użytkownik obiektu budowlanego, na którym spoczywa obowiązek w zakresie napraw określonych w przepisach odrębnych bądź umowach, zobowiązany jest w czasie lub bezpośrednio po przeprowadzonej kontroli usunąć stwierdzone uszkodzenia oraz uzupełnić braki, które mogłyby spowodować zagrożenie życia lub zdrowia ludzi, bezpieczeństwa mienia, bądź środowiska, w szczególności katastrofę budowlaną, pożar, wybuch, porażenie prądem elektrycznym lub zatrucie gazem[115].

Awarie telekomunikacyjne

Na podstawie art. 176 ustawy Prawo telekomunikacyjne, przedsiębiorcy świadczący usługi telekomunikacyjne na obszarze większym niż jedna gmina są zobowiązani do posiadania planu działań w sytuacjach szczególnych zagrożeń określających m.in. sposób zabezpieczenia publicznych sieci i urządzeń telekomunikacyjnych przed zakłóceniami, skutkami katastrof i klęsk żywiołowych oraz nieuprawnionym dostępem[116]. Z analizy planów opracowanych dotychczas przez przedsiębiorców telekomunikacyjnych wynika, że na zakłócenia w sieciach i systemach łączności mogą wpływać następujące kategorie zagrożeń:[117]:

- klęski żywiołowe i katastrofy naturalne,
- katastrofy i awarie techniczne,
- terroryzm i cyberterroryzm oraz zdarzenia o charakterze kryminalnym.

Bezpieczeństwo krytycznej infrastruktury telekomunikacyjnej jest istotnym zagadnieniem. Zapewnienie odpowiedniego poziomu obsługi oraz gotowości jest niezbędne w celu zapewnienia ciągłości działania. Kluczową rolę w tym procesie odgrywa współpraca z odpowiednimi organami państwowymi, samorządowymi oraz innymi

[114] Ustawa z dnia 7 lipca 1994 r.- Prawo budowlane (Dz. U. z 2019 r. poz. 1186 z późn. zm.).
[115] https://asystentbhp.pl/przyczyny-awarii-sieci-gazowych/ (data dostępu 03.08.2021).
[116] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.
[117] https://samorzad.gov.pl/web/gmina-buczkowice/zarzadzanie-kryzysowe-zagrozenia (data dostępu 04.08.2021).

organizacjami świadczącymi usługi telekomunikacyjne[118]. Współpraca pomiędzy dostawcami usług telekomunikacyjnych oraz agencjami radowymi lub unijnymi odgrywa istotną rolę w procesie zapewnienia bezpieczeństwa i dostępności sieci telekomunikacyjnej[119]. Ogólnie można stwierdzić, że omówione wyżej klasy awarii technicznych powodować mogą nieakceptowalny poziom ryzyk i dlatego wymagają wcześniejszego monitorowania, prognozowania a nawet symulowania (stosowania modeli symulacyjnych) przebiegu procesu eksploatacji obiektów infrastruktury krytycznej determinującej ciągłość funkcjonowania wybranych sektorów a przez to ciągłość funkcjonowania państwa. Stąd tak duża rola dla platformy Internetu Rzeczy i innych usług IT/ICT, co będzie Przedmiotem dalszych rozważań.

Katastrofy budowlane

Ustawa z dn. 7.07.1994 r. o Prawie budowlanym, art. 73 ust. 1, definiuje katastrofę budowlaną jako niezamierzone, gwałtowne zniszczenie obiektu budowlanego lub jego części, a także konstrukcyjnych elementów rusztowań, elementów formujących, ścianek szczelnych i obudowy wykopów. Ustawowa definicja dotyczy tylko zdarzenia, które spełnia łącznie trzy kryteria: kryterium niezamierzoności zniszczenia, kryterium gwałtowności zniszczenia oraz kryterium przedmiotu zniszczenia[120].Katastrofa budowlana to zniszczenie określonego obiektu lub jego części. Można ją sklasyfikować wg następujących kryteriów[121]:

- przedm*iot*owe – odnoszące się do kwestii materialnych, rzeczowych oraz technicznych,
- podmiotowe – odnoszące się do zidentyfikowania podmiotu odpowiedzialnego za powstanie zniszczenia.

Katastrofy budowlane najczęściej występują na skutek[122]:

- wybuchu gazu,
- obsunięcia stropów lub nadwyrężenia ważnych elementów konstrukcyjnych budynków,

---

[118] M. Szyłkowska, *Cyfrowa globalizacja determinantem współczesnego bezpieczeństwa*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy 16 (3), Legnica 2015, s. 75.

[119] K. Baniak , Analiza zagrożeń telekomunikacyjnych sektora publicznego, Bezpieczeństwo w telekomunikacji i teleinformatyce, Biblioteka „Bezpieczeństwa Narodowego", kwartalnika wydawanego przez Biuro Bezpieczeństwa Narodowego, tom 3, 2007.

[120] Ustawa z 7 lipca 1994 r. Prawo budowlane (Dz.U. z 2010 r. nr 243, poz. 1623 z późn. zm.).

[121] J. Baryłka, Katastrofy budowlane – określenia i analiza zdarzeń. Referat na XII Konferencji Naukowo-Technicznej nt. Warsztat pracy rzeczoznawcy budowlanego. Kielce-Cedzyna, 16 – 18.05.2012 r.

[122] https://gminadebno.pl/katastrofy-budowlane.html (data dostępu 03.08.2021).

- tąpnięć.

Najczęściej katastrofy budowlane występują w czasie eksploatacji obiektów budowlanych. Przyczyny tych zdarzeń wynikają ze skumulowania się błędów projektowych, wykonawczych i eksploatacyjnych[123]. Podobnie, jak poprzednio opisane awarie techniczne również ta kategoria awarii wymaga wykorzystania różnych współczesnych technologii IT/ICT do określania stopnia prawdopodobieństwa ich wystąpienia w powiązaniu z innymi zagrożeniami (w tym z klęskami żywiołowymi) i symulowania ich skutków oraz sposobów zachowania i przeciwdziałania. Syntetyczna informacja dla określonych scenariuszy może być podstawą świadomych i skutecznych zachowań wybranej grupy interesariuszy.

Zagrożenia wynikające z działalności człowieka

Działalność człowieka może wywołać negatywne skutki dla środowiska naturalnego, bezpieczeństwa i porządku publicznego. Na skutek tych działań istnieje ryzyko zagrożenia życia, zdrowia oraz środowiska naturalnego. Potencjalne zagrożenia spowodowane działalnością człowieka można podzielić na trzy rodzaje:[124]:

- zakłócenia bezpieczeństwa i porządku publicznego,
- katastrofy techniczne,
- akty terroru.

Zakłócenia bezpieczeństwa i porządku publicznego to głównie przestępczość zarówno gospodarcza jak i kryminalna; niezgodna z prawem działalność osób nieletnich, zakłócenia porządku publicznego m.in. wykroczenia i naruszenia norm zwyczajowych, zjawiska nadużywania alkoholu czy też zażywania narkotyków bądź innych substancji psychoaktywnych, prostytucja, analfabetyzm, agresja, masowe migracje, stres, hazard, bezdomność, kradzież dóbr kultury, kult przemocy, kryzys demograficzny, ubożenie i głód dużych grup społecznych, katastrofy i kataklizmy (klęski) prowadzące do bezrobocia, a także rozwój destrukcyjnych grup psychomanipulacyjnych[125].

W przypadku tego typu zagrożeń można przyjąć, że wręcz niemożliwe jest całkowite pozbycia się ich z życia, a wymienione zagrożenia stanowią ważny problem dla

---

[123] A. Baryłka, J. Baryłka, Okresowe kontrole jako ważny etap diagnostyki technicznej obiektów budowlanych. Referat na V Krajowej Konferencji Naukowo-Technicznej ARCHBUD 2012 „Problemy współczesnej architektury i budownictwa", Zakopane, 3 – 6.09.2012 r

[124] S. Michałowski, *Bezpieczeństwo ekonomiczne w stosunkach Wschód – Zachód*, Sprawy międzynarodowe, Warszawa ,1990, Vol. 36, nr.4, s 22–23.

[125] T. Michalski, *Zagrożenia we współczesnym świecie jako temat edukacji geograficznej*, Wydawnictwo Szkolne i Pedagogiczne, 2008, s. 7.

wszystkich mieszkańców kuli ziemskiej. Brak możliwości wyeliminowania ich z życia codziennego nie oznacza, że nie można im przeciwdziałać profilaktyczne oraz zmniejszać poziom skutków ich wystąpienia. Identyfikacja tego typu zagrożeń oraz skutków społeczno-ekonomicznych i kulturowych ich materializacji a także upowszechnianie modelowych zachowań indywidulanych i grupowych – może być ważną rolą rozwiązań informatycznych związanych ze współczesnymi technologiami IT/ICT (w tym systemy *Big Data*). Dostępność syntetycznych raportów w tym obszarze problemowym może istotnie wzmacniać poziom świadomości sytuacyjnej.

Zakłócenia bezpieczeństwa i porządku publicznego

Porządek publiczny to przestrzeń zewnętrzna, w której obywatele funkcjonują według określonych zasad, przepisów i form, których załamanie prowadzi do zagrożeń ze strony osób niemających na celu podporządkowania się zasadom, formom oraz nakazom[126].

Bezpieczeństwo publiczne to taki stan w państwie, który umożliwia normalne funkcjonowanie i korzystanie z praw i wolności gwarantowanych przez Konstytucję i inne ustawy, bez narażania otoczenia na szkody spowodowane zachowaniem człowieka, siłami natury, technologią itp. Zadania realizowane w zakresie zapewnienia porządku publicznego i bezpieczeństwa dotyczą zwalczania czynów zabronionych takich, jak[127]:

- przestępczość pospolita i zorganizowana o charakterze ekonomicznym,
- narkomania,
- przestępczość kryminalna.

W zakresie ochrony życia i zdrowia oraz mienia obowiązek zwalczania przestępstw w głównej mierze spoczywa na Policji. Zapewnienie porządku publicznego oraz bezpieczeństwa na odpowiednim poziomie to skuteczne zapobieganie ich naruszeniom, a także wykrywanie przestępstw i wykroczeń godzących w życie, zdrowie i mienie obywateli, jak również interesy Państwa[128].

Katastrofy techniczne

Katastrofy techniczne to nagłe tragiczne w skutkach zdarzenia, na skutek których ktoś ucierpiał poniósł śmierć lub spowodowane zostały straty materialne

[126] W. Czapliński, Bezpieczeństwo, spokój i porządek publiczny – próba konstrukcji teoretycznej, „Gazeta Administracji i Policji Państwowej" 1929, nr 19, s. 678
[127] Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2014, s. 36
[128] Tamże s. 36.

i ekologiczne. Katastrofy techniczne w uproszczony sposób można sklasyfikować dzieląc je na wypadki oraz awarie [129]:

- wypadek to zdarzenie, które w swoich skutkach dotknęło niewielką liczbę osób oraz posiada mały zasięg terytorialny, niemniej jednak może ono zyskać miano katastrofy[130],
- awaria to nagłe uszkodzenie lub zniszczenie obiektu, urządzenia technicznego, lub systemu, które powoduje przerwę w jego działaniu lub utratę jego funkcjonalności[131].

Katastrofy techniczne często kojarzone są z bezpośrednią działalnością człowieka i trudno określić, które czynniki miały wpływ na ich rozwój. Katastrofy techniczne można podzielić na[132]:

- awarie urządzeń infrastruktury technicznej,
- katastrofy budowlane,
- awarie chemiczne,
- awarie ekologiczne,
- katastrofy komunikacyjne,
- pożary,
- epidemie.

Często jedna katastrofa techniczna może być przypisana do różnych kategorii ze względu na skutki, jakie wywołuje np. wypadek drogowy cysterny z niebezpieczną substancją (katastrofa drogowa) oraz wydostanie się materiałów niebezpiecznych z cysterny do środowiska (skażenie chemiczne).

Awarie urządzeń infrastruktury technicznej

Awarie urządzeń infrastruktury technicznej mogą powstać na skutek uszkodzenia instalacji i sieci gazowej, rozdzielczej sieci wodociągowej, kanalizacyjnej, a także sieci ciepłowniczej i energetycznej. Szczególnie niebezpiecznym rodzajem zagrożenia jest awaria różnego rodzaju typu gazociągów, które mogą wywołać poważne zagrożenie dla mieszkańców rejonu, na którym doszło do uszkodzenia. Awarie takie jak uszkodzenia linii energetycznych czy instalacji wodociągowych, nie stanowią bezpośredniego zagrożenia dla pojedynczego obywatela, niemniej jednak mo-

[129] J.Rokitowska, Vademecum Bezpieczeństwa, w. O. Wasiuta, R. Klepka, R. Kopeć(red.), Wydawnictwo LIBRON– Filip Lohner, 2018, Kraków, s. 366.
[130] Tamże s. 366.
[131] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2017 r. poz. 1897).
[132] Tamże.

gą znacznie utrudniać jego funkcjonowanie i obszaru, na którym się on znajduje. W przypadku obiektów specjalnych takich, jak np. szpitale, mogą one stanowić zagrożenia dla życia lub zdrowia. Awarie techniczne mogą powstać na skutek działalności człowieka lub mogą być efektem działania sił natury takich, jak pożar, wichury, powódź itp.[133].

Katastrofa budowlana

Katastrofa budowlana to niezamierzone, gwałtowne zniszczenie obiektu lub jego części, a także konstrukcyjnych elementów rusztowań, elementów urządzeń formujących, ścianek szczelnych i obudowy wykopów[134]. Na skutek katastrofy budowlanej uszkodzeniu mogą ulec instalacje: elektryczne, wodociągowe, kanalizacyjne, ciepłownicze i gazowe.

Wypadki budowlane mogą być spowodowane siłami natury lub innymi zagrożeniami takimi, jak ataki terrorystyczne, niedopełnienie obowiązków przez osoby zarządzające infrastrukturą lub na skutek nie przestrzegania zasad bezpieczeństwa. Tego typu zagrożenia mogą powodować duże straty i stwarzać bezpośrednie zagrożenie dla życia ludzkiego. Stała konserwacja obiektów, regularne prace porządkowe takie, jak np. odśnieżanie dachów w czasie intensywnych opadów śniegu i przestrzeganie zasad bezpieczeństwa może przyczynić się do zmniejszenia ryzyka potencjalnego uszkodzenia budynków.

Katastrofy komunikacyjne

Katastrofy komunikacyjne to wypadki w ruchu lądowym, wodnym lub powietrznym. Można je sklasyfikować, dzieląc je na trzy kategorie :

- zagrożenia spowodowane przez człowieka – do tej grupy należy zaliczyć wszelkiego rodzaju sytuacje spowodowane bezmyślnością oraz brakiem ostrożności i wyobraźni kierowców, p. brawura lub niedostawanie prędkości do warunków, które panują na drodze,
- zagrożenia wynikające z wad konstrukcyjnych – do tej grupy zagrożeń należy zaliczyć wady konstrukcyjne pojazdów oraz m.in. ubytki w powierzchni dróg,
- zagrożenia wynikające z sił przyrody – do tej grupy należy zaliczyć zjawiska atmosferyczne takie, jak silne burze, burze śnieżne itp.

Katastrofy komunikacyjne mogą zostać sklasyfikowane ze względu na katastrofy, w ruchu lądowym, morskim, powietrznym i kolejowym. Każda z tych katastrof może

[133] Plan Zarządzania Kryzysowego Powiatu Płockiego.
[134] Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane (Dz.U. z 2021 r. poz. 2351).

wywołać zagrożenie dla życia zdrowia i mienia, a także środowiska naturalnego obejmując swoim zasięgiem małe tereny lub katastrofę o większym zasięgu terytorialnym[135].

Katastrofa chemiczna

Katastrofa chemiczna to przedostanie się do środowiska naturalnego substancji toksycznych lub promieniotwórczych, stanowiących zagrożenie dla zdrowia i życia roślin, zwierząt i człowieka[136]. Na skutek katastrofy chemicznej do środowiska uwalniają się zanieczyszczenia pochodzenia przemysłowego, komunalnego i transportowego, a także zanieczyszczenia ekosystemu spowodowane przez toksyczne odpady i katastrofy ekologiczne.

Istotę katastrofy chemicznej stanowi niepożądana obecność substancji chemicznych, biologicznych lub promieniotwórczych, które ze względu na swoje szkodliwe właściwości mogą przyczynić się do utraty życia lub zdrowia[137]. W przypadku katastrof chemicznych należy zwrócić uwagę na fakt, że nie każdą szkodliwą substancje można określić mianem skażenia. Aby substancja została uznana za skażenie, ilość substancji toksycznej musi być wystarczająco duża, aby spowodować zagrożenie, które jest określone przez stężenie substancji. Podstawą klasyfikacji substancji chemicznej jako zagrożenie jest Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy[138]. Zagrożenia skażeniami należy traktować jako źródło poważnych sytuacji kryzysowych powstających na skutek obecności niepożądanej substancji chemicznej, promieniotwórczej lub biologicznej. Zjawiska te mogą wystąpić w konsekwencji uszkodzeń infrastruktury na skutek: zanieczyszczeń powietrza, użycia środków bojowych (pomimo zakazu używania broni chemicznej),środków toksycznych i przemysłowych[139]. W przypadku wystąpienia skażeń należy zachować szczególną ostrożność stosować się do zasad

---

[135] Wypadki drogowe w Polsce w 2013 roku, raport Komendy Głównej Policji, Biuro prewencji i ruchu drogowego, Wydział Ruchu Drogowego, Warszawa 2014.

[136] Z. Otałęga, *Encyklopedia biologiczna tom X,* Wydawnictwo Agencja Publicystyczno-Wydawnicza Opres, Kraków 2000, s. 18.

[137] Bezpieczeństwo ekologiczne Rzeczypospolitej Polskiej, http://adamkorcz.dl.interia.pl/, zagrożeń *(data dostępu:* 10.10.2022).

[138] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy (Dz. U. 2002 nr 217, poz. 1833).

[139] Tamże.

bezpieczeństwa określonych przez organy właściwe w państwie, aby uniknąć poważnych konsekwencji zdrowotnych.

Katastrofa ekologiczna

Katastrofa ekologiczna powstaje na skutek bezpośredniego lub pośredniego działania człowieka, w wyniku którego mogą nastąpić: zagrożenie życia i zdrowia istot żywych oraz znaczące zmiany środowiska naturalnego[140]. Katastrofy ekologiczne mogą przyczynić się do zniszczenia lub uszkodzenia środowiska i mogą być one wywołane również na skutek działalności człowieka – antropomorficzne lub na skutek dziania sił natury – nieantropomorficzne. Do katastrof ekologicznych zaliczane są: katastrofy naturalne i przemysłowe, zanieczyszczenia powietrza, wody i gleby na masową skalę, wykorzystywanie niebezpiecznych technologii przemysłowych, niekontrolowana eksploatacja zasobów naturalnych, a także próby nuklearne oraz testy nowych typów broni[141].

Pomimo, iż katastrof ekologicznych nie da się uniknąć, a rozwój cywilizacji i wpływ działalności człowieka sprawia, że wyrządzają one poważne szkody, to można zmniejszyć ich skutki poprzez podejmowanie działań zmierzających do ochrony środowiska. Każda osoba może mieć wpływ na otoczenie i bezpieczeństwo ekologiczne dbając o nie poprzez podejmowanie działań zmierzających np. do niezanieczyszczania środowiska. Niemożliwe jest całkowite wyeliminowanie zagrożeń wynikających np. z wydostania się niebezpiecznych substancji do atmosfery, wypadków komunikacyjnych lub zanieczyszczeń środowiska. Poprzez właściwe uświadamianie obywateli o zagrożeniach możliwe jest zwiększenie świadomości sytuacyjnej na ich temat oraz częściowe ograniczenie ich skutków. Ważną przesłanką do kształtowania odpowiedniego poziomu świadomości sytuacyjnej dla postrzegania, rozumienia i przeciwdziałania zagrożeniom płynącym z zachowań ludzkich jest obraz statystyczny realizacji tej klasy zagrożeń oraz poziomu skutków. Raporty tego typu powinny być dostępne na forach internetowych. Aktualność danych może być warunkowana wykorzystaniem różnego typu systemów monitorujących a w tym odpowiednich czujników (sensorów) rejestrujących w czasie rzeczywistym symptomy narastania zagrożenia a potem jego następstw. Taki spójny obraz działań może kreować pożądany poziom świadomości sytuacyjnej obywateli i całych społeczeństw.

---

[140] D. Kompała, I*stota zagrożeń,* Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 3, 2014, s. 26.
[141] Tamże s. 26.

Epidemia

Epidemia to pojawienie się kilku określonych chorób (najczęściej zakaźnych) w tym samym czasie lub w krótkim okresie czasu. Epidemia stanowi duże zagrożenie dla zdrowia i życia i może być wywołana przez[142]:

- spożycia zakażonej żywności lub wody,
- kontaktu z chorym,
- wydychania skażonego powietrza.

W polskim prawie administracyjnym epidemia definiowana jest jako: „wystąpienie na danym obszarze zakażeń lub zachorowań na chorobę zakaźną w liczbie wyraźnie większej niż we wcześniejszym okresie albo wystąpienie zakażeń lub chorób zakaźnych dotychczas niewystępujących”[143].

Kilka przypadków bardzo rzadkiej choroby można sklasyfikować jako epidemię, podczas gdy wiele przypadków powszechnej choroby (takiej jak przeziębienie) nie. Epidemia może spowodować bardzo duże szkody poprzez straty finansowe, a także pogorszenie stanu zdrowia i utratę życia.

Terroryzm

Terroryzm to różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz państwa i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych; realizowane bezwzględnie, za pomocą różnych środków (nacisk psychologiczny, przemoc fizyczna, użycie broni i ładunków wybuchowych) w warunkach specjalnie nadanego rozgłosu i celowo wytworzonego w społeczeństwie lęku[144].

Terroryzm nie jest zjawiskiem nowym, lecz zjawiskiem zmiennym, wieloaspektowym i dynamicznym, w tym: zmieniają się formy, środki i cele działalności terrorystycznej. Na terroryzm wpływa rozwój cywilizacyjny oraz rozwój nauki i technologii, zwłaszcza w zakresie nowych środków przekazu, środków masowego przekazu i zaawansowanych technologii komunikacyjnych[145].

---

[142] D. Borowska-Mostafa, Encyklopedia PWN A-Z Oryginalna Azetka, Wydawnictwo Naukowe PWN SA, Warszawa, 2012.
[143] Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu i zwalczaniu zakażeń i chorób zakaźnych i ludzi (Dz.U. z 2021 r. poz. 2069).
[144] D. Borowska-Mostafa, Oryginalna Azetka Encyklopedia PWN, Wydawnictwo Naukowe PWN SA, Warszawa, 2012, s. 1046.
[145] G. Nowacki, *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, nr 44, część 1, 2015, s. 408.

Rozwój współczesnych technologii IT/ICT spowodował, że powstały wspominane wcześniej nowe zagrożenia i tak terroryzm przeniósł się również do przestrzeni cyfrowej tworząc jego rozgałęzienie w formie cyberterroryzmu, który stanowi konwergencję terroryzmu i cyberprzestrzeni. Powszechnie uważa się, że są to bezprawne ataki i groźby ataków na komputery, sieci i przechowywane w nich dane w celu zastraszenia lub zmuszenia rządu lub jego obywateli do realizacji celów politycznych lub społecznych. Ponadto, aby sklasyfikować ataki jako cyberterroryzm akcentuje się przemoc wobec ludzi i mienia lub powodowanie szkody wywołującej strach[146].

Zagrożenia takie, jak katastrofy naturalne, awarie techniczne oraz powstałe na skutek działalności człowieka mogą zaburzyć funkcjonowanie państwa a nawet spowodować materializację ryzyka utraty jego informacyjno-decyzyjnej ciągłości działania oraz utraty bezpieczeństwa pojedynczego obywatela. Stąd tak ważna staje się sprawność i niezawodność sytemu informacyjnego (w tym także informatycznych rozwiązań), który może na bieżąco wspierać zweryfikowanymi danymi o konkretnym zagrożeniu, prognozowanych skutkach a także o zasadach (algorytmach) postępowania w zaistniałych warunkach (wg prawdopodobnego lub realnie realizowanego scenariusza). Ponadto, aby zapobiec ww. zagrożeniom w Polsce, zorganizowano System Zarządzania Kryzysowego wspierany – aktualnie niewystarczająco – dostępnymi platformami narzędziowymi IT/ICT.

3.3. Strukturalno-organizacyjne aspekty funkcjonowania systemu zarządzania kryzysowego

Współczesne zagrożenia mogą pojawić się w sposób gwałtowny i mogą skutkować w wymiarze ogólnospołecznym a nawet globalnym oraz indywidualnym, a w tym utratą życia, zdrowia, dóbr materialnych oraz prowadzić do destabilizacji m.in. rozwoju gospodarczego. Wystąpienie ich na różnych obszarach może wywołać nieprzewidywalne skutki. Istotne zatem jest odpowiednie przeciwdziałanie tym zagrożeniom oraz ograniczenie potencjalnych strat poprzez wykorzystanie dostępnych sił i środków. Istotą zarządzania kryzysowego jest zapobieganie sytuacjom kryzysowym, będącym następstwem zagrożeń poprzez przygotowanie się na nie w drodze zaplanowanych działań oraz odpowiednie reagowanie w momencie ich wystąpienia, dążąc do usunięcia ich potencjalnych skutków. W zarządzaniu kryzysowym kluczową rolę odgrywa nie tylko reagowanie w momencie pojawienia się zagrożeń, ale również po-

[146] M. Staruch, *praca mgr pt.", Cyberterroryzm jako współczesne zagrożenie informacyjnego bezpieczeństwa kraju", napisana pod kierunkiem, dr inż. R. Hoffmana, W*AT, Warszawa, 2018 s. 15.

dejmowanie odpowiednich kroków zmierzających do uniknięcia ich, a jeśli już powstaną, to dążenie do działań mających na celu przywrócenie stanu sprzed zaistniałej sytuacji[147].

Skuteczne zarządzanie kryzysowe to działania profilaktyczne, zabezpieczające niejako przed materializacją poszczególnych rodzajów zagrożeń dzięki sprawnemu systemowi informacyjnemu. Przedłużeniem tego procesu jest dążenie do maksymalnego ograniczenia strat ludzkich, utraty mienia, a także strat w środowisku naturalnym przy pomocy możliwych do wykorzystania sił i środków. W Polsce funkcjonuje wieloszczeblowy System Zarządzania Kryzysowego (SZK). Struktura tego systemu obejmuje szczeble administracyjne, rządowe i samorządowe. System ten posiada adekwatną do potrzeb strukturę organizacyjno-funkcjonalną, która umożliwia realizację zadań zmierzających do ochrony infrastruktury krytycznej państwa oraz zdrowia, życia, mienia i środowiska naturalnego. System ten jest zintegrowany z systemami NATO oraz UE. SZK składa się z podsystemów zarządczych na szczeblu krajowym, wojewódzkim, powiatowym i gminnym[148]. Skuteczne funkcjonowanie Systemu Zarządzania Kryzysowego zależy od wielu czynników takich, jak np. regulacje prawne, stosowne uprawnienia osób funkcyjnych systemu, rozwiązania strukturalne oraz powiązania organizacyjne, odpowiednie przygotowanie fazy planowania poprzez utworzenie wielowariantowych planów zarządzania kryzysowego uwzględniających możliwe do użycia siły i środki potrzebne do wykorzystania w momencie zaistnienia zagrożenia. W tym celu niezbędny jest stały monitoring każdej grupy zagrożeń, dzięki któremu możliwe jest otrzymywanie aktualnych, kompleksowych i rzetelnych informacji o zagrożeniach. Kluczową rolę w zarządzaniu kryzysowym odgrywa systematyczne szkolenie kadr kierowniczych, prowadzenie ćwiczeń oraz symulacja zagrożeń, bazująca na danych historycznych, tworząc scenariusze zbliżone do warunków panujących w czasie rzeczywistym[149]. Warto jednak podkreślić, że systemu zarządzania kryzysowego nie można zorganizować „raz na zawsze". System taki wymaga stałego doskonalenia poprzez rozwijanie go o nowe technologie[150]. Ważnym elementem w procesie doskonalenia Systemu Zarządzania Kryzysowego jest korzystanie z do-

[147] Z. Ciekanowski, S. Krysiński, Zarządzanie kryzysowe w Polsce w sytuacjach zagrożeń niemilitarnych jako sposób umacniania bezpieczeństwa państwa, PWSTE, Jarosław 2014, s. 37
[148] G. Sobolewski, Model *zarządzania przepływem informacji w sytuacjach kryzysowych*, Wydawnictwo: Akademia Obrony Narodowej, Warszawa 2013, s. 7.
[149] J. Pawłowski, Zarys teorii sytemu bezpieczeństwa państwa, Akademia Obrony Narodowej, Warszawa 2013, s. 9.
[150] Tamże s. 9.

świadczeń innych krajów. Poprzez wdrażanie nowych rozwiązań zwiększa się potencjał całej organizacji umożliwiający poprawę świadomości sytuacyjnej ludności. Odpowiednie rozpoznawanie zagrożeń oraz skutków z nimi związanych w połączeniu z wykorzystaniem Systemów Zarządzania Kryzysowego może rzutować na poprawę świadomości sytuacyjnej ludności nie tylko w momencie wystąpienia kryzysu, ale również może sprawić, że społeczeństwo będzie na nie lepiej przygotowane. Dlatego tak istotne jest udoskonalanie Systemu Zarządzania Kryzysowego, wzbogacając jego funkcjonalność poprzez modernizację bazy techniczno-technologicznej i wdrażanie nowych funkcji w istniejących rozwiązaniach. Akcentuje się zatem potrzebę pozyskiwania i wdrażania uniwersalnych rozwiązań oraz systemu zdolnego do skutecznej detekcji zagrożeń i możliwości prognozowania i planowania sposobów reagowania na zagrożenia. Istotne w tym procesie jest analiza i ocena aktualnych rozwiązań takich, jak Rządowe Centrum Bezpieczeństwa (RCB), Krajowy System Ratowniczo-Gaśniczy (KSRG), Obrona Cywilna Kraju (OCK) oraz innych elementów wchodzących w skład Systemu Zarządzania Kryzysowego, poszukując potencjalnie możliwych kierunków jego rozwoju z uwzględnieniem zwiększania możliwości kreowania pożądanego poziomu świadomości sytuacyjnej poprzez rozszerzenie jego funkcjonalności.

System Zarządzania Kryzysowego stanowi główny filar bezpieczeństwa Państwa i społeczeństwa w przypadku wystąpienia zagrożeń i obejmuje[151]:

- identyfikację i monitorowanie zagrożeń,
- określenie negatywnych skutków dla ludzi, mienia oraz infrastruktury krytycznej,
- ewaluację i ocenę ryzyka,
- określenie katalogu przedsięwzięć strukturalno-organizacyjnych i funkcjonalnych,
- określenie procedur postępowania na wypadek wystąpienia sytuacji kryzysowej,
- przygotowanie i utrzymanie niezbędnych sił i środków możliwych do wykorzystania,

[151] G. Sobolewski, *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, w: G. Sobolewski, D. Majchrzak (red.) *Wybrane zagadnienia zarządzania kryzysowego*, Warszawa 2012, s. 21.

- określenie zasad współdziałania podmiotów zaangażowanych podczas reagowania kryzysowego.

Jednym z warunków prawidłowego funkcjonowania Systemu Zarządzania Kryzysowego jest kategoryzacja zagrożeń, kreowanie świadomości sytuacyjnej na temat zagrożeń, wykorzystanie różnorodnych technologii, a także poznanie potrzeb ludności w zakresie ochrony przed zagrożeniami. Kolejnym, istotnym elementem prawidłowo funkcjonującego Systemu Zarządzania Kryzysowego jest dotarcie do ludności z informacją o zagrożeniu w formie dostosowanej do jak największej liczby odbiorców[152]. Ponadto, warunkiem sprawnie funkcjonującego SZK jest zapewnienie łączności oraz właściwe planowanie. Oznacza to, że są to komponenty wpływające na sposób i poziom uzyskiwania świadomości sytuacyjnej tak przez decydentów, jak i każdego obywatela i całe społeczeństwo lub lokalne społeczności. Art. 2 Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nakazuje tworzenie planów zarządzania kryzysowego na wszystkich szczeblach. Interesujące jest to, że według A. Skrabacz: „obecnie w Polsce nie istnieje system reagowania kryzysowego. Autorka uważa, że model zarządzania bezpieczeństwem na poziomie państwa jest nieefektywny, pozostający w gestii poszczególnych służb nadzorowanych przez premiera lub poszczególnych ministrów”[153]. Co więcej pomimo ustawy o zarządzaniu kryzysowym, w Polsce nadal nie ma efektywnego Systemu Zarządzania Kryzysowego. Istnieją wprawdzie elementy tego systemu, lecz nie funkcjonują spójnie jako całość, czego dowodem mogą być aktualne wydarzenia związane z incydentami na terenie RP (w tym nierozpoznane obiekty) i dlatego tak istotne jest wykorzystanie tradycyjnych i nowoczesnych technologii monitorowania i identyfikacji różnego typu źródeł zagrożeń oraz kreowanie świadomości sytuacyjnej obywateli w zakresie rozpoznawania, oceny i niwelowania skutków zagrożeń. W sytuacjach kryzysowych, a więc w fazach: zapobiegania, przygotowania, reagowania oraz odbudowy istotną rolę odgrywa wydajność systemu informowania ludności o zagrożeniach oraz radzenia sobie z zagrożeniami. W czasie zagrożeń kluczowe jest przygotowanie służb na zaistniałą sytuację oraz sposób radzenia sobie z nimi, a także możliwość obserwacji zachowań obywateli w celu określenia poziomu ich świadomości sytuacyjnej i uzupełniania luk stwierdzonych w działaniach rzeczywistych.

---

[152] W. Kitler, Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system, Akademia Obrony Narodowej, Warszawa 2011, s. 269.

[153] Kitler W., Skrabacz A., *Ochrona ludności i obrona cywilna w świetle współczesnych uwarunkowań bezpieczeństwa narodowego*, Wydawnictwo: AON, Warszawa 2009, s.199.

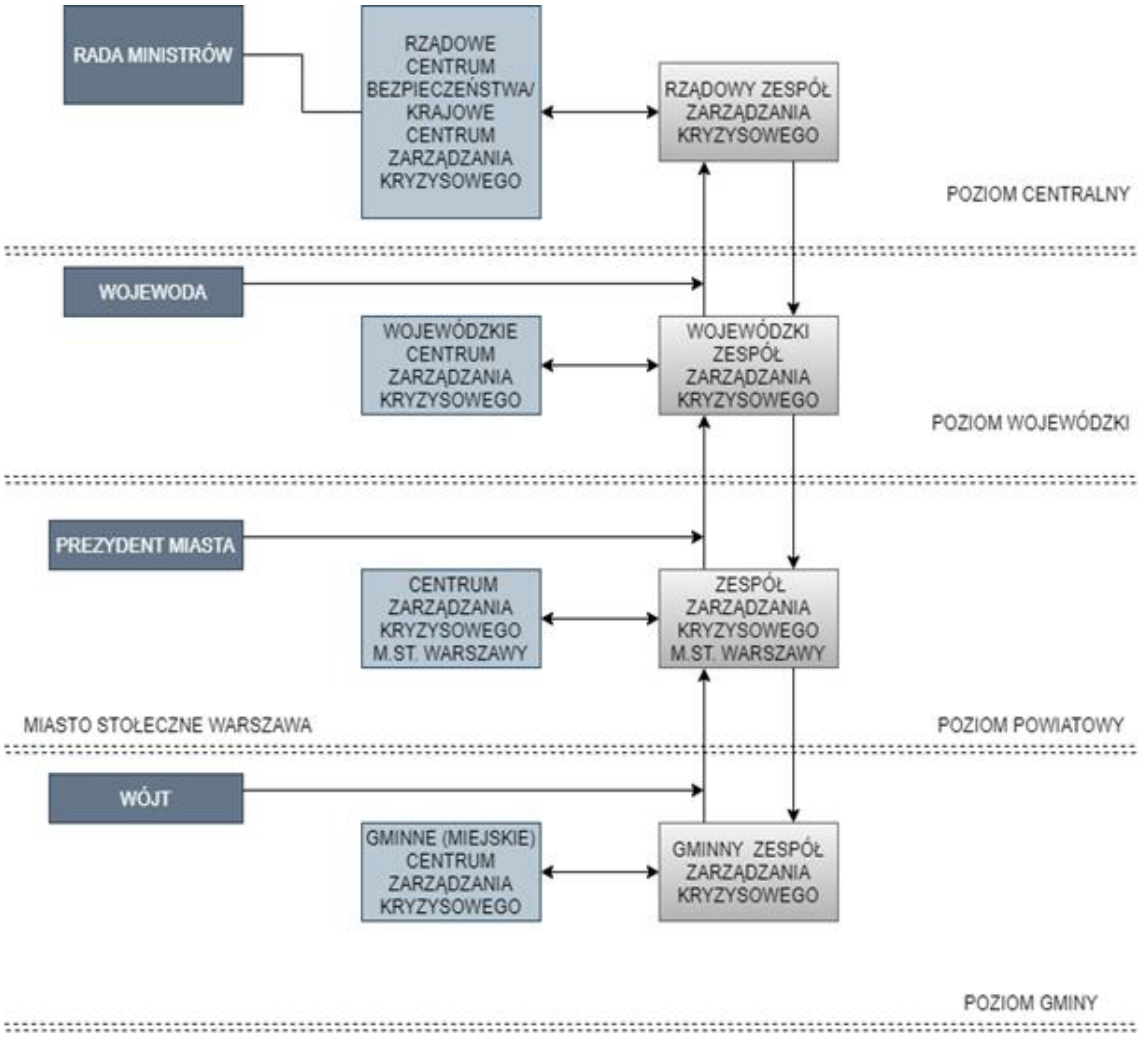
Zarządzanie kryzysowe jest działalnością organów administracji państwowej, wchodzącą w skład zarządzania bezpieczeństwem państwa. Polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu się do zarządzania nimi poprzez zaplanowane działania, reagowaniu na sytuacje kryzysowe, eliminowaniu ich skutków oraz odbudowie zasobów i infrastruktury krytycznej.[154]. Narastające zagrożenia w wielu obszarach funkcjonowania państwa tworzą nowe sytuacje kryzysowe, co wymaga podejmowania skoordynowanych działań. Pomimo rozwoju nowoczesnych technologii IT/ICT, te mogą okazać się nieskuteczne w przypadku niektórych klęsk żywiołowych i awarii technicznych. Ochrona ludności jest jednym z ważniejszych zadań w aspekcie bezpieczeństwa narodowego. Dlatego też w obliczu zagrożeń szczególnie takich, jak awarie techniczne czy zagrożenia wywołane na skutek działalności człowieka lub sił natury, niezbędne jest podjęcie kroków mających na celu ratowanie życia i zdrowia, ewakuacji ludności, zapewnienie poszkodowanej ludności podstawowych warunków przetrwania oraz zabezpieczenie mienia[155].

Zagwarantowanie oraz utrzymywanie stanu bezpieczeństwa jest jednym z głównych konstytucyjnych celów Państwa. W art. 5. Konstytucji RP jest mowa o tym, że Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli[156]. Realizując ten obowiązek Państwo powinno rozwijać istniejący SZK oraz poszukiwać nowych rozwiązań, niezbędnych do kreowania świadomości sytuacyjnej na temat zagrożeń w celu usprawnienia całej struktury zarządzania kryzysowego.

W Polsce obowiązującym dokumentem z zakresu zarządzania kryzysowego jest ustawa o zarządzaniu kryzysowym wydana 26 kwietnia 2007 roku. Wspomniana ustawa określa organy podejmujące decyzje w sprawach zarządzania kryzysowego, a także określa zasady ogólnego finansowania zadań kryzysowo-administracyjnych (w tym ogólno-społecznym i militarnym). Jak już wspomniano System Zarządzania Kryzysowego (rys. 3.2) posiada czteropoziomową strukturę (tab. 3.2) i jest ona powiązana ze szczeblami administracji publicznej[157].

---

[154] https://bezpieczna.um.warszawa.pl/zarzadzanie-kryzysowe (data dostępu : 01.10.2021).
[154] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590).
[155] B. Michailiuk, *Praca naukowo badawcza Korelacja systemu ochrony ludności z systemem zarzadzania*, D. Majchrzak, B. Michailiuk, J. Denysiuk, Warszawa, 2016, s. 9.
[156] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., (Dz. U. 1997, Nr 78, poz. 483 ze zm.).
[157] M. Górnikiewicz, T. Szczurek T. *Determinanty kształtowania bezpieczeństwa wewnętrznego*



Rysunek 3.2. System Zarządzania Kryzysowego w Polsce.

Źródło: opracowanie na podstawie Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 r., nr 89, poz. 590 z późn. zm.)

Tabela 3.2. Poziomy zarządzania kryzysowego w Polsce.

POZIOM 1	Prezes Rady Ministrów Minister Spraw Wewnętrznych I Administracji Minister Administracji I Cyfryzacji Rządowy Zespół Zarządzania Kryzysowego Rządowe Centrum Bezpieczeństwa Zespół Zarządzania Kryzysowego Ministerstw I Centralnych Organów Administracji Rządowej Zespół Zarządzania Kryzysowego Ministerstw I Centralnych Organów Administracji Rządowej
POZIOM 2	Wojewoda Wojewódzki Zespół Zarządzania Kryzysowego Wojewódzkie Centrum Zarzadzania Kryzysowego
POZIOM 3	Starosta Powiatowy Powiatowy Zespół Zarządzania Kryzysowego Powiatowe Centrum Zarządzania Kryzysowego
POZIOM 4	Wójt (Burmistrz, Prezydent Miasta) Gminny Zespół Zarządzania Kryzysowego Gminne Centrum Zarzadzania Kryzysowego

Źródło opracowanie własne

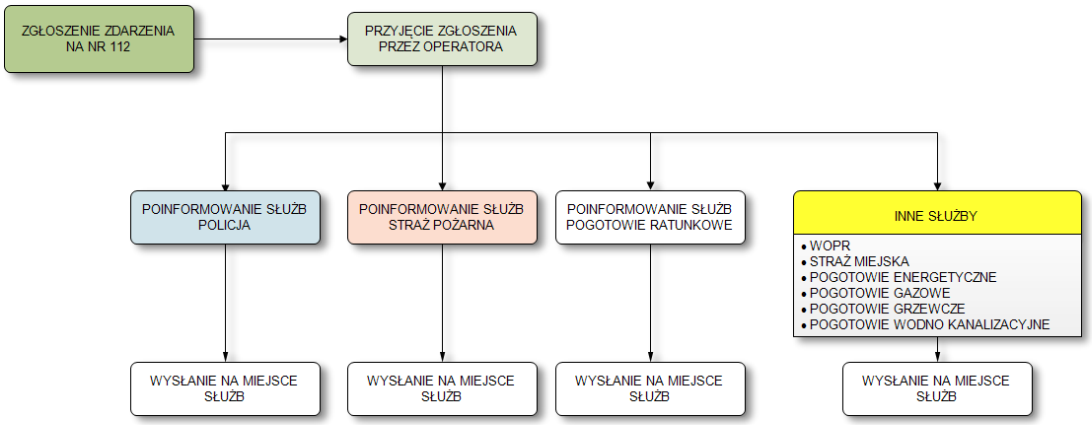
---

w: Ślachcińska E. (red.), Prognozowanie międzynarodowych stosunków wojskowych na podstawie uwarunkowań społeczno-kulturowych, , 2017, Poznań.

System zarządzania kryzysowego uruchamiany jest na poszczególnych poziomach administracyjnych (gminy, powiatu, województwa i centralnym) w zależności od obszaru, na którym wystąpiło zagrożenie. Ponadto można go również uruchomić, gdy wprowadzane są stopnie alarmowe lub stany nadzwyczajne.

System Powiadomienia Ratunkowego (SPR)

Zgodnie z ustawą z dnia 22 listopada 2013 r. o systemie powiadamiania (Dz.U. z 2019 r. poz. 1077) System Powiadamiania Ratunkowego (SPR) funkcjonuje jako kluczowy element zarządzania kryzysowego w Polsce. Wyżej wymieniona ustawa weszła w życie w Polsce 1 stycznia 2014 roku. oraz określa zasady i zadania Centrum Powiadomienia Ratunkowego w Polsce.. Zadaniem SPR jest obsługa komunikatów alarmowych wysyłanych na numery alarmowe (rys. 3.3), 112 (Centrum powiadomienia ratunkowego – jednolity ogólnoeuropejski numer alarmowy), 997 (Policja), 998 (Straż Pożarna), 999 (Pogotowie Ratunkowe), a następnie przekazanie ich do odpowiednich służb ratowniczych. W ramach systemu alarmowego mogą być również obsługiwane takie numery, jak: 991 (Pogotowie Energetyczne), 992 (Pogotowie Gazowe), 993 (Pogotowie Ciepłownicze), 994 (Pogotowie Wodno-Kanalizacyjne), 987 (Centrum Zarządzania Kryzysowego)i inne numery osób odpowiedzialnych. To. ochrona życia, zdrowia, porządku publicznego, środowiska lub mienia oraz bezpieczeństwo. Znajomość wspomnianych kontaktów jest bardzo ważną częścią świadomości sytuacyjnej, która wspomaga proces identyfikacji i reagowania na różnego rodzaju zagrożenia.



Rysunek 3.3. Proces zgłoszenia zdarzenia na numer alarmowy 112

Źródło: Opracowanie własne.

Na rysunku 3.3. przedstawiony jest schemat przyjęcia zgłoszenia na numer alarmowy 112. Cały proces rozpoczyna się od zgłoszenia informacji o rodzaju zagrożenia. Następnie operator przekazuje dane o zagrożeniu do odpowiednich służb ratunkowych. Operator przyjmujący zgłoszenie w przypadku osób kontaktujących się z telefonu komórkowego automatycznie uzyskuje dane takie jak[158]:

- współrzędne geograficzne,
- numer osoby dzwoniącej,
- dane osoby, na którą został zarejestrowany telefon komórkowy.

W przypadku zgłoszenia zdarzenia z telefonu stacjonarnego operator przyjmujący zgłoszenie otrzymuje takie informacje, jak: adres i dane osoby, na którą telefon został zarejestrowany. Zaletą systemu jest niewątpliwie identyfikacja numerów zastrzeżonych. Operatorzy bardzo szybko są w stanie rozpoznać fałszywe, niezasadne oraz złośliwe połączenia, które stanowią około 83% wszystkich połączeń kierowanych na numer 112. Ta konstatacja może wskazywać na niski poziom świadomości sytuacyjnej naszego społeczeństwa i potrzebę stałego uświadamiania o powstawaniu dodatkowego zagrożenia opóźniania ważnych i niezbędnych działań w przypadku „zamulania" przepływów informacyjnych nieużytecznymi informacjami. Ważna jest jednak tutaj możliwość podnoszenia niezawodności systemu komunikowania się, gdy nastąpi awaria jednego z Centrów Powiadomień Ratunkowych lub w momencie, gdy liczba połączeń w danym województwie przekracza możliwości szybkiej obsługi, to połączenia te zostają przekierowywane do innego województwa[159].

Do zadań realizowanych w zakresie CPR należą[160]:

1) obsługa zgłoszeń alarmowych kierowanych na numer 112, w tym:
   - odbiór zgłoszenia alarmowego,
   - powiązanie zgłoszenia alarmowego z danymi teleadresowymi miejsca zgłoszenia oraz jego pozycją geograficzną,
   - wybór odpowiedniej grupy podmiotów, do której zostaną skierowane zgromadzone dane o zgłoszeniu alarmowym,
   - przekazywanie zebranych informacji drogą elektroniczną z wykorzystaniem systemu teleinformatycznego oraz, w uzasadnionych przypad-

[158] J. Piwowarski, *Polska droga od filozofii bezpieczeństwa do nauk o bezpieczeństwie i kultury bezpieczeństwa*, w. M. Kubiak (red.), *Konteksty bezpieczeństwa personalnego i strukturalnego – jedność w różnorodności*, 2021.
[159] Tamże.
[160] Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego.

kach, wraz z przekierowaniem połączenia telefonicznego zgodnie z ważnością zgłoszenia, Policji, Państwowej Straży Pożarnej i dysponentów zespołów ratownictwa medycznego lub do podmiotów, których numery przetwarzane są w systemie,

- wymiana informacji o zgłoszeniach alarmowych przetwarzanych w systemie teleinformatycznym w zakresie określonym w art. 5 ust. 6 pkt 4 oraz art. 13 ust. 3 pkt 3 ustawy o Systemie Powiadamiania Ratunkowego z Policją, Państwową Strażą Pożarną, dysponentami zespołów ratownictwa medycznego lub innymi jednostkami, których numery telefonów wykorzystywane są w systemie.

2) zapisywanie i przechowywanie w systemie teleinformatycznym przez okres 3 lat informacji o treści zgłoszeń alarmowych, w tym nagrań rozmów telefonicznych obejmujących całość zgłoszenia alarmowego, danych sygnalistów i innych osób zgłoszonych w związku z otrzymaniem zgłoszenia, informacji o miejscu i rodzaj wydarzenia oraz krótki opis wydarzenia.
3) przeprowadzanie analiz związanych z funkcjonowaniem systemu powiadamiania ratunkowego na obszarze obsługiwanym przez centrum oraz sporządzanie statystyk dotyczących liczby, rodzaju i czasu trwania zgłoszeń alarmowych.
4) współpraca i wymiana informacji z ośrodkami zarządzania kryzysowego określonymi w ustawie o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz. U. z 2013 r., poz. 1166),
5) wymiana informacji i danych, z wyjątkiem danych osobowych, do analizy przez Policję, Strażą Pożarną, dysponentów zespołów ratownictwa medycznego oraz jednostki, których numery telefonów zostały uwzględnione w systemie,
6) jeżeli dokonanie zgłoszenia alarmowego nie jest możliwe w systemie i jeżeli jest to uzasadnione charakterem zgłoszenia, podjęcia działań zmierzających do przekazania informacji o tym zgłoszeniu podmiotom, do których zadań należy ochrona życia, zdrowia, bezpieczeństwa i porządku publicznego, mienia lub środowiska i których numery telefonów . nie są przechowywane w systemie.

System obsługi zgłoszeń alarmowych obsługuje również zgłoszenia kierowane do SPR za pośrednictwem wiadomości tekstowych *SMS*, co jest szczególnie użyteczne w momencie, gdy werbalny sposób kontaktu jest utrudniony.

Krajowy System Ratowniczo Gaśniczy (KSRG)

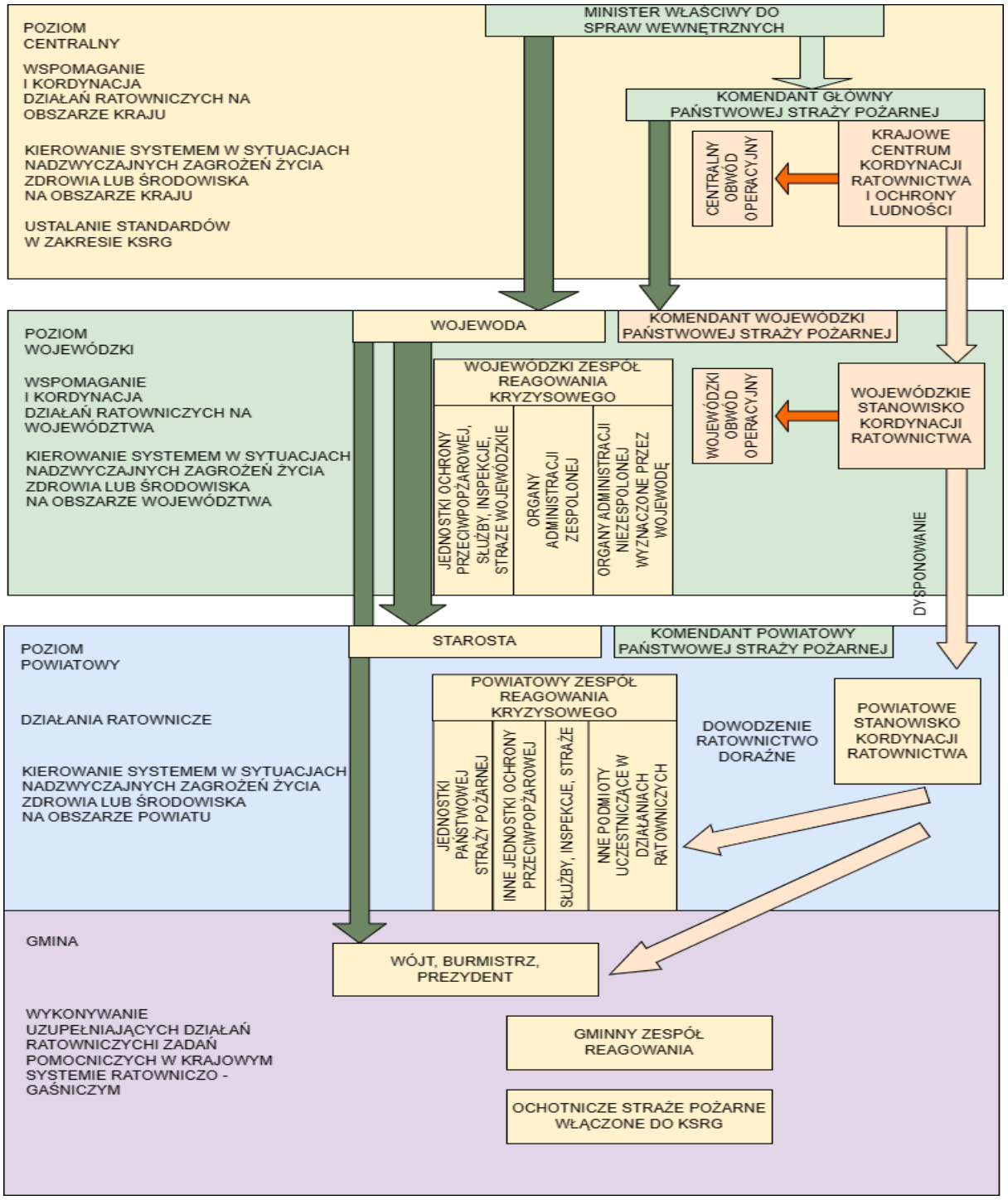
Podstawą do stworzenia Krajowego Systemu Ratowniczo-Gaśniczego była ustawa o ochronie przeciwpożarowej[161] oraz ustawa o Państwowej Straży Pożarnej [162]. Działalność KSRG jest bezpośrednio związana z ratowaniem życia, zdrowia, mienia i środowiska przed klęskami żywiołowymi, awariami technicznymi i katastrofami spowodowanymi przez człowieka. System ten stanowi integralną część organizacji bezpieczeństwa wewnętrznego państwa i jego działania obejmują ratowanie życia, zdrowia, mienia lub środowiska, prognozowanie, wykrywanie i zwalczanie pożarów, klęsk żywiołowych lub innych lokalnych zagrożeń. System ten zrzesza jednostki ochrony przeciwpożarowej, inne służby, inspekcje, ochronę, instytucje i społeczności, które dobrowolnie zobowiązały się do współpracy w akcjach ratowniczych na podstawie umowy cywilnej [163] .

W lipcu 1992 na mocy ustawy z dnia. 24 sierpnia 1991 o ochronie pożarowej oraz ustawy z dnia 24 sierpnia 1991 o Państwowej Straży Pożarnej[164] przekształcono zawodową straż pożarną w państwową straż pożarną, której powierzono rolę zorganizowania Krajowego Systemu Ratowniczo-Gaśniczego (rys. 3.4). W ramach przygotowania jednostek KSRG do prowadzenia działań z zakresu ratownictwa medycznego realizowane są działania takie jak szkolenie z zakresu udzielania pierwszej pomoc oraz przystosowanie niezbędnego sprzętu. do ratowania zdrowia i życia ludzi, w zależności od rodzaju i miejsca zdarzenia oraz liczby osób zagrożonych[165].

W tym względzie bardzo ważne jest zapewnienie ciągłości procesu i właściwych procedur zapewniających poszkodowanym profesjonalną i kompleksową opiekę medyczną.

---

[161] Ustawa o ochronie przeciwpożarowej (Dz.U. 1991 nr 81 poz. 351)
[162] Ustawa o Państwowej Straży Pożarnej (Dz. U. 1991 Nr 88 poz. 400
[163] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, (Dz. U. z 2017 r., poz. 736 (z późn. zm.)
[164] Tamże.
[165]J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego. Część 1. Zarządzanie kryzysowe w administracji publicznej*, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010., s. 193–204



Rysunek 3.4. Schemat blokowy Krajowego Systemu Ratowniczo-Gaśniczego

Źródło: opracowanie własne na podstawie: Wymiana dobrych praktyk oraz analiza porównawcza aktów prawnych dla pracowników administracyjnych JST odpowiedzialnych za funkcjonowanie jednostek OSP pogranicza polsko-słowackiego (dostęp na stronie https://wsb.edu.pl/files/pages/3276/materialy_10_11_pl.pdf)

Obecny stan prawny KSRG ustalany jest na podstawie zarządzenia Ministra Spraw Wewnętrznych i Administracji. z dnia 18 lutego 2011 r [166]. Do zadań realizowanych w ramach KSRG należy[167]:

- gaszenie pożarów,
- eliminowanie lokalnych zagrożeń (działania ratownicze),
- ratownictwo chemiczne i ekologiczne,
- ratownictwo techniczne,
- ratownictwo medyczne w zakresie udzielania kwalifikowanej pierwszej pomocy.

KSRG funkcjonuje na wszystkich szczeblach w kraju (poziom centralny, województwo, powiat, gmina), co powoduje, że niezbędne jest ujenolicenia realizacji działań interwencyjnych przez jednostki zlokalizowane w różnych częściach kraju poprzez wdrożenie jednolitego systemu informacyjnego; standaryzacja wdrażanych urządzeń i ujednolicenie technologii, wymienność ról w działaniach ratowniczych[168].

Spełnienie powyższych kryteriów, co stanowi istotę KSRG, umożliwia pełną współpracę i podporządkowanie służb i jednostek ratowniczych dla osiągnięcia jednego celu, którego celem jest kompleksowe i skuteczne ratowanie życia i zdrowia.

System Obrony Cywilnej (SOC)

System Obrony Cywilnej (SOC) Polski funkcjonuje w oparciu o ustawę o powszechnym obowiązku obrony z dnia 21 listopada 1967 r. (z późn. zm.).[169].

Za obronę cywilną w kraju opowiada Komendant Główny Państwowej Straży Pożarnej. Do obowiązków kierowników ochrony ludności na szczeblu gminnym, powiatowym i wojewódzkim należy sporządzanie planów obrony cywilnej oraz wydawanie aktów prawnych, które stanowią główne instrukcje. gdy populacja jest zagrożona. Szefem obrony cywilnej na szczeblu wojewódzkim jest wojewoda, na powiatowym lub miejskim na prawach powiatu– starosta lub prezydent miasta, na szczeblu gminnym – burmistrz, wójt, prezydent miasta. Głównymi jednostkami systemu są:[170]

- formacje Obrony Cywilnej, składające się z oddziałów przeznaczonych do wykonywania zadań ogólnych,

[166] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego.
[167] Tamże.
[168] J. J. Skoczylas, *Prawo ratownicze, wyd. 2*, LexisNexis, Warszawa 2011, s. 57–58.
[169] Tamże.
[170] Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej.

- jednostki specjalne, np. ratownictwa.

Jednostki te tworzone są na mocy decyzji lokalnych organów administracji i pracodawców[171].

W pierwszej fazie odpowiedzialność za ochronę ludności w Polsce ponoszą:

1) Służby ratownicze, a w szczególności:
   - Państwowa Straż Pożarna.
   - Państwowe Ratownictwo Medyczne.
2) Organizacje ratownicze i humanitarne o charakterze społecznym, a zwłaszcza:
   - Górskie Ochotnicze Pogotowie Ratunkowe.
   - Tatrzańskie Ochotnicze Pogotowie Ratunkowe.
   - Wodne Ochotnicze Pogotowie Ratunkowe.
   - Polski Czerwony Krzyż.
3) Służby ochrony bezpieczeństwa i porządku publicznego, a w szczególności:
   - Policja.
   - Straż Miejska.

Pomimo, iż ochrona wpływa bezpośrednio na instytucje publiczne, niektóre działania z nią związane mogą mieć także charakter indywidualny i dotyczyć każdego obywatela. Do takich działań zalicza się[172]:

- poznawanie i akceptowanie zasad ewakuacji,
- rozpoznawanie sygnałów alarmowych oraz ostrzegawczych,
- poznawanie zasad zachowania się na wypadek ogłoszenia alarmu,
- indywidualne środki ochrony przed zanieczyszczeniem,
- informacje na temat sposobu zabezpieczenia majątku,
- informacje dotyczące pierwszej pomocy,
- przeciwdziałanie zagrożeniom.

Zgodnie z ustawą z dnia 21 listopada 1967 r. zadania realizowane przez System Obron Cywilnej można podzielić na zadania wykonywane w czasie pokoju oraz wojny. Do tych pierwszych zalicza się m.in.

[171] Tamże.
[172] Tamże.

- planowanie przedsięwzięć dotyczących ochrony ludności, miejsc pracy, mienia publicznego i dóbr kultury przed skutkami działań zbrojnych,
- wykrywanie zagrożeń i stwarzanie warunków do ostrzegania i alarmowania mieszkańców,
- przygotowanie schronów i ukryć dla ludności oraz utrzymanie ich w gotowości do użycia,
- gromadzenie i przechowywanie środkow ochrony indywidualnej dla formacji Obrony Cywilnej i ludności,
- wyposażenie formacji Obrony Cywilnej w specjalny sprzęt ratowniczy, oraz środki do wykrywania zagrożeń,
- systematyczne szkolenie kadr administracyjnych administracji państwowej i samorządowej, formacji OC oraz ludności w zakresie samoobrony powszechnej,
- współpraca na rzecz zwalczania klęsk żywiołowych i zagrożeń środowiska, oraz eliminowania ich skutków.

Do obowiązków wykonywanych w czasie wojny należy m.in. [173]:

- zorganizowanie ewakuacji ludności, zaciemnianie i wygaszanie oświetlenia,
- organizować i przeprowadzać akcje ratownicze, zapewniając rannym opiekę medyczną,
- organizowanie pomieszczeń i zaopatrzanie poszkodowanej ludności,
- zapewnienie ludności sprzętu oraz środków ochrony indywidualnej,
- eliminacja skażeń i zanieczyszczeń,
- pomoc w przywracaniu i utrzymaniu porządku na terenach dotkniętych klęskami,
- pomoc w budowie oraz przebudowie awaryjnych punktów poboru wody pitnej,
- pomoc w ratowaniu żywności i innych rzeczy niezbędnych do przeżycia,
- udzielanie niezbędnej pomocy przy pochówku zmarłych,

Odpowiedzialność za prawidłowe administrowanie tym obszarem dla zapewnienia bezpieczeństwa Polski należy do Obronie Cywilnej Kraju.

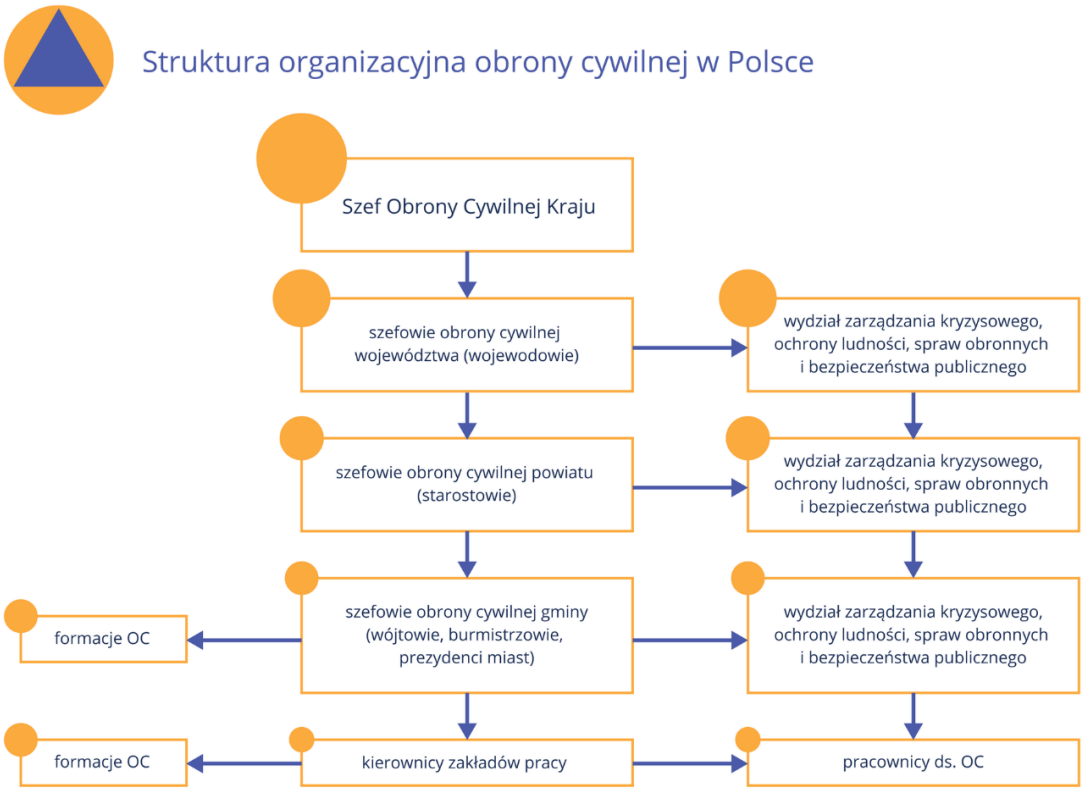
Zadaniem szefów Obrony Cywilnej na szczeblu wojewódzkim, gminnym i powiatowym jest przygotowywanie i wydawanie oświadczeń w sprawie planów obrony cywilnej, które stanowią kluczową instrukcję dla władz cywilnych w sytuacji kryzysowej.

[173] Tamże.

Centralnym organem administracji publicznej jest szef Obrony Cywilnej, do którego zadań należy[174]:

- przygotowywanie planów działań na rzecz Obrony Cywilnej,
- wzmocnienie ogólnych zasad niezbędnych do realizacji Obrony Cywilnej,
- koordynacja projektów specjalnych i nadzór nad zadaniami władz państwowych i samorządowych,
- nadzór nad odbywaniem służby w ramach Obrony Cywilnej.

Dowódcami terenowymi jednostek Obronny Cywilnej są starostowie, wójtowie, burmistrzowie, prezydenci miast, wojewodowie (rys. 3.5).



Rysunek 3.5. Struktura organizacyjna obrony cywilnej w Polsce

Źródło:https://epodreczniki.pl/a/zadania-obrony-cywilnej-i-ochrona-ludnosci/Dkf7nISSZ

Do zadań szefów Obrony Cywilnej należy określanie zadań do realizacji w ramach Obrony cywilnej, kontrolowanie ich wykonania oraz kierowanie działalnością jednostek niższego szczebla .

[174] Tamże.

Wojska Obrony Terytorialnej (WOT)

Wojska Obrony Terytorialnej zostały utworzone 16 listopada 2016 roku w drodze zmiany ustawy o ogólnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Zadania WOT obejmują np.: realizacja działań obronnych we współpracy z siłami operacyjnymi i elementami pomocniczymi systemu pozamilitarnego, prowadzenie samodzielnych działań niekonwencjonalnych, przeciw dywersyjnych i przeciwdesantowych, udział w zabezpieczeniu przyjęcia i rozwinięcia sojuszniczych sił wzmocnienia w nakazanych rejonach, realizacja projektów w obszarach: zarządzania kryzysowego, zwalczania klęsk żywiołowych i usuwania ich skutków, ochrony mienia, działań poszukiwawczo-ratowniczych, realizacja działań informacyjnych.

Wojska Obrony Terytorialnej są najmłodszą formacją Sił Zbrojnych RP, utworzoną 1 stycznia 2017 roku, a dokument prawnie potwierdzający jej utworzenie jest datowany na 16 listopada 2016 r. Ustawa RP o powszechnym obowiązku obrony RP. Wojska Obrony Terytorialnej są samodzielnym rodzajem Sił Zbrojnych Rzeczypospolitej Polskiej i nie podlegają Ministerstwu Spraw Wewnętrznych i Administracji (MSWiA) tylko Ministrowi Obrony Narodowej (MON). Dowódca WOT jest właściwy w zakresie dowodzenia formacjami wojskowymi i związkami organizacyjnymi tych wojsk w czasie sytuacji kryzysowej, pokoju i wojny. Działania informacyjne realizowane przez WOT koncentrują się na przekazywaniu informacji w sposób zrozumiały dla potencjalnego odbiorcy przy wykorzystaniu potencjału mediów społecznościowych[175]. Można uznać, że jest to komponent wzmacniający system kreowania świadomości sytuacyjnej dla uprawnionego odbiorcy.

3.4. Rządowe Centrum Bezpieczeństwa (RCB) i jego funkcje

Rządowe Centrum Bezpieczeństwa to jednostka budżetowa, która podlega Prezesowi Rady Ministrów. Strukturą RCB zarządza dyrektor przy pomocy zastępców oraz kierowników, a także komórek organizacyjnych. Centrum to zostało utworzone 26 kwietnia 2007 r. na podstawie ustawy o zarządzaniu kryzysowym[176], ale rozpoczęło działalność 2 sierpnia 2008 r. Sposób działania RCB określa Rozporządzenie Prezesa Rady Ministrów z dnia 24 marca 2015 r. w sprawie publikacji tekstu jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa. Celem utworzenia RCB było

[175] https://terytorialsi.wp.mil.pl/faq/struktura-i-zadania (data dostępu : 13.10.2021).
[176] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590).

stworzenie funkcjonującego systemu zarządzania kryzysowego, do którego zadań należy zapobieganie kryzysom oraz minimalizowanie i eliminowanie skutków zagrożeń w przypadku ich wystąpienia[177].

Rządowe Centrum Bezpieczeństwa pełni funkcję organu wykonawczego jako krajowego centrum zarządzania kryzysowego. Do głównych zadań RCB, które mają wpływ na procesy informowania ludności w sytuacjach kryzysowych, należą[178]:

- Monitoring, klasyfikacja i analiza zagrożeń,
- opracowywanie racjonalnych/skutecznych rozwiązań, które pojawiają się w sytuacjach kryzysowych,
- przepływ informacji dotyczących zagrożeń,
- wdrażanie procedur zarządzania kryzysowego,
- planowanie działań mających na celu ochronę infrastruktury krytycznej,
- nadzór nad spójnością procedur reagowania kryzysowego,
- organizacja szkoleń mających na celu przygotowanie się na zagrożenie - ważny komponent wzrostu świadomości sytuacyjnej),
- realizacja zadań mających na celu zapobieganiu oraz likwidowaniu skutków zagrożeń,
- współpraca międzynarodowa ze szczególnym uwzględnieniem państw członkowskich NATO oraz UE.

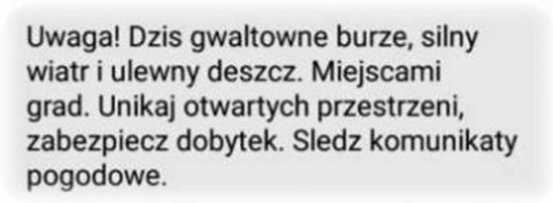
Rządowe Centrum Bezpieczeństwa zapewnia również prezesowi Rady Ministrów, Radzie Ministrów oraz Rządowemu Zespołowi Zarządzania Kryzysowego niezbędne wsparcie w procesie podejmowania decyzji w obszarze szeroko rozumianego bezpieczeństwa, a także dostarcza opracowania i analizy. Stąd wypływa ważna rola RCB a mianowicie kształtowanie świadomości sytuacyjnej decydentów szczebla strategicznego. W zależności od sytuacji kryzysowej Rządowe Centrum Bezpieczeństwa monitoruje i analizuje zaistniałe zagrożenie, współpracując z instytucjami krajowymi oraz międzynarodowymi, w zależności od skali zagrożenia. Dzięki nowelizacji ustawy z dnia 12 grudnia 2018 roku o prawie telekomunikacyjnym zostało stworzone nowe

[177] Obwieszczenie Prezesa Rady Ministrów z dnia 24 marca 2015 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa.
[178] Tamże.

narzędzie do informowania o zagrożeniach – Alert RCB, dzięki któremu możliwe jest ostrzeganie osób, które znajdują się na zagrożonym terenie[179].

Alert RCB powstał na kanwie katastrofy z 2017 roku, w której dwie harcerki zginęły na obozie w Suszku. Aktualne rozwiązania mające na celu informowanie ludności w sytuacjach kryzysowych bazują na systemie SMS-owym, wprowadzonym przez Rządowe Centrum Bezpieczeństwa. Informacje o wystąpieniu zdarzenia, które zagraża życiu lub zdrowiu, przekazywane są przez RCB do wszystkich osób użytkujących telefony komórkowe bez wcześniejszej konieczności ich rejestracji oraz bez względu na to, w jakiej sieci komórkowej znajduje się telefon i bez wymogu posiadania specjalnej aplikacji. Ponadto, Alert z Rządowego Centrum Bezpieczeństwa wysyłany jest do wszystkich użytkowników telefonów komórkowych niezależnie od generacji telefonu. RCB przekazuje w formie wiadomości tekstowej SMS informacje o zagrożeniu wszystkim osobom znajdującym się na obszarze, w którym może wystąpić sytuacja zagrażająca bezpośrednio życiu lub zdrowiu. Jedyny warunek otrzymania wiadomości w formie tekstowej wraz z krótkimi zaleceniami jak postępować to aktywny w sieci telefon komórkowy[180]. Warto jednak podkreślić, że tego typu rozwiązanie ma swoje wady w postaci ograniczonej liczby znaków (SMS – 160). Organem odpowiedzialnym za wysłanie komunikatów nie jest Rządowe Centrum Bezpieczeństwa, tylko operator sieci. RCB nie gromadzi danych o użytkownikach i odpowiada tylko za utworzenia komunikatu oraz podjęcia decyzji, na który obszar ma zostać ten komunikat wysłany. Alert RCB o zagrożeniu powstaje na podstawie zgromadzonych informacji o możliwych zagrożeniach, które Rządowe Centrum Bezpieczeństwa otrzymuje od takich służb jak: Policja, Straż pożarna, Straż graniczna, urzędy oraz instytucje centralne, urzędy wojewódzkie ministerstwa oraz Instytut Metrologii i Gospodarki Wodnej[181]. Początkowo najmniejszym regionem, na który były wysyłane komunikaty o zagrożeniach było województwo, ale z dniem 12 grudnia 2018 r. po – zmianie prawa telekomunikacyjnego alerty RCB wysyłane są do mieszkańców powiatów, na których występuje zagrożenie. Treść komunikatu zawiera dane o rodzaju zagrożenia oraz zalecania jak się zachować w momencie jego wystąpienia (rys. 3.6).

[179] Ustawa z dnia 10 maja 2018 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. 2018 poz. 1118).
[180] http://rcb.gov.pl/wp-content/uploads/KPZK-cz.3.pdf (dostęp: 02.07.2021 r.).
[181] https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi (data dostępu 22.04.2021).



Rysunek 3.6. Przykładowy alert RCB

Źródło: Alert otrzymany od RCB przez autora rozprawy (w dn. 17.08.2021)

Aby każda osoba wyposażona w telefon komórkowy, niezależnie od tego, czy jest starszej czy nowej generacji, mogła odczytać komunikat o zagrożeniu, został przyjęty schemat wysyłania wiadomości bez polskich znaków - dzięki czemu przy dłuższym komunikacie nie zamienia się on automatyczne w MMS i możliwe jest przekazanie większej liczby informacji. Alerty RCB wysyłane są tylko w wyjątkowych sytuacjach, gdy występuje bardzo duże zagrożenie życia lub zdrowia. Dane osobowe użytkowników telefonów, na które są przesyłane alerty nie są w żaden sposób gromadzone i przetwarzane przez RCB. Przyjęta w Polsce forma powiadamiania o zagrożeniach oparta o SMS-owy system ostrzegania jest obecnie najskuteczniejszą metodą informowania oraz ostrzegania i informowania o zagrożeniach[182]. Sam proces powiadamiania od strony technicznej jest mało złożonym przedsięwzięciem, jednak z punktu widzenia wiarygodności i aktualności treści bardzo duże znaczenie ma status źródła, na podstawie którego opracowywany jest komunikat alertowy. Stąd tak duże znaczenia mają systemy i narzędzia IT/ICT pozyskujące ten sam rodzaj informacji z wielu heterogenicznych źródeł, porównywanej i statystycznie potwierdzonej do użytku pod względem przydatności i wiarygodności oraz aktualności treści dla potencjalnych adresatów.

Warto pamiętać, że nie da się przewidzieć i zapobiec wszystkim zdarzeniom. Często zdarza się tak, że lokalne zagrożenia mogą stanowić bezpośrednie niebezpieczeństwo dla życia lub zdrowia. Bez względu na to, czy obywatel otrzyma alert komunikat z RCB, należy przestrzegać zasad bezpieczeństwa dostosowanych do zagrożenia w jakim się znaleźliśmy i zachować zdrowy rozsądek. Ważną zaletą Alertów RCB jest to, że swoim obszarem obejmują również obcokrajowców przebywających w Polsce korzystających z zagranicznych sieci komórkowych, a także Polaków przebywających za granicą. Wysłanie komunikatu RCB do Polaków za granicą,

[182] Tamże.

oprócz możliwości ostrzeżenia ich o zagrożeniu, pozwala również na oszacowanie ich liczby, co może w znaczny sposób ułatwić proces ich ewakuacji. Monitorowanie obszaru całego kraju na wypadek wystąpienia potencjalnych zagrożeń odbywa się przez 24 godziny na dobę 7 dni w tygodniu, a jeśli pojawi się potencjalne zagrożenie, wysyłany jest Alert.

Zasadę funkcjonowania alertów RCB reguluje ustawa o zarządzaniu kryzysowym (Dz. U. 2019 poz. 1398)[183]:

1) Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują dyrektora Centrum o zagrożeniu, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej, oraz o konieczności powiadomienia ludności o zagrożeniu.
2) Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej niezwłocznie informują dyrektora Centrum oraz właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.
3) Operator ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954, 2245 i 2354 oraz z 2019 r. poz. 643, 730 i 1030), zwany dalej „operatorem”, jest obowiązany do niezwłocznego, nieodpłatnego wysłania, na żądanie dyrektora Centrum, komunikatu do wszystkich użytkowników końcowych na określonym przez niego obszarze.
4) Rada Ministrów określa w drodze rozporządzenia, sposób i tryb współpracy dyrektora Centrum z operatorem w celu realizacji obowiązku, o którym mowa w ust. 3 ustawy i zarządzaniu kryzysowym[184], niezbędne elementy komunikatu oraz sposób jego przekazania użytkownikom końcowym, mając na uwadze konieczność:
    - zapewnienia efektywnego i niezakłóconego przepływu informacji między Centrum a operatorem,

[183] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 5 lipca 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Dz. U. 2019 poz. 1398).
[184] Tamże.

- zapewnienia sprawnej dystrybucji komunikatu na obszarze zagrożonym wystąpieniem sytuacji kryzysowej oraz łatwości zrozumienia treści zawartych w komunikacie i zastosowania się do nich.

Wyżej wymieniona ustawa narzuca na operatorów sieci obowiązek przesłania alertu wszystkim obywatelom znajdującym się w obszarze wskazanym przez dyrektora RCB. Komunikaty wysyłane są bez zgody użytkownika, ponieważ są to działania występujące w sytuacjach wyższej konieczności spowodowanej zagrożeniem życia lub zdrowia.

Oprócz przesyłania przez RCB w formie SMS-owej oraz zamieszczania informacji w mediach o zagrożeniach, wykorzystywane są inne metody informowania ludności o sytuacjach kryzysowych. W celu powiadomienia ludności często wykorzystuje się transport publiczny oraz pojazdy służb ratowniczych jako swoiste forum publikacyjne. Niemniej jednak w środkach transportu publicznego pojawią się głównie informacje dotyczące restrykcji wprowadzonych w trakcie wystąpienia zagrożenia, czy też informujące o zagrożeniach, na które obywatele są narażeni, wybierając tę formę transportu. Wykorzystanie potencjału technologii używanych w środkach transportu publicznego może przyczynić się do poprawy świadomości sytuacyjnej ludności o zagrożeniach. W przypadku służb ratowniczych zarówno w trakcie przygotowania się do zagrożenia, jak i podczas jego trwania, służby ratownicze wykorzystują swój sprzęt w celu informowania ludności, np. poprzez rozpowszechnianie przez megafony komunikatów głosowych o środkach ostrożności i o tym, jak należy się zachować w danej sytuacji.

Od 2022 r. na mocy porozumienia Rządowego Centrum Bezpieczeństwa z firmą *Screen Network S.A.* komunikaty o nadchodzących zagrożeniach wyświetlane są na ekranach reklamowych w przestrzeni miejskiej, a założeniem wspomnianego rozwiązania jest zwiększenie skuteczności informowania ludności na temat nadchodzących zagrożeń. Wykorzystanie tego typu technologii zwiększa funkcjonalność Rządowego Centrum Bezpieczeństwa, które oprócz komunikatów wysyłanych na telefony komórkowe wzbogaca proces informowania ludności na temat zagrożeń w postaci zobrazowanej na ekranach wielkoformatowych, na których wyświetlane są informacje o aktualnych zagrożeniach. Niemniej jednak tę funkcjonalność można istotnie rozszerzyć o dodatkowe funkcje (Rozdział VI)[185].

[185] https://screennetwork.pl/alert-rcb-ekrany-reklamowe/ (data dostępu 23.09.2022).

3.5. Ocena funkcjonowania polskiego SZK w kontekście kształtowania świadomości sytuacyjnej

Ogólna analiza i ocena Systemu Zarządzania Kryzysowego w Polsce prowadzi do konkluzji o różnych lukach i wadach w jego funkcjonowaniu. Takie stwierdzenie jest upoważnione dzięki analizie przeprowadzonej przez Najwyższą Izbę Kontroli (NIK), która oceniając ważny komponent tego systemu, jakim jest Obrona Cywilna Kraju (OCK) uważa jej strukturę i organizację jako anachroniczną. Liczba formacji OCK jest nieadekwatna do zidentyfikowanych zagrożeń i z każdym kolejnym rokiem maleje. Ponadto, sprzęt wykorzystywany przez OCK został oceniony jako niekompletny i przestarzały a część sprzętu pochodzi z lat 50 i 60 ubiegłego wieku. Jako przyczynę nieprawidłowości w działaniu OCK, którą wskazał NIK, są wieloletnie zaniedbania, brak kompleksowych uregulowań prawnych, lekceważenie planów, procedur i struktur na wypadek wystąpienia zagrożeń oraz niewystarczające finansowanie zadań[186].

Kluczową rolą w działaniu Obrony Cywilnej powinno być to, aby miała powszechny charakter. W tym celu należy stworzyć odpowiednią formułę, która pomoże obywatelom zdobyć niezbędną wiedzę i umiejętności. Wiedza ta powinna dotyczyć zarówno wiedzy o udzielaniu pierwszej pomocy jak i na temat tego, jak się zachować w momencie zaistnienia sytuacji kryzysowej. Tego typu rozwiązanie powinno przewidywać zatem przeszkolenie maksymalnej liczby osób w taki sposób, aby były one w stanie utworzyć pewien system, którego zadaniem byłoby nie tylko kształtowanie świadomości sytuacyjnej na odpowiednim poziomie, ale umiejętność wykorzystania tej sprawności. Ponadto w momencie zaistnienia sytuacji kryzysowej powinni oni mieć odpowiednią świadomość na temat tego, gdzie się mają zgłosić i jakie zadania są im przydzielone.

Przy założeniu, że przeszkolone osoby zgłoszą się do wykonania przydzielonych im zadań w ramach wolontariatu, to zbudowanie odpowiedniego systemu wspierającego zarządzanie kryzysowe oraz proces informowania ludności o zagrożeniach wiąże się z kosztami takimi jak np. prowadzenie i finasowanie szkoleń. Aktualnie istniejący system OCK nie funkcjonuje prawidłowo, a jego rolę częściowo przejęły Wojska Obrony Terytorialnej (WOT), co pokazała obecna pandemia COVID-19. Budowa nowego systemu powinna być związana ze świadomością tego, że niezbędne jest

[186] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 03.08.2021).

opracowanie systemu ochrony ludności, którego zadaniem musi być kreowanie świadomości sytuacyjnej na temat zagrożeń w taki sposób, aby maksymalnie zmniejszyć ich skutki i przygotować na nie społeczeństwo, poprzez szkolenia o pierwszej pomocy i propagowanie informacji o zagrożeniach.

W oparciu o raport NIK, a także na podstawie własnych badań autora rozprawy oceniono funkcjonowanie SZK w Polsce oraz poziom świadomości sytuacyjnej ludności w na temat zagrożeń. Na podstawie analiz zweryfikowano hipotezę H.1: ***Świadomość sytuacyjna ludności o zagrożeniach i ryzyku utraty bezpieczeństwa w warunkach materializacji zagrożeń i kryzysów kształtuje się na niskim poziomie.***

Wykres 3.1. Ocena świadomości sytuacyjnej ludności na temat zagrożeń (N=112).
Źródło: opracowanie własne

Ocenie została poddana realizacja działań obywateli w sytuacjach kryzysowych. Weryfikację hipotezy H.1 oparto na analizie i ocenie odpowiedzi od reprezentatywnej grupy obywateli (wyk. 3.1).

Badanie przeprowadzone zostało na próbie 112 obywateli. Do oceny świadomości sytuacyjnej ludności na temat zagrożeń przyjęto 5-cio stopniową skalę określającą stopień zgody z poszczególnym stwierdzeniem (1 - bardzo niski, 2 - niski, 3 - umiarkowany, 4 - wysoki, 5 - bardzo wysoki). W celu określenia poziomu świadomości sytuacyjnej utworzone zostały 3 przedziały - zgodne z modelem zaprezentowanym na rys. 2.2 w rozdziale 2 - które posłużyły do oceny poziomu świadomości sytuacyjnej ludności (tab. 3.3).

W celu oceny poziomu świadomości sytuacyjnej ludności sformułowano następujące stwierdzenia:

1. *Jestem w stanie przygotować się do zagrożenia bez potrzeby otrzymywania komunikatów o nich.*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 29 osób oceniło swoją wiedzę na temat zagrożeń na bardzo wysokim poziomie, a 40 na wysokim poziomie, co pokazuje, że 61% obywateli potrafi samodzielnie przygotować się na nadchodzące zagrożenia, a ich świadomość sytuacyjna stoi na średnim poziomie. Osoby z niskim poziomem świadomości sytuacyjnej stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (24), niski (16) oraz bardzo niski (3). Na tej podstawie stwierdzono, że poziom przygotowania się ludności na zagrożenia kształtuje się na akceptowalnym poziomie i wynosi 3,68.

2. *Jestem w stanie zaplanować wszystkie niezbędne czynności, jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi znane.*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 35 osób oceniło swój sposób przygotowania się na znane zagrożenia na bardzo wysokim poziomie, a 44 na wysokim, co pokazuje, że 70% obywateli jest w stanie przygotować się na powtarzające się zagrożenie. Osoby z mniejszą wiedzą na temat czynności, jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest im znane stanowią 30% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (8) oraz bardzo niski (3). Na tej podstawie stwierdzono, że poziom planowania działań w momencie wystąpienia zagrożenia kształtuje

się na akceptowalnym poziomie i wynosi 3,89, ale widoczne są luki w badanym zakresie.

3. *Jestem w stanie zaplanować wszystkie niezbędne czynności, jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi obce*.

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 29 osób oceniło swój sposób przygotowania się na nowe zagrożenia na bardzo wysokim poziomie, a 47 na wysokim, co pokazuje, że 67% obywateli jest w stanie przygotować się na obce zagrożenia. Osoby z mniejszym poziomem świadomości sytuacyjnej na temat nowych zagrożeń stanowią 33% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (10) oraz bardzo niski (4). Na tej podstawie stwierdzono, że poziom przygotowania się na obce zagrożenia kształtuje się na akceptowalnym poziomie i wynosi 3,78, ale widoczne są luki w badanym zakresie.

4. Moja wiedza na temat zagrożeń kształtuje się na wysokim poziomie.

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 34 osoby oceniły swój poziom wiedzy na temat zagrożeń na bardzo wysokim poziomie, a 42 na wysokim, co pokazuje, że 67% obywateli ocenia swój poziom świadomości sytuacyjnej w tym zakresie na wysokim poziomie. Osoby z mniejszym poziomem świadomości sytuacyjnej na temat zagrożeń stanowią 33% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (26), niski (8) oraz bardzo niski (2).

Na tej podstawie stwierdzono, że wiedza na temat zagrożeń kształtuje się na akceptowalnym poziomie i wynosi 3,88, ale widoczne są luki w badanym zakresie.

5. Jestem świadomy tego, że podjęcie odpowiednich kroków w odpowiednim czasie może zniwelować skutki zagrożenia.

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 55 osób oceniło, na bardzo wysokim poziomie stwierdzenie że podjęcie odpowiednich kroków w odpowiednim czasie może zniwelować skutki zagrożenia, a 29 na wysokim, co pokazuje, że 68% obywateli jest świadoma tego, że podjęcie odpowiednich kroków w odpowiednim czasie może zniwelować skutki zagrożenia. Osoby z mniejszym poziomem świadomości sytuacyjnej stanowią 32% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (19), niski (6) oraz bardzo niski (3). Na tej podstawie stwierdzono, że poziom wiedzy na temat niezbęd-

nych do podjęcia kroków w momencie wystąpienia zagrożenia kształtuje się na akceptowalnym poziomie i wynosi 3.91, ale widoczne są luki w badanym zakresie.

6. *Jestem świadomy tego, że odpowiednia reakcja na zagrożenie może uchronić mnie przed jego skutkami.*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 53 osoby oceniły na bardzo wysokim poziomie swoją świadomość na temat tego, że odpowiednia reakcja na zagrożenie może uchronić ich przed jego skutkami, a 32 na wysokim, co pokazuje, że 75% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości sytuacyjnej stanowią 25% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (26), niski (8) oraz bardzo niski (2). Na tej podstawie stwierdzono, że poziom przygotowania się ludności na zagrożenia kształtuje się na zadowalającym poziomie i wynosi 4,07.

7. *Jestem w stanie ocenić stopień zagrożenia na podstawie obserwacji.*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 34 osoby oceniają na bardzo wysokim poziomie stopień zagrożenia na podstawie obserwacji, a 36 na wysokim, co pokazuje, że 63% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem oceny stopnia zagrożenia na podstawie obserwacji stanowią 37% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (32), niski (4) oraz bardzo niski (6). Na tej podstawie stwierdzono, że poziom oceny zagrożenia kształtuje się na akceptowalnym poziomie i wynosi 3,79.

8. *Jestem w stanie przewidzieć skutki zagrożenia*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 36 osób jest w stanie przewidzieć skutki zagrożenia na bardzo wysokim poziomie, a 39 na wysokim, co pokazuje, że 66% obywateli potrafi przewidzieć skutki zagrożenia. Osoby z mniejszym poziomem przewidywalności stanowią 34% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (27), niski (5) oraz bardzo niski (5). Na tej podstawie stwierdzono, że poziom przewidywania skutków zagrożeń kształtuje się na akceptowalnym poziomie i wynosi 3,86, ale widoczne są luki w badanym zakresie.

9. *Jestem w stanie na podstawie alertów RCB zaplanować odpowiednie kroki działania na wypadek wystąpienia zagrożenia*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 44 osoby oceniają na bardzo wysokim poziomie umiejętność planowania odpowiednich działań na wypadek wystąpienia zagrożenia na podstawie alertów RCB, a 35 na wysokim, co pokazuje, że 70% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem oceny stopnia zagrożenia na podstawie obserwacji stanowią 30% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (5) oraz bardzo niski (6). Na tej podstawie stwierdzono, że poziom planowania działań na podstawie alertów RCB kształtuje się na akceptowalnym poziomie i wynosi 3,96, ale widoczne są luki w badanym zakresie.

10. *Jestem świadomy podstawowych zagrożeń, jakie występują na terenie województwa, w którym mieszkam*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 46 osób bardzo wysoko ocenia poziom świadomości na temat zagrożeń na terenie województwa, w których mieszkają, a 35 na wysokim, co pokazuje, że 72% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 28% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (23), niski (5) oraz bardzo niski (4). Na tej podstawie stwierdzono, że wiedza na temat zagrożeń występujących na terenie województwa ankietowanych kształtuje się na zadowalającym poziomie i wynosi 4,01.

11. *Jestem w stanie rozpoznać zagrożenie takie jak powódź*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 37 osób jest w stanie rozpoznać zagrożenie takie jak powódź na bardzo wysokim poziomie, a 31 na wysokim, co pokazuje, że 60% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 40% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (25), niski (13) oraz bardzo niski (6). Na tej podstawie stwierdzono, że rozpoznawalność zagrożenia powodziowego kształtuje się na akceptowalnym poziomie i wynosi 3,71.

12. *Jestem w stanie rozpoznać zagrożenie na podstawie zmysłów (wzrok, słuch, węch)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 38 osób jest w stanie rozpoznać zagrożenie na podstawie zmysłów (wzrok, słuch, węch) na bardzo wysokim poziomie, a 37 na wysokim, co pokazuje, że 66% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 34% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (25), niski (7) oraz bardzo niski (5). Na tej podstawie stwierdzono, że poziom rozpoznania zagrożenia na podstawie zmysłów kształtuje się na akceptowalnym poziomie i wynosi 3,86, ale widoczne są luki w badanym zakresie.

13. *Jestem świadomy ryzyka jakie niesie ze sobą niestosowanie się do alertów RCB*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 44 osoby są świadome ryzyka jakie niesie ze sobą niestosowanie się do alertów RCB na bardzo wysokim poziomie, a 43 na wysokim, co pokazuje, że 77% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 23% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (17), niski (3) oraz bardzo niski (5). Na tej podstawie stwierdzono, że świadomość ryzyka wynikająca z niestosowania się do alertów RCB kształtuje się na zadowalającym poziomie i wynosi 4,05.

14. *Komunikaty wysyłane przez RCB są dla mnie zrozumiałe*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 48 osób ocenia zrozumiałość komunikatów RCB na bardzo wysokim poziomie, a 34 na wysokim, co pokazuje, że 73% obywateli ocenia swój poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 27% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (16), niski (11) oraz bardzo niski (3). Na tej podstawie stwierdzono, że zrozumiałość komunikatów RCB kształtuje się na zadowalającym poziomie i wynosi 4,01.

15. *Uważam, że dzięki poradnikom na temat zagrożeń jestem w stanie lepiej się do nich przygotować*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli, 37 osób ocenia przydatność poradników na temat zagrożeń na bardzo wysokim poziomie, a 43 na wysokim, co pokazuje, że 71% obywateli ocenia swój

poziom świadomości sytuacyjnej na wysokim poziomie. Osoby z mniejszym poziomem świadomości stanowią 29% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (20), niski (7) oraz bardzo niski (5). Na tej podstawie oceniono przydatność poradników na temat zagrożeń na akceptowalnym poziomie i wynosi 3,89, ale widoczne są luki w badanym zakresie.

W celu weryfikacji powyższych stwierdzeń przy pomocy oprogramowania PS IMAGO PRO wyznaczone zostały statystki pozycji (tab. 3.3).

Tabela 3.3. Oceny respondentów wg zidentyfikowanych czynników

Symbol czynnika	Nazwa czynnika	Średnia arytmetyczna (ocena)
C1	Jestem w stanie przygotować się do zagrożenia bez potrzeby otrzymywania komunikatów o nich	3,89
C2	Jestem w stanie zaplanować wszystkie niezbędne czynności jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi znane	4,01
C3	Jestem w stanie zaplanować wszystkie niezbędne czynności jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi obce	4,05
C4	Moja wiedza na temat zagrożeń kształtuje się na wysokim poziomie	4,01
C5	Jestem świadomy tego, że podjęcie odpowiednich kroków w odpowiednim czasie może zniwelować skutki zagrożenia	3,96
C6	Jestem świadomy tego, że odpowiednia reakcja na zagrożenie może uchronić mnie przed jego skutkami	3,86
C7	Jestem w stanie ocenić stopień zagrożenia na podstawie obserwacji	4,07
C8	Jestem w stanie przewidzieć skutki wystąpienia zagrożenia	3,91
C9	Jestem w stanie na podstawie alertów RCB zaplanować odpowiednie kroki działania na wypadek wystąpienia zagrożenia	3,88
C10	Jestem świadomy podstawowych zagrożeń, jakie występują na terenie województwa, w którym mieszkam	3,78
C11	Jestem w stanie rozpoznać zagrożenie takie jak powódź	3,89
C12	Jestem w stanie rozpoznać zagrożenie na podstawie zmysłów (wzrok, słuch, węch)	3,68
C13	Jestem świadomy ryzyka jakie niesie ze sobą niestosowanie się do alertów RCB	3,79
C14	Komunikaty wysyłane przez RCB są dla mnie zrozumiałe	3,71
C15	Uważam, że dzięki poradnikom na temat zagrożeń jestem w stanie lepiej się do nich przygotować	3,86

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

Następnie oszacowano wartości średniej dla próby badawczej. W tym celu wykorzystany został wzór 2.1, który przyjmuje następującą formułę:

$$PŚSL^{187} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.1)$$

Następnie obliczona została średnia ocena dla całej próby badawczej (tab. 3.4).

Tabela 3.4. Statystyki opisowe dla wskaźnika PŚSL (N=112).

Statystyka	Wartość
N	112
Rozstęp	4,00
Minimum	1,00
Maksimum	5,00
Średnia	**3,89**
Odchylenie standardowe	0,79149
Wariancja	0,626
Skośność	0,939
Kurtoza	1,692

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

W celu weryfikacji hipotezy H.1 określono poziom świadomości sytuacyjnej ludności zgodnie ze schematem zaprezentowanym w rozdziale II (rys. 2.1). Na pod-

[187] PŚSL - Poziom Świadomości Sytuacyjnej Ludności

stawie powyższych wyników można dokonać częściowej falsyfikacji hipotezy H.1, ponieważ poziom świadomości sytuacyjnej ludności osiąga wg wykonanych badań i przyjętych kryteriów wartość praktycznie akceptowalną lub nawet zadowalającą (zgodnie z przyjętym wcześniej 3 – poziomowym modelem świadomości sytuacyjnej).

Następnie dokonano analizy skupień (metodą k-średnich) w oparciu wystandaryzowaną zmienną PŚSL (tab. 3.5).

Tabela 3.5. Skupienie odchyleń pod kątem poziomu świadomości sytuacyjnej (N=112)

Ostateczne centra skupień			
	Skupienie		
	Niski poziom świadomości sytuacyjnej	Umiarkowany poziom świadomości sytuacyjnej	Wysoki poziom świadomości sytuacyjnej
Nazwa skupienia	1	2	3
Stand: Poziom świadomości sytuacyjnej ludności	-3,66926	-0,66506	0,77236
Liczba respondentów w każdym ze skupień	2	54	56

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

Zaprezentowane w tabeli 3.5 wyniki ukazują, że spośród 112 badanych 2 osoby (2%) stanowią grupę o niskim poziomie świadomości sytuacyjnej, 54 osoby (48%) posiadają umiarkowany poziom świadomości sytuacyjnej a 56 osób (50%) wyróżnia się wysokim poziomem świadomości sytuacyjnej.

Tabela 3.6. Podstawowe cechy respondentów odznaczających się określonym poziomem świadomości sytuacyjnej (N=112)

		Nazwa skupienia obserwacji			
		Niski poziom świadomości	Umiarkowany poziom świadomości	Wysoki poziom świadomości	Ogółem
Płeć	Kobieta	0	24	34	58 51%)
	Mężczyzna	2	30	22	54 49%)
Ogółem		2	54	56	112
		Numer skupienia obserwacji			
		Niski poziom świadomości	Umiarkowany poziom świadomości	Wysoki poziom świadomości	Ogółem
Wiek	do 25 lat	1	11	10	22 20%)
	26-35	1	24	28	53 47%)
	36-50	0	17	17	34 (30%)
	51-65	0	0	1	1 (1%)
	powyżej 65	0	2	0	2 (2%)
Ogółem		2	54	56	112
		Numer skupienia obserwacji			
		Niski poziom świadomości	Umiarkowany poziom świadomości	Wysoki poziom świadomości	Ogółem
Wykształcenie	podstawowe	1	2	0	3 (3%)
	gimnazjalne	0	2	0	2 (2%)
	zasadnicze zawodowe	0	3	2	5 (5%)
	średnie	0	22	19	41 36%)
	wyższe	1	25	35	61 54%)
Ogółem		2	54	56	112
		Numer skupienia obserwacji			
		Niski poziom świadomości	Umiarkowany poziom świadomości	Wysoki poziom świadomości	Ogółem
Miejsce zamieszkania	wieś	0	5	8	13 12%)
	do 20 tys.	0	7	10	17 15%)
	21–50 tys.	0	9	11	20 18%)
	powyżej 50 tys.	2	33	27	62 55%)
Ogółem		2	54	56	112

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

Szczegółową analizę respondentów przedstawiono w tabeli 3.6, w której określono: płeć, wiek, wykształcenie i miejsce zamieszkania respondentów o niskim, umiarkowanym oraz wysokim poziomie świadomości sytuacyjnej.

Ostatecznie hipoteza H.1 została częściowo sfalsyfikowana, ponieważ świadomość sytuacyjna plasuje się na akceptowalnym a nawet zadowalającym (dość wysokim) poziomie, ale z możliwością jego wzrostu poprzez zastosowanie dodatkowych narzędzi. Warto bowiem zwrócić uwagę na fakt, że w grupie respondentów znajdują się również osoby o niskim i umiarkowanym poziomie świadomości sytuacyjnej na temat zagrożeń i należy podjąć kroki zmierzające do podniesienia tego poziomu. Należy również zauważyć, że miara średniej nie w pełni obiektywizuje obraz oceny wynikowej poziomi świadomości sytuacyjnej, ponieważ może to się przekładać na dość znaczące ryzyko strat dla populacji o niższym poziomie świadomości sytuacyjnej w danym zakresie działania.

3.6. Podsumowanie rozdziału trzeciego

Zagrożenia zawsze towarzyszą funkcjonowaniu każdego systemu działania i każdemu podmiotowi oraz całemu społeczeństwu i dlatego tak ważne jest ich prawidłowe identyfikowanie i wczesne wykrywanie. Właściwy sposób przygotowania się do nich polega na wyborze odpowiedniej strategii. Stąd też istotne jest przygotowanie społeczeństwa i Zespołów Zarządzania Kryzysowego. Poczucie bezpieczeństwa można stworzyć m.in. poprzez kreowanie świadomości sytuacyjnej na temat zagrożeń, umiejętności ich rozpoznawania i radzenia sobie z nimi, gdy się pojawią.

Zagrożenia stanowią bezprecedensowe wyzwania dla rządów i każdego podmiotu indywidualnego lub grupowego na całym świecie. Tego typu zdarzenia zagrażające życiu i zdrowiu mają poważny wpływ na wszystkie dziedziny życia, takie jak edukacja, polityka, bezpieczeństwo publiczne czy działalność gospodarcza. Agendy rządowe reagują na zagrożenie na różne sposoby i z różnym skutkiem[188]. Istnieją dwa rodzaje strategii radzenia sobie z zagrożeniami: zapobiegawcze i łagodzące. Strategia zapobiegawcza to taka za pomocą, której państwo stara się zapobiec materializacji zagrożenia. Strategia łagodzenia to taka, która pomaga kontrolować rozprzestrzenianie się zagrożenia. Analiza zarówno strategii zapobiegania, jak i łagodzenia skutków w obecnym krajobrazie zagrożeń może pomóc zrozumieć, dlaczego niektóre kraje odnoszą większe sukcesy niż inne. Zachowania często obserwowane

[188] https://www.tandfonline.com/doi/full/10.1080/23276665.2020.1784769 (data dostępu 09.08.2021).

w sytuacjach awaryjnych to: ewakuacja, ucieczka, panika, letarg, szok, cisza, izolacja, schronienie, pomoc w przypadku klęski żywiołowej, poszukiwanie bliskich, nagłe zachowania „antyspołeczne”, ciekawość powrotu do domu lub pracy. Kryzysy mogą dotknąć każdego podmiotu, w dowolnym miejscu i czasie, a skuteczna komunikacja może być najważniejszym czynnikiem w osiąganiu i utrzymywaniu świadomości sytuacyjnej. Świadomość sytuacyjna jest dynamiczna, trudna do utrzymania i łatwa do utraty zwłaszcza w złożonych, stresujących sytuacjach. W rozdziale zidentyfikowano klęski żywiołowe, awarie techniczne i zakłócenia spowodowane działalnością człowieka oraz opisano wyniki analizy i zaprezentowano ocenę obecnie funkcjonującego Systemu Zarządzania Kryzysowego RP oraz wybranych jego komponentów ze wskazaniem ważniejszych luk naruszających poziom świadomości sytuacyjnej decydentów i obywateli. Oceny te były pochodną ocen uprawionych do tego organów państwowych.

W rozdziale pokazano także wyniki własnych badań ankietowych, które potwierdzają ogólnie akceptowalny poziom świadomości sytuacyjnej ludności i decydentów, ale widoczne są także dość istotne luki w niektórych obszarach i stąd wskazuje się na potrzebę minimalizacji ryzyka częściowej nawet utraty świadomości sytuacyjnej, która może generować dość znaczące straty dla państwa i społeczeństwa oraz poszczególnych grup obywateli. Taki cel jest możliwy do osiągnięcia poprzez wykorzystanie nowoczesnych technologii IT/ICT.

ROZDZIAŁ IV
INFORMOWANIE LUDNOŚCI O SYTUACJACH KRYZYSOWYCH W RP

4.1. Istota informowania ludności w sytuacjach kryzysowych

Informowanie ludności o zagrożeniach odgrywa istotne znaczenie, szczególnie w kontekście nie tylko planowania, ale przede wszystkim całego cyklu zarządzania kryzysowego. W przypadku kryzysu opinia publiczna ma podstawowe prawo do uzyskania informacji o tym, co się stało, co się dzieje, jak władze zamierzają zareagować na kryzys i jakie są jego potencjalne konsekwencje – co wynika z demokratycznego ustroju państwa. Pojęcie demokracji określa członków społeczeństwa jako odpowiedzialnych i zdolnych do uczestniczenia w procesie decyzyjnym kraju[189]. Oczekuje się, że obywatele będą działać odpowiedzialnie w czasie kryzysu, a dostęp do właściwe informacji jest podstawowym warunkiem umożliwiającym skuteczne podjęcie tych obowiązków. Istotnym bowiem elementem społeczeństw demokratycznych, a w szczególności tzw. społeczeństwa informacyjnego jest dostęp do informacji[190]. Społeczeństwo jest stosunkowo tolerancyjne wobec błędów, o ile te są naprawiane oraz władze państwowe potrafią to czynić jawnie . Właściwe zarządzanie informacją jest szczególnie ważne w kontekście kryzysu. Informacje są istotnym elementem łagodzenia skutków kryzysu i mogą w wielu przypadkach chronić ludzi przed pogarszającą się sytuacją a przede wszystkim umożliwić im świadome działanie.

W czasie kryzysu władze i organizacje ratownicze wymagają wsparcia i współpracy ze strony ludności. Jeśli współpraca układa się dobrze, to wysiłek może być znacznie mniejszy na przekonanie ludzi, że podejmowane są odpowiednie środki. Obywatele, którzy mają zaufanie do decydentów różnych szczebli, chętniej będą postępować zgodnie z instrukcjami, nawet jeśli instrukcje są sprzeczne z osobistymi preferencjami. Dlatego celem każdej organizacji zarządzania kryzysowego jest dobre poznanie swoich obywateli. Ta praca zaczyna się w normalnych warunkach, kiedy nie ma kryzysu. Ważne zatem jest, aby organizacje zarządzania kryzysowego były również dobrze znane przedstawicielom mediów i aby zawiązały się między nimi relacje bazujące na zaufaniu, zachęcając media do zachowania uczciwości w momencie wystąpienia zagrożenia. Można to osiągnąć, wspierając codzienną pracę mediów

[189] D. Borowska-Mostafa, Oryginalna Azetka Encyklopedia PWN, Wydawnictwo Naukowe PWN SA, War-szawa, 2012, s. 218.
[190] https://www.prezydent.pl/download/gfx/prezydent/pl/defaultopisy/2467/4/1/demokracja.pdf (data dostępu 12.08.2021).

i stosując otwartą politykę informacyjną. Kluczowym elementem pomyślnego radzenia sobie z kryzysem i w sytuacji kryzysowej jest wysoki stopień wiarygodności. W przeciwnym razie analiza, oceny, decyzje i zalecenia organu nie będą traktowane zobowiązująco[191], co jest ważnym komponentem świadomości sytuacyjnej.

Wiarygodność opiera się na czterech ważnych elementach: otwartości, kompetencji, uczciwości i empatii[192]. Informacje publiczne nie są oparte na relacji nadawca-odbiorca dlatego też treść przekazu musi być dobrze skonstruowana, należy również wziąć pod uwagę niewerbalne komunikaty towarzyszące takim szczególnym przekazom. Jeśli organ nie zdecyduje się na udzielenie informacji o jakiejś sprawie, to milczenie samo w sobie może być źle zinterpretowane. Komunikacja kryzysowa obejmuje wymianę informacji zachodzącą wewnątrz i pomiędzy władzami, organizacjami, mediami, zainteresowanymi osobami i grupami, przed, w trakcie i po kryzysie. Istnieją trzy główne wymiary komunikowania się w sytuacji kryzysowej[193]:

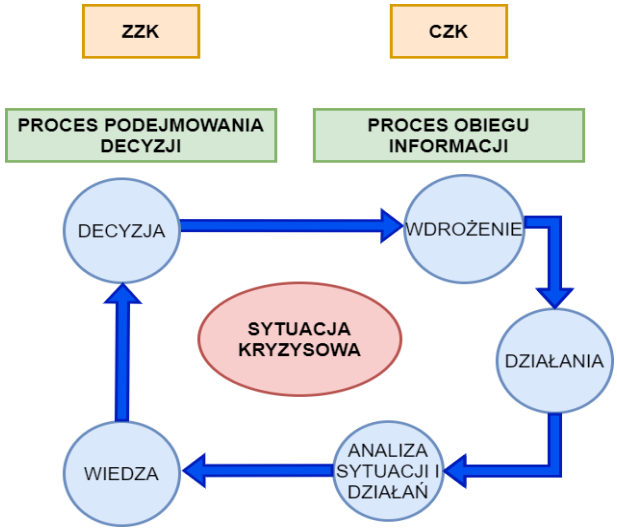
- Komunikowanie/informowanie w czasie rzeczywistego kryzysu,
- informowanie o sposobie radzenia sobie z kryzysem,
- zobrazowanie kryzysu ze szczególną dbałością o zrozumienie przekazywanych treści.

Największe problemy nierzadko wynikają nie z samego kryzysu, ale z radzenia sobie z kryzysem lub z niewłaściwego postępowania podczas kryzysu przez osoby, które są w niego zaangażowane lub są bezpośrednimi odbiorcami jego skutków, np. słabe przygotowanie, trudności w znalezieniu rozwiązań, brak elastyczności, niepełna znajomość wydarzeń, problemy ze zrozumieniem nowych ról i funkcji itp.[194]Typową cechą sytuacji kryzysowej jest to, że ta pojawia się w najmniej spodziewanym momencie, a w związku z tym wymagania związane z czasem przekazu aktualnej i pełnej informacji rosną bardzo szybko. Zarządzanie informacjami operacyjnymi i aktualizacjami, udzielanie porad, wskazówek i bieżących wyjaśnień w trybie interaktywnym musi odbywać się szybko i skutecznie. Ponadto analizowanie otrzymanych informacji oraz podejmowanie świadomych decyzji musi odbywać się bardzo szybko. Duża liczba informacji, które muszą być wymieniane, często może powodować przeciążenie kanałów informacyjnych, dlatego należy zapewnić im odpowiednią przepu-

[191] W. Walczak, *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej*, „Przedsiębiorczość i Zarzadzanie" nr 8 z 11.08.2009 r., s.108.
[192] F. Dahns*, A Practical Guide to Public Information during a Crisis (Budapest Guidelines III)*, NATO Civil Preparedness Civil Protection Group, s.6-9.
[193] Tamże s.6-9.
[194] F.P. Seitel, *Public Relations w praktyce,* Wydawnictwo Felberg SJA, Warszawa 2003, s. 229.

stowość[195]. Skuteczna komunikacja kryzysowa zależy od uporządkowania procesów informacyjnych i struktury całego systemu sprawnego i profesjonalnego obiegu informacji. Oznacza to, że każda organizacja powinna mieć ustaloną strategię i politykę informacyjną, która określa ich podstawowe atrybuty, a w tym otwartość, szybkość, dostępność, wiarygodność i ciągła ocena aktualności dostępnych zasobów informacyjnych. Niezbędne są również zasoby techniczne do wydawania i otrzymywania informacji (telefony, faksy, infrastruktura teleinformatyczna i związane z tym technologie informacyjne itp.). Należy zatem zakładać, że obraz kryzysu powinien być w każdej chwili rzeczywisty. Słabe radzenie sobie z obrazem kryzysu może spowodować, że rzeczywisty kryzys będzie się rozszerzał lub przybierał inną formę i kierunek. Kryzys i obraz kryzysu muszą być spójne. W procesie zarządzania informacją można wyodrębnić dwa współzależne od siebie podprocesy (rys 4.1)[196] :

1) proces podejmowania decyzji,
2) proces obiegu informacji,



Rysunek 4.1. Zarządzanie informacją w sytuacjach kryzysowych.

Źródło opracowanie własne

Oba te procesy są od siebie zależne, a defekt w działaniu jednego z nich, wpływa na skuteczność całego systemu informowania i przepływu informacji.

Obraz kryzysu w dużej mierze kształtują media, które relacjonują przebieg kryzysu w określonej formie i w zakresie nie zawsze pełnym. Dzisiejsze społeczeństwo informacyjne samo w sobie może być ważnym źródłem szybko ewoluujących

[195] Tamże s.229.
[196] G. Abgarowicz, I. Abgarowicz, *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, Uniwersytet Szczeciński Zeszyty Naukowe Nr 882, Szczecin 2015.

informacji, które mogą być przesyłane przez całą dobę, niezależnie od czasu i miejsca. Społeczeństwo ma dostęp do nowych systemów medialnych, dzięki czemu rozwinęły się nowe „nawyki medialne", np. monitorowanie wiadomości międzynarodowych przez Internet, dostęp do mediów zagranicznych[197]. W związku z tym coraz ważniejsze staje się opracowywanie przez organa odpowiedzialne za zarządzanie sytuacją kryzysową systematycznej i ciągłej analizy wydarzeń na całym świecie. Różnorodność kulturowa i wymiana międzynarodowa oznacza również, że służby zbierające informacje muszą być świadome kwestii wielokulturowości.

Organy decyzyjne komunikujące się z interesariuszami w czasie sytuacji kryzysowej powinny precyzyjnie identyfikować grupy społeczne, do których zamierzają wysyłać wiadomość. Wymagania, oczekiwania, specyficzna sytuacja i nawyki medialne odbiorcy decydują o tym, jakie informacje należy przesłać i jak te zasoby będą wpływać na poziom pożądanej świadomości sytuacyjnej. Dotyczy to informacji, których poszukują, gromadzą i wykorzystują obywatele, grupy, organizacje i firmy, a także kanałów, którymi posługują się odbiorcy w celu uzyskania informacji, które są uznawane za wiarygodne. Dialog z różnymi odbiorcami wymaga, aby zarządzający obiektywnie przedstawiali swoją ocenę sytuacji oraz intencje związane z dalszym działaniem. Organa odpowiedzialne za przekaz użytecznej informacji muszą pracować nad osiągnięciem i utrzymaniem wysokiego stopnia wiarygodności, co jest ważnym atrybutem koncepcji komunikowania się w sytuacji kryzysowej. Warto tu zatem przypomnieć, że odbiorcy oceniają wiarygodność organu na podstawie czterech podstawowych kryteriów: otwartości, kompetencji, obiektywizmu i empatii.

4.2. Wymiana informacji w sytuacjach kryzysowych oraz zapewnienie informacyjnej ciągłości działania

Sprawne i skuteczne procesy informacyjne powinny gwarantować dostęp do informacji wiarygodnych i wyczerpujących oraz dostosowanych do sytuacji. Informacje powinny być zatem neutralne, aktualne i adekwatne do sytuacji. W procesie wymiany informacji ważne jest, aby podać jak najwięcej informacji w kontrolowanej, jasnej i zrozumiałej formie. Jeżeli sytuacja nie uległa znaczącej zmianie, należy również przekazać taką informację. Zakres informacyjny powinien być dostosowany do

[197] Tamże.

sytuacji[198]. Dobra praktyka informacyjna zakłada zrozumienie sytuacji osób dotkniętych kryzysem. Informacje powinny odzwierciedlać ich potrzeby, zainteresowania i odpowiadać ich głównym troskom. W sprawnym systemie informacyjnym pytania i odpowiedzi można z przygotować z wyprzedzeniem szczególnie w przypadku dysponowania współczesnymi technologiami IT/ICT. Ponadto zapewnienie obiektywnych informacji jest ważne w zarządzaniu kryzysowym. Jeśli opinia publiczna wątpi w obiektywizm przekazu, to proces informacyjny jest mało skuteczny. Otwarta, proaktywna i neutralna polityka informacyjna jest zatem jedynym sposobem uniknięcia postrzegania przez ludność niewiarygodności przekazu. Właściwa prezentacja informacji o sytuacji kryzysowej opiera się na „zasadzie jednego głosu". Od początku kryzysu powinien funkcjonować rzecznik organu decyzyjnego, który relacjonuje obowiązującą ocenę sytuacji i zamiar działania. W ten sposób organ ten jest uosabiany przez konkretną osobę, która pomaga w budowaniu zaufania. Rzecznik przedstawia mediom stanowisko organu i odpowiada na pytania natury ogólnej. Konkretne pytania wymagają wsparcia specjalistów/ekspertów. Wrażenia na temat tego, jak zespół zarządzania kryzysowego radzi sobie z sytuacją, są oparte na tym, co ludzie widzą, słyszą lub czytają. W przypadku dodatkowych wyjaśnień/konkretnych pytań istnieje ryzyko, że rzecznik wyda się nieprecyzyjny, niejasny lub udzieli fałszywej odpowiedzi. Specjaliści mogą pomóc w takich przypadkach, ale przed rozmową z mediami należy ich odpowiednio poinstruować. Źle sprecyzowana merytorycznie odpowiedź może czasami być zbyt złożona dla ogółu społeczeństwa. Może wywołać dalsze pytania i zwiększyć niepokój opinii publicznej[199]. Ważne jest, aby znaleźć właściwą równowagę między informacjami, które są rozbudowane i merytorycznie uzasadnione (poprawne technicznie), a informacjami, które można łatwo przekazać. Szybkie i otwarte przekazywanie informacji powinno być skorelowane z kompletnością przekazu, co może wprowadzać niepożądane opóźnienia. Są ku temu dwa główne powody. Po pierwsze, zapewnienie ciągłych aktualizacji obrazu sytuacji, nawet jeśli ta nie uległa zmianie oraz ogłoszenie terminu następnej informacji prasowej, co może zmniejszać liczbę kontroli krzyżowych przeprowadzanych przez media[200]. Po drugie, społeczeństwo musi być stale informowane. Regularny przepływ informacji o aktual-

[198] A. Szymańska, Efektywna komunikacja w zarządzaniu kryzysami i problemami, w. Tworzydło D., Soliński T.(red.), *Public relations – wyzwania współczesności*, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Rzeszów 2004, s. 127-142.
[199] Tamże s. 127.
[200] Tamże s. 127-141.

nym stanie wydarzeń świadczy o tym, że prace są w toku i podejmowane są działania. Opinia publiczna nie może nigdy odnieść wrażenia, że jest „porzucana" lub pozostawiana do samodzielnego rozwiązywania problemów. Częste aktualizacje pozwalają uniknąć tego typu oceny.

Rozpowszechnianie informacji w czasie kryzysu powinno rozpocząć się jak najszybciej, zwykle poprzez zwołanie konferencji prasowej. We wczesnej fazie sytuacji kryzysowej może być konieczne częste publikowanie, np. co godzinę komunikatów prasowych[201]. Jeśli to możliwe, audycje radiowe stanowią skuteczny sposób szybkiego reagowania na główne obawy opinii publicznej. Listy kontaktowe mediów powinny być przygotowane z wyprzedzeniem i gotowe do natychmiastowego użycia. Aby zapewnić szybką dystrybucję, odpowiednia infrastruktura techniczna (na przykład szybki faks, odpowiednia technologia IT/ICT itp.) powinna być dostępna na miejscu. Co więcej należy jak najszybciej uruchomić infolinię dla ogółu społeczeństwa, która musi być wsparta odpowiednią infrastrukturą, a liczba linii telefonicznych powinna odpowiadać dostępnemu personelowi. Infolinia musi być w stanie odpowiadać na liczne pytania i wątpliwości różnych interesariuszy, 24 godziny na dobę i przez cały okres trwania kryzysu w zależności od charakteru i zasięgu kryzysu oraz jego wpływu na społeczeństwo. Udzielanie informacji w fazie odbudowy po kryzysie może odbywać się przez kilka miesięcy lub lat i zwykle rozpoczyna się wkrótce po incydencie[202]. Głównym celem jest poinformowanie kompetentnych organizacji (np. pracowników pomocy humanitarnej) i zainteresowanych stron o powstałych problemach, podjętych środkach i proponowanych rozwiązaniach. W praktyce trudno jest określić fazę reagowania i fazę odbudowy po sytuacji kryzysowej, ponieważ te nieuchronnie nakładają się na siebie. To nakładanie się i przedłużający się okres odbudowy mogą skomplikować pokryzysowy obraz sytuacji i proces informowania. Ponadto, w fazie odbudowy władze muszą zająć się problemami wielu grup docelowych. Obiektywny plan dostarczania ustrukturyzowanych informacji w fazie odbudowy jest ważny. Plan kryzysowy przewiduje ustalenia dotyczące naprawy i odbudowy[203]. Celem takiego planu jest powrót państwa, różnych organizacji oraz pojedyn-

[201] W. Macierzyński, *Rola mediów w komunikacji kryzysowej*, w: M. Jabłonowski, L. Smolak (red.), Zarządzanie kryzysowe w Polsce, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2007, s. 383-400.
[202] Tamże s. 383-400.
[203] W. Kitler, A. Skrabacz, Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny, Wydawnictwo Towarzystwo Wiedzy Obronnej, Warszawa 2010.

czego obywatela do funkcjonowania sprzed zagrożenia. Informacje przekazane w tej fazie dotyczą dwóch głównych obszarów[204]:

- uwarunkowań społeczno-politycznych sposobu realizacji procesów reagowania,
- identyfikacji problemów, które pojawiły się lub mogą powstać w wyniku kryzysu oraz sposobów radzenia sobie z nimi.

Sposób przekazywania informacji, ich liczba i częstotliwość zależą od rodzaju i zasięgu kryzysu[205]. Po każdym kryzysie zawsze pojawią się pytania, np. Jakie są skutki kryzysu? Czy istnieje możliwość ponownego wystąpienia? Inne prawdopodobne tematy pytań to: dlaczego powstał kryzys?, Dlaczego nic nie zrobiono wcześniej, czy można było tego uniknąć? Odpowiedzi na te pytania są szczególnie istotne w przypadku kryzysu spowodowanego przez człowieka. Informacje powinny być otwarte i jasne. Informacje pokryzysowe należy przekazywać ofiarom zgodnie ze zindywidualizowanym podejściem[206] (wyodrębnienie klastrów interesariuszy/poszkodowanych). Może to być również konieczne w przypadku kryzysu za granicą. Ofiary powracające do domu mogą czuć się odizolowane z powodu traumy, zwłaszcza w konfrontacji z ich zwykłym otoczeniem. Mogą czuć się zagubieni i nie mieć kontaktu z innymi, którzy doświadczyli tej samej traumy. Osobiste podejście jest pomocne, aby podkreślić, że traumatyczne doświadczenia są traktowane poważnie przez władze[207]. W następstwie kryzysu osoby rządzące w państwie odpowiedzialne są za określenie polityki naprawy w oparciu o badanie skutków kryzysu. Za realizację tej polityki odpowiedzialny jest zespół operacyjny. W zespole tym powinni uczestniczyć przedstawiciele serwisu informacyjnego. Przygotowania do informacji w fazie odbudowy mogą zbiegać się z przygotowaniami do dostarczania informacji podczas samego kryzysu. Na przykład, gdy przedsiębiorstwa lub gminy uzgadniają z lokalnymi lub regionalnymi nadawcami ogłoszenia i ostrzeżenia w czasie kryzysu, można również podać informacje na temat fazy odbudowy. Podczas opracowywania strategii informacyjnej można rozważyć potrzebę udziału innych podmiotów (np. pośredni-

[204] A Practical Guide to Public Information during a Crisis (Budapest Guidelines III) - https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170612_170612-Budapest_Guidelines_en.pdf s. 6-9 (dostęp w internecine 21.08.2021).
[205] J. A. F. Stoner, R. E. Freedman, D. G. Jr. Gilbert, *Kierowanie*, Wydawnictwo Państwowe Wydawnictwo Ekonomiczne, Warszawa 1998, s. 613.
[206] Tamże, s. 613.
[207] B. Rozwadowska, Public relations w sytuacjach kryzysowych, Wrocław 2002, s. 65.

cy) w skutecznym dostarczaniu informacji na etapie odbudowy. Dotyczy to zwłaszcza szczególnych grup docelowych takich, jak różne osoby z defektami poznawczymi lub osoby mówiące innymi językami. Ponadto, należy uzgodnić z organizacjami je reprezentującymi interesy grup. W tym celu pomocne mogą się okazać:[208]:

- publiczne numery telefonów do celów informacyjnych,
- listy organizacji dla konkretnych pytań,
- listy z ostatnimi danymi o: zabitych, zaginionych i rannych,
- listy zawierające główne pytania / odpowiedzi dotyczące zdrowia publicznego, zagrożeń itp.,
- listy adresów wsparcia psychologicznego,

Ofiarami są wszystkie osoby, które w jakiś sposób poniosły szkody: fizyczne, psychiczne lub materialne. Krewni rannych lub zabitych również stanowią grupę wymagającą specjalnej opieki. Pomoc ofiarom należy zorganizować jak najszybciej po kryzysie, która powinna obejmować organizację punktu informacyjnego, w którym można uzyskać pomoc lub informacje, w tym informacje o odszkodowaniach i organizacjach oferujących porady prawne. Ponadto, organa decyzyjne muszą udzielać informacji, jak w razie potrzeby uzyskać pomoc w zakresie zakwaterowania tymczasowego lub zastępczego[209]. Podobnie jak w fazie przedkryzysowej i kryzysowej, zasada otwartego i regularnego informowania ludzi o aktualnościach ma zastosowanie w fazie odbudowy w celu zapewniania ciągłości działania w państwie[210] i w jego podrzędnych strukturach. Jak widać złożoność procesów informowania ludności może istotnie wpływać na sposób, zakres i formę przekazu realizowanego w aktualnych warunkach a to może determinować poziom świadomości sytuacyjnej ludności.

4.3. Modele zapewnienia świadomości sytuacyjnej

Model świadomości sytuacyjnej wg M. R. Endsley to obiektywne postrzeganie istniejącej sytuacji oraz dokładne zrozumienie tego, co dzieje się w danym środowisku i co może się zdarzyć w najbliższej przyszłości. Jak wcześniej sygnalizowano –

[208] https://www.duw.pl/czk/informatory-i-poradniki/poradniki/7106,Przygotowanie-na-wypadek-naglego-zdarzenia.html (data dostępu 16.02.2023).
[209] A. Żebrowski, Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej, Kraków 2012, s. 24.
[210] Tamże s. 24.

Endsley w swojej definicji świadomości sytuacyjnej zaleca uwzględnienie trzech procesów [211]:

- Monitorowania i postrzegania tego, co się dzieje (Poziom 1);
- Zrozumienia tego, co zostało dostrzeżone (Poziom 2);
- Prognozowania przyszłych wydarzeń i działań (Poziom 3);

Poziomy świadomości sytuacyjnej stworzone przez M. R. Endsley można ukonkretnić i rozszerzyć o pytania z nimi związane[212]:

- **Poziom 1 – Jakie informacje zostały wygenerowane i jakich informacji potrzebują odbiorcy/interesariusze?, czyli co wnosić powinno monitorowanie sytuacji oraz jak przygotować i doprowadzić pozyskane informacje do świadomości odbiorcy.** Na tym poziomie następować powinno zatem nie tylko rozpoznawanie, ale także bieżące monitorowanie elementów opisujących sytuację, ponieważ te mogą - zmieniać się w czasie.
- **Poziom 2** – **Co to dla interesariusza/odbiorcy oznacza pozyskana informacja?, czyli zrozumienie przekazu oraz** pożądana interpretacja obecnej sytuacji. Oznacza to, że poziom 2 świadomości sytuacyjnej wymaga integracji informacji postrzeganych na poziomie 1 w celu zrozumienia znaczenia tych elementów dla pożądanych celów lub wyników. Dzięki procesom rozpoznawania, interpretacji i oceny wzorców, a przede wszystkim trafnego i logicznego wnioskowania możliwe jest zrozumienie otoczenia, elementów oraz zdarzeń.
- **Poziom 3** – **Czego można się spodziewać?, czyli zaawansowana eksploracja danych i uzyskanych informacji w celu** przewidywania przyszłego stanu sytuacji (lub wręcz nawet kreowanie przyszłego stanu). Trzeci i najwyższy poziom świadomości sytuacyjnej obejmuje zdolność do prognozowania przyszłego stanu elementów w środowisku. Biorąc pod uwagę percepcję (monitorowanie) i zrozumienie sytuacji (poziomy 1 i 2 świadomości sytuacyjnej), a także wiedzę o tym, jak elementy wzajemnie na siebie oddziałują dynamicznie, poziom 3 osiąga się poprzez wykorzystanie tych informacji – tj. projekcje prawdopodobnych przyszłych stanów środowiska, które są ważne lub przydatne do podjęcia dalszych decyzji.

---

[211] https://www.skybrary.aero/index.php/Situational_Awareness_(OGHFA_BN) (data dostępu 21.08.2021).

[212] C.A. Bolstad, M.R. Endsley, *Tools for supporting team collaboration, Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society,* Santa Monica, CA: HFES. s. *374-378.*

Osiągnięcie każdego z poziomów świadomości sytuacyjnej zależy w dużym stopniu od kontekstu danej sytuacji kryzysowej lub scenariusza[213]. Oznacza to, że informacje niezbędne pilotowi do osiągnięcia świadomości sytuacyjnej są zupełnie inne niż te, które są wymagane od operatora elektrowni jądrowej. Tak samo informacje niezbędne urzędnikowi zdrowia publicznego do zachowania świadomości sytuacyjnej podczas pandemii są zupełnie inne od dwóch pozostałych zawodów.

W dynamicznie zmieniającym się środowisku te trzy poziomy świadomości sytuacyjnej są osadzone w pętli, w której sytuacja ciągle się zmienia, zarówno w odpowiedzi na wpływy zewnętrzne, jak i zmiany wynikające z wcześniejszych decyzji, które następnie wpływają na ocenę bieżącego stanu sytuacji. Oznacza to, że zmiany w środowisku mogą wpływać na świadomość sytuacyjną, czasami ją poprawiając lub pogarszając.

Jak wcześniej wspomniano - istotny wkład w postrzeganie i odwzorowanie świadomości sytuacyjnej wniósł J. Cooper, który postanowił zobrazować poziomy świadomości sytuacyjnej za pomocą kolorów. Każdy kolor reprezentuje potencjalny stan świadomości i pomaga w rozpoznawaniu, ocenianiu i unikaniu potencjalnych zagrożeń. Kolory J. Coopera pierwotnie nie miały nic wspólnego z sytuacjami taktycznymi, poziomem czujności oraz ze świadomością sytuacyjną, a raczej ze stanem umysłu. Uważał on, że wprowadzone przez niego kolory odnoszą się do stopnia niebezpieczeństwa i pozwalały przejść z jednego poziomu myślenia do drugiego, aby umożliwić właściwe działanie w zaistniałych sytuacjach (rys. 4.2). tak więc J. Cooper jako pierwszy użył kolorów do wskazania de facto stanu psychicznego i tak [214]:

- **Kolor biały** określa stan zrelaksowania i nieświadomości tego, co się dzieje wokół Nas. Jest to stan całkowitego rozproszenia i braku obserwacji. Tętno w tym stanie jest normalne, a osoba zaatakowana narażona jest na śmierć chyba, że napotka na niekompetentnego atakującego. Ten stan jest zwykle określany jako „śnienie na jawie" lub „zajęty". J. Cooper uważa, że ludzie w bieli chodzą z opuszczonymi głowami, jakby obserwowali własne stopy. Nie zauważają zbliżającego się niebezpieczeństwa, dopóki dosłownie nie dosięgnie ich niespodziewana sytuacja,

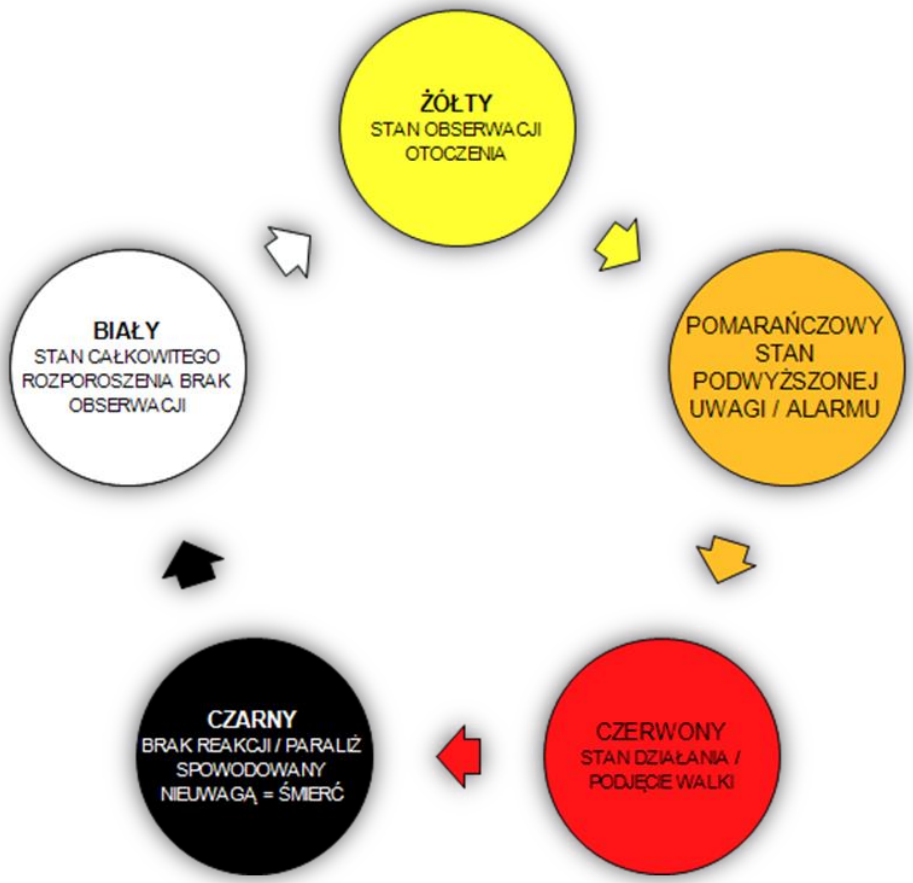
[213] M. R. Endsley, *Theoretical underpinnings of situation awareness: A critical review*, M.R. Endsley & D.J. Garland (red.), *Situation awareness analysis and measurement*, Mahwah, NJ: LEA, 2000 str. 3-32.
[214] J. Ahern, Gun *Digest Buyer's Guide to Concealed-Carry Handgun, "Gun Digest Books*", Stany Zjednoczone, 2010, s. 60.

- **Kolor żółty** określa stan zrelaksowania, ale również obserwacji otoczenia. Osoba w tym stanie jest czujna oraz świadoma tego, co dzieje się wokół niej. Tętno w tym stanie jest normalne a stan świadomości określany jest jako optymalny. Pomimo wyostrzonych zmysłów samo poleganie na nich nie zwiększy czujności. Dlatego J. Cooper zaleca, aby pozostać w stanie relaksacji co pozwala na otwartą koncentrację oraz daje dostęp do większej liczby sytuacji na temat otoczenia, w którym podmiot znajduje się.
- **Kolor pomarańczowy** opisywany jest przez J. Coopera jako podwyższony stan czujności z odnotowanym konkretnym celem. Różnica między stanem żółtym, a pomarańczowym polega na skupieniu się na określonym celu. Tętno w tym stanie jest podwyższone, co oznacza, że istnieje potencjalne zagrożenie, które przyciągnęło uwagę. Może to być prawie wszystko i zwykle nie skutkuje niczym, w takim przypadku następuje powrót do koloru żółtego.
- **Kolor czerwony** występuje sytuacji, gdy skupienie uwagi na stanie pomarańczowym powoduje uznanie sytuacji za groźną w wyniku czego następuje przejście do stanu czerwonego. W tym stanie zidentyfikowane zagrożenie uznawane jest za realne i oznacza gotowość do działania. Osoba w tym stanie jest mentalnie przygotowana do realizacji swojego planu.
- **Kolor czarny** oznacza poddanie się panice i stresowi do tego stopnia, że nie jesteśmy w stanie zareagować na bodźce. Paraliż ten został najprawdopodobniej wywołany z powodu braku przygotowania psychicznego w jakimkolwiek innym stanie świadomości omawianym wcześniej. Najbardziej prawdopodobnym scenariuszem jest to, że w pobliżu znajduje się osoba, która może zaoferować swoją pomoc lub że konflikt zakończy się bez szkody, ale to uczucie na zawsze będzie miało trwały wpływ na ludzką psychikę.

Kolory J. Coopera zostały opracowane, aby pomóc w uświadamianiu stanów psychicznych mających istotny wpływ na funkcjonowanie i zachowanie się jednostek w groźnej sytuacji kryzysowej lub walki. Wraz ze wzrostem niebezpieczeństwa wzrasta gotowość do podjęcia pewnych działań. Model ten jest szeroko stosowany w np. psychologii społecznej, czy też ekonomia behawioralnej, a przypisanie kolorów do zachowań ludzkich pozwala łatwiej zrozumieć psychikę człowieka[215] i ocenić jego

[215] http://www.cmagriffin.com/situational-awareness-level/ (data dostępu 28.09.2021).

predyspozycje przede wszystkim do rozumienia i podejmowania adekwatnych działań do pozyskanych informacji.



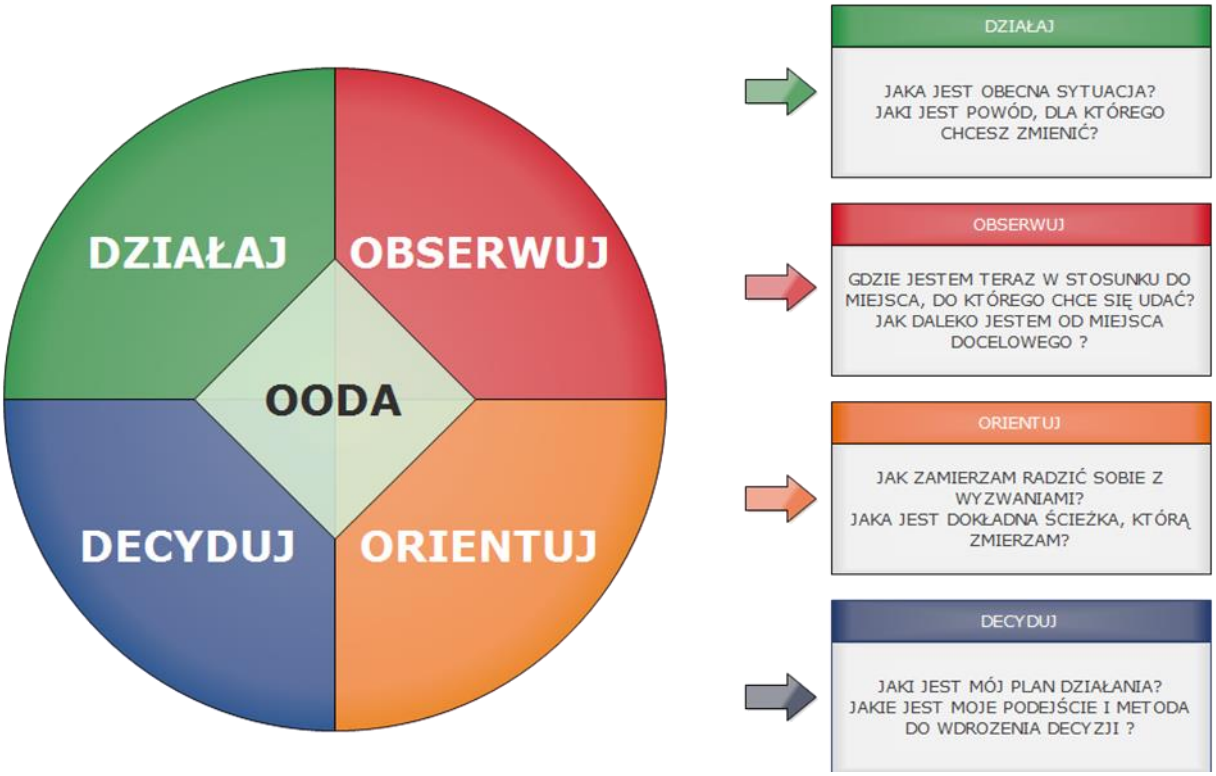
Rysunek 4.2. Poziomy świadomości sytuacyjnej wg. J. Coopera

Źródło: opracowanie własne na podstawie J. Ahern, *Gun Digest Buyer's Guide to Concealed-Carry Handgun*, w: Gun Digest Books, Stany Zjednoczone, 2010, s. 60.

Ważnym uzupełnieniem dla identyfikacji stanu świadomości sytuacyjnej jest pętla *OODA* (*Observe, Orient, Decide, Act*[216]) będąca czteroetapowym podejściem opracowanym przez stratega wojskowego Johna Boyda (rys. 4.3). Jak wskazuje termin „pętla", proces ten jest ciągły, iteracyjny. Koncepcja pętli odnosiła się do zdolności posiadanych przez pilotów myśliwców, które pozwoliły im odnieść sukces na polu bitwy. Obecnie model ten używany jest przez amerykańskie oddziały Marines i inne organizacje. Państwa na całym świecie wykorzystują pętlę OODA jako część swojej strategii wojskowej, która została także przyjęta przez przedsiębiorstwa, aby pomóc im rozwijać się w niestabilnej i wysoce konkurencyjnej gospodarce. Jest to szczególnie istotne w procesie reagowania na zmieniające się okoliczności i warunki

[216] Observe, Orient, Decide, Act, (OODA) – Obserwacja, Orientacja, Decyzja, Działanie.

panujące na świecie, aby uzyskać przewagę nad konkurencją (przeciwnikiem, atakującym itp.). Model pętli OODA mapuje proces gromadzenia danych, ich analizy, udostępniania i wykorzystywania w działaniu. Zespoły zarządzania kryzysowego mogą wykorzystać cykl OODA jako model teoretyczny do opracowywania procesów analizy, planowania i oceny sytuacji kryzysowych.

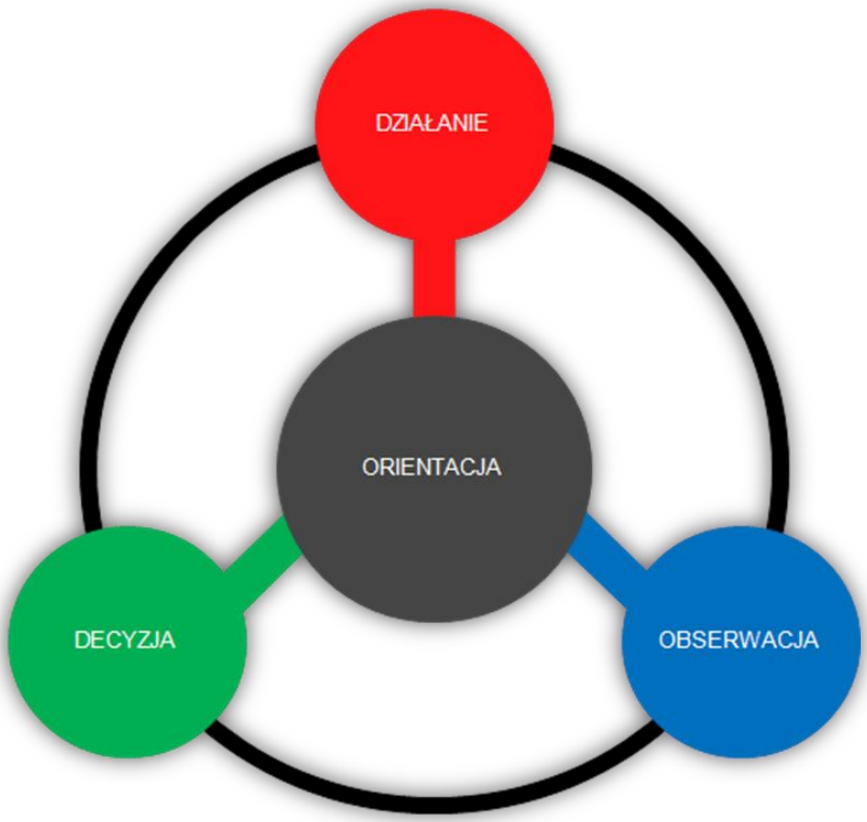


Rysunek 4.3. Pętla OODA

Źródło opracowanie własne na podstawie (https://www.samatters.com/enhancing-the-ooda-loop/

Dzięki efektywnemu zarządzaniu procesami możliwe jest wypracowanie strategii bezpieczeństwa i innowacyjnych modeli szybszego ograniczania lub eliminowania skutków zagrożeń[217]. Model *OODA* można interpretować jako interaktywną sieć zorientowaną na „rdzeń", którym może być orientacja na cel i zakres oraz sposób działania i wykorzystania zasobów (rys. 4.4)[218].

[217] J. Marczak, *Bezpieczeństwo narodowe – pojęcie, charakter, uwarunkowania* ,w. R. Jakubczak, J. Flis (red.), *Bezpieczeństwo narodowe Polski w XXI wieku: wyzwania i strategie*, Bellona, Warszawa 2006, s. 15.
[218] http://www.nwlink.com/~donclark/leadership/ooda.html (data dostępu 03.02.2023).



Rysunek 4.4. Interaktywne podejście do pętli OODA

Źródło opracowanie własne na podstawie http://www.nwlink.com/~donclark/leadership/ooda.html

Orientację należy zatem traktować jako sposób, w jaki interpretuje się sytuację w oparciu o kulturę, doświadczenie, nowe informacje, analizę, syntezę i dziedzictwo[219].

W związku z powyższym pętla ta jest zestawieniem interakcji, w których są przechowywane informacje w trybie ciągłym. Dzięki twórczemu wykorzystaniu pętli OODA państwo oraz obywatele są w stanie działać w sposób ciągły dostosowując się do panującej sytuacji. Świadomość sytuacyjna odnosi się zatem do stopnia, w jakim postrzeganie sytuacji odpowiada rzeczywistości. W kontekście zarządzania kryzysowego brak utrzymania świadomości sytuacyjnej może skutkować rozszerzaniem i przedłużaniem się kryzysu. Analiza dziedziny problemu i podjęte badania wskazują na potrzebę podniesienia rangi procesów informowania ludności w zarządzaniu kryzysowym, a w szczególności na potrzebę kreowania poziomu świadomości sytuacyjnej ludności oraz samych decydentów w SZK poprzez wykorzystanie tradycyjnych i współczesnych technologii IT/ICT.

[219] Tamże.

4.4. Aktualne rozwiązania dotyczące informowania ludności w sytuacjach kryzysowych

W momencie wystąpienia sytuacji nadzwyczajnej lub kryzysowej ważną rolę odgrywa pozyskiwanie wiarygodnych informacji, które są warunkiem skutecznego reagowania kryzysowego. Informacja powinna być określona i zdefiniowana poprzez istotne dla kreowania poziomu świadomości sytuacyjnej atrybuty informacji takie, jak[220]:

- terminowość, dostępność, wiarygodność informacji,
- treść (aktualność, trafność, prawdziwość, obiektywizm, stosowność),
- forma/format,
- cena i wartość użytkową informacji,
- legalność.

Informacje należy definiować zatem jako każdy sygnał (znak), który ma sens dla komunikatora i odbiorcy, a więc dane, które możemy interpretować[221].

Można zatem przyjąć, że w procesie informowania ludności o zagrożeniach kluczową rolę odgrywają zasoby informacyjne w różnej postaci, a w tym dane i wiedza, jak i cały system informacyjny. System informacyjny jest jednostką organizacyjno-funkcjonalną, która zapewnia gromadzenie, przetwarzanie, przechowywanie i dostępność informacji i danych[222]. Według *Cyber Security Glossary*, system informacyjny powinien być postrzegany jako "funkcjonalny agregat umożliwiający zorientowane na cel i systematyczne pozyskiwanie, przetwarzanie, przechowywanie danych". Ponadto system powinien obejmować źródła danych i informacji, nośniki, sprzęt, oprogramowanie i narzędzia, technologie i procedury. Wsparcie informacyjne w zakresie zarządzania kryzysowego zależy *de facto* od potrzeb i potencjału danego kraju[223]. Potrzeba wsparcia informacyjnego spowodowana jest sytuacjami nadzwyczajnymi typowymi dla kraju. Istnieje wiele metod informowania ludności o sytuacjach kryzysowych. W aktualnie funkcjonujący SZK RP informacje mogą być przekazywane za pomocą systemów dźwiękowych, komunikatów *SMS*, stron internetowych, mediów społecznościowych, radioodbiorników, telefonów itp. Ważny przy tym jest spo-

[220] K. Holla, J. Ristvej, M. Titko, *Crisis Management - Theory and Practice*, *IntechOpen* United Kingdom, 2018, s.39.
[221] Tamże s. 39.
[222] M. Tvrdíková, Implementation and Innovation of Information Systems in Companies. 1st ed. Prague: Grada; 2010.
[223] Tamże.

sób zbierania, monitorowania, przetwarzania i dystrybucji informacji – do czego w szczególny sposób mogą przyczynić się współczesne technologie IT/ICT[224].

Aktualne rozwiązania dotyczące informowania ludności o zagrożeniach można podzielić na metody tradycyjne oraz wykorzystujące współczesne technologie. Pod koniec XX wieku środki masowego przekazu można było podzielić na osiem branż medialnych: książki, Internet, czasopisma, filmy, gazety, radio, nagrania i telewizję. Rozwój technologii komunikacji cyfrowej na przełomie XX i XXI wieku zrewolucjonizował metody informowania ludności o zagrożeniach. Zanim zostały wprowadzone rozwiązania takie jak telefon komórkowy czy komputer i związany z nim rozwój Internetu, główne sposoby informowania ludności o zagrożeniach odbywały się metodami tradycyjnymi takimi jak radio, telewizja, gazeta, list telegram, telefon stacjonarny, systemy alarmowe itp.[225]

Podobna sytuacja związana z ewolucją technologiczną ma miejsce w przypadku telefonów komórkowych, które współcześnie niejednokrotnie są w stanie zastąpić również i komputery. Początki rozwoju telefonii komórkowej datowane są na rok 1908 kiedy to Nathan Stubblefield zaprezentował patent na bezprzewodowy telefon działający na zasadzie dwukierunkowego radia[226]. Pierwszy telefon komórkowy, którego działanie zbliżone jest do współczesnych rozwiązań powstał w 1973 roku, a pierwsza rozmowa za jego pomocą została wykonana w 1973 przez inżyniera Motoroli – Martina Coopera[227]. Technologia telefonii komórkowej ewoluowała od 1G do 5G (tab. 4.1).

Tabela 4.1. Rozwój telefonii komórkowej

1G (1980)	2G (1990)	3G (2000)	4G (2010)	5G (2020)
- analogowe połączenie głosowe, - łączność mobilna.	- cyfrowe połączenie głosowe, - wiadomości tekstowe, - podstawowe usługi danych.	- mobilny Internet szerokopasmowy, - wprowadzenie smartfonów.	-szybkie mobilne łącze, - protokół internetowy	- ulepszona mobilna łączność szerokopasmowa, - bezprzewodowa łączność

Źródło opracowanie własne na podstawie (*http://site.ieee.org/prc-com/files/2019/03/165B2040-30FC-42DA-AF7B-1F82A9D4A812.jpeg*.)

[224] M. McLuhan, *Zrozumieć media. Przedłużenia człowieka*, przedm. L.H. Lapham, przeł. N. Szczucka, w. Wydawnictwo WNT, Warszawa 2004, s. 39.
[225] https://learn.g2.com/history-of-computers(data dostęp 18.08.2021).
[226] https://www.thevintagenews.com/2018/01/06/wireless-phone/ (data dostęp 18.08.2021).
[227] https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html (data dostęp 18.08.2021).

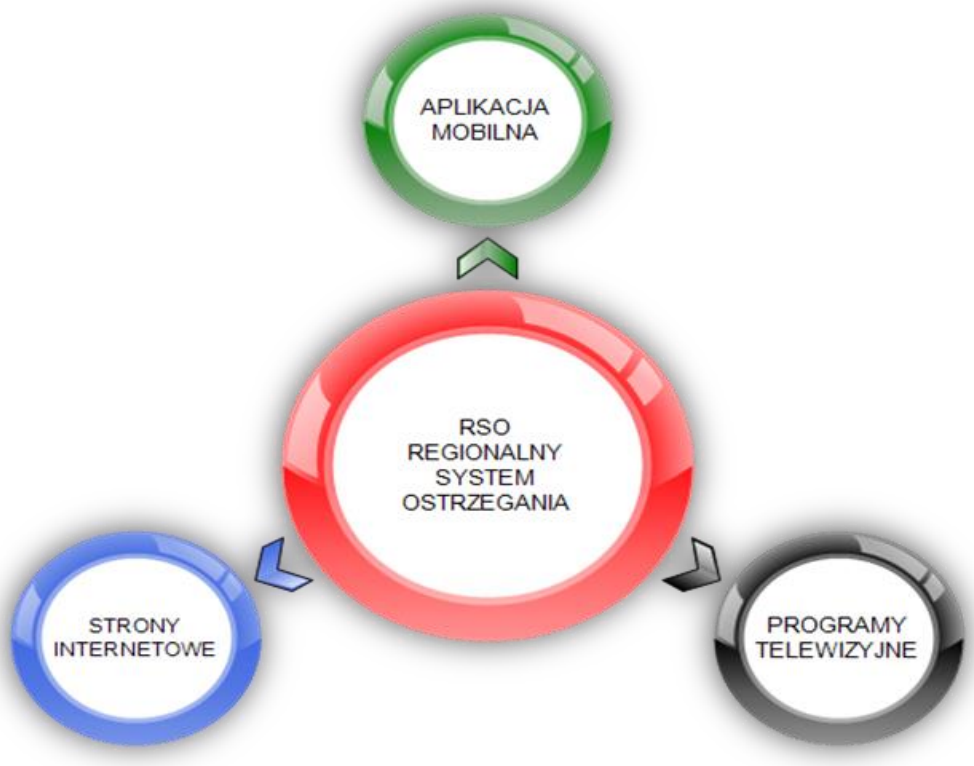
W tabeli 4.1 przedstawiono rozwój telefonii mobilnej według generacji (1G-5G) wraz z czasem wdrożenia. Co ciekawe lata wdrożenia technologii w Polsce są odmienne od dat wykorzystania technologii na świecie. I tak, np. technologia 1G została wdrożona w Polsce dopiero w 1992 r. [228]. Możliwości telefonii komórkowej i dostęp do sieci oznacza, że telefony komórkowe stają się domyślną metodą komunikacji i mogą być użyteczne w różnych formach informowania o sytuacji kryzysowej. Mnogość dostępnych aplikacji – głosowych, SMS-owych i szerokopasmowych – oraz ich znajomość przez obywateli jest w stanie podnieść wydajność procesów informacyjnych i zwiększyć poziom świadomości sytuacyjnej oraz możliwości lepszego przygotowania się na zagrożenia. Funkcjonalność współczesnych telefonów ułatwia nie tylko proces komunikacji, ale również zapewnia narzędzia pomocne w kreowaniu świadomości sytuacyjnej o zagrożeniach poprzez wykorzystanie różnorodne aplikacji, których celem jest komunikatywne informowanie ludności o zagrożeniach[229].

Regionalny System Ostrzegania (RSO)

Regionalny System Ostrzegania (RSO) jest darmową ogólnodostępną usługą informacyjną Ministerstwa Spraw Wewnętrznych i Administracji, a także wojewodów. Zadaniem RSO jest informowanie ludności o zagrożeniach. Usługa ta została stworzona na podstawie umowy pomiędzy MSWiA oraz Telewizją Polską S.A. zawartej dn. 14 października 2013 roku[230]. Po pobraniu aplikacji na telefon w zakładce Informacje o RSO można przeczytać szczegółowe informacje na temat działania systemu, który jest zarządzany na co dzień przez Wojewódzkie Centra Zarządzania Kryzysowego (WCZK) podlegające wojewodom (rys. 4.5). W aplikacji mobilnej umieszczone są informacje dotyczące ostrzeżeń meteorologicznych, hydrologicznych, a także dotyczące aktualnej sytuacji na danym terenie dostosowane do panujących warunków atmosferycznych, sytuacji na drogach, wypadków itp. Ponadto, w aplikacji umieszczona jest mapa, która prezentuje stan polskich wód. Dodatkową funkcją aplikacji są poradniki dotyczące m.in. sposobu zachowania się podczas wystąpienia katastrof naturalnych, awarii technicznych czy zagrożeń wywołanych na skutek działalności człowieka. Poradniki te zostały opracowane przez Ministerstwo Administracji

[228] https://www.orange.pl/poradnik/siec-komorkowa/od-1g-do-5g-czyli-historia-technologii-mobilnej/ (data dostęp 18.08.2021).
[229] Tamże.
[230] https://www.gov.pl/web/mswia/regionalny-system-ostrzegania (data dostęp 18.08.2021).

i Cyfryzacji na podstawie materiałów udostępnionych przez urzędy wojewódzkie i Rządowe Centrum Bezpieczeństwa[231].



Rysunek 4.5. Struktura Regionalnego Systemu Ostrzegania

Źródło: opracowanie własne

W zależności od rejonu zamieszkania, powiadomienia dostosowane są do konkretnych województw. Ponadto, poprzez udostępnienie lokalizacji na urządzeniu mobilnym użytkownik jest informowany o zagrożeniach występujących na terenach obejmujących miejsce jego pobytu. Za treść komunikatów o zagrożeniach odpowiada Wojewódzkie Centrum Zarządzania Kryzysowego, jeśli dotyczy problemu na terenie województwa oraz Ministerstwo Spraw Wewnętrznych i Administracji, jeśli problem dotyczy zagrożenia ogólnopolskiego: Aplikacja RSO jest darmowa i dostępna dla systemów operacyjnych takich, jak *Android*, *iOS*, *Windows Phone*. Wszystkie funkcje zawarte w aplikacji dostępne są również na stronach internetowych urzędów wojewódzkich. Ponadto z aplikacji RSO można korzystać za pomocą dedykowanej telewizji hybrydowej (*HbbTV*) oraz cyfrowej telewizji *DVB-T*[232].

[231] Tamże.
[232] Tamże.

Krajowy System Wykrywania Skażeń i Alarmowania (KSWSiA)

Klęski żywiołowe mogą negatywnie wpłynąć na zdrowie publiczne, spowodować straty w mieniu oraz przyczynić się do osłabienia potencjału warunkującego sprawne funkcjonowanie państwa. Skuteczna komunikacja jest kluczowym elementem właściwego zarządzania incydentami i reagowania na nie. W sytuacjach kryzysowych istotną rolę odgrywa informowanie i ostrzeganie o zagrożeniach bez zbędnych opóźnień. Sposoby informowania są różnorodne, ale dzięki pojawiającym się i upowszechnianym współczesnym IT/ICT technologiom i zmianom kulturowym systemy powiadamiania o sytuacjach kryzysowych stają się coraz bardziej sprawne i skuteczne w ochronie ludzi i zdrowia. Kluczową rolę w procesie informowania ludności cywilnej o zagrożeniach odgrywają sygnały alarmowe i komunikaty ostrzegawcze, które przyjmują pewną ustaloną formę. Aby zapobiec skutkom sytuacji kryzysowych wywołanych materializacją zagrożeń takich, jak katastrofy naturalne, awarie techniczne, czy chociażby działania terrorystyczne został stworzony w Polsce jednolity Krajowy System Wykrywania Skażeń i Alarmowania (KSWSiA), do którego zadań, oprócz monitorowania i wykrywania zagrożeń należy zaliczyć zapobieganie skutkom katastrof oraz wspieranie ćwiczeń, treningów oraz symulacji w celu zmniejszenia bądź zniwelowania skutków zagrożeń. W skład KSWSiA wchodzą takie systemy, jak moduł[233]:

- obserwacji,
- pomiarów,
- analiz,
- prognozowania skażeń i powiadamiania o skażeniach.

Ponadto KSWSiA posiada swoje struktury organizacyjno-funkcjonalne, do których zadań należy analiza skażeń i ocena sytuacji oraz opracowanie, ogłoszenie i wprowadzenie działań interwencyjnych. KSWSiA stanowi integralną składową systemu zarządzania kryzysowego[234].

W Polsce dokumentem przewodnim związanym z systemem wykrywania skażeń i alarmowania o nich jest Rozporządzenie Rady Ministrów w sprawie systemów wykrywania i zgłaszania skażeń oraz uprawnień organów w tych sprawach wydane

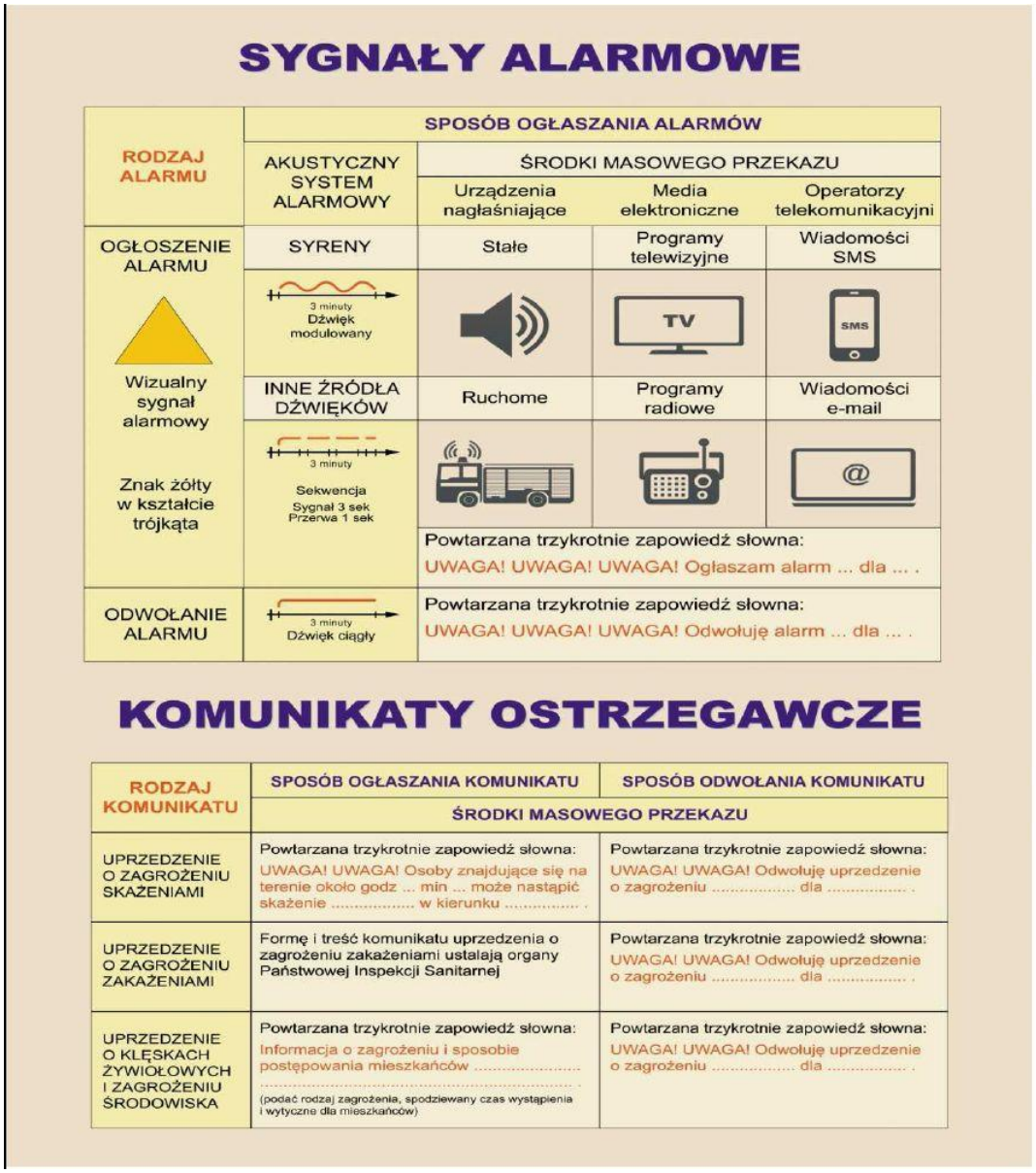
[233] https://epodreczniki.pl/a/ostrzeganie-i-alarmowanie/D9S0KGBEH (data dostęp 18.08.2021).
[234] Tamże.

z dnia 7 stycznia 2013 r. Oprócz zasad działania systemu, określono w ustawie terminy takie jak m.in.[235]:

- alarm – informacja o skażaniu lub sytuacji kryzysowej powstałej na skutek katastrofy naturalnej awarii technicznej, działań terrorystycznych, zagrożenia wojennego lub wojny,
- zakażenie – skutki skażenia ludzi zwierząt lub roślin zakaźnymi czynnikami biologicznymi,
- skażenie – zanieczyszczenie środowiska, żywności, pasz oraz powierzchni ciała ludzi lub zwierząt, niebezpiecznymi substancjami i mieszaninami chemicznymi materiałami promieniotwórczymi lub zakaźnymi czynnikami biologicznymi, niezależnie od ich rodzaju i czasu ich oddziaływania,
- alarmowanie – wysyłanie sygnału do władz, służb i ludności danego obszaru, informowanie o zagrożeniu skażeniem, skażeniu lub sytuacji kryzysowej spowodowanej klęską żywiołową, awarią techniczną, działalnością terrorystyczną, wojną lub zagrożeniem wojną,
- prognozowanie – ocena rozwoju sytuacji, prognoza i prezentacja możliwych skutków skażenia środowiska naturalnego, powierzchni ciała ludzi lub zwierząt oraz określanie wynikających z tego skutków dla funkcjonowania strefy publicznej i obiektów szczególnie ważnych dla ogółu obszaru regionu bezpieczeństwa i obronności państwa,
- powiadamianie – przekazanie informacji, której celem jest ostrzeżenie władz i społeczeństwa o możliwości wystąpienia zagrożenia, o jego wystąpieniu lub usunięciu, a także poinformowanie o sposobie postępowania w konkretnym przypadku,
- monitoring skażeń – systematyczny monitoring w celu wykrycia substancji zanieczyszczających powodujących skażenie, które przedostały się do środowiska lub w celu określenia stopnia skażenia,
- obserwacja – działania mające na celu identyfikację źródła skażenia, miejsca zakażenia, przedostania się materiałów zanieczyszczających do środowiska lub zmiany stopnia tego skażenia,

[235] Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach.

- ostrzeganie – dostarczanie komunikatów i informacji z wyprzedzeniem o prawdopodobnych zagrożeniach oraz na temat zalecanych środków ochronnych.



Rysunek 4.6. Sygnały alarmowe i komunikaty ostrzegawcze

Źródło: https://brzeszcze.pl/renegade-cwiczenia-z-wykorzystaniem-syren-alarmowych-28-30-05-2019,9323

W przypadku wykrycia i zidentyfikowania zagrożeń takich jak skażenie, zakażenia lub klęski żywiołowe, awarie techniczne, zagrożenie wojną, działalnością terrorystyczną, główną metodą informowania ludności znajdującej się w bezpośrednim niebezpieczeństwie przyjęto wykorzystanie sygnałów alarmowych. Komunikaty ostrzegawcze wysyłane są w przypadku zagrożenia zanieczyszczeniem lub klęską

żywiołową. W załączniku do rozporządzenia Rady Ministrów z dnia 7 stycznia 2013 r. – w sprawie systemów wykrywania skażeń i zgłaszania ich wystąpienia zgodnie z kompetencjami organów właściwych w tych sprawach – zostały udostępnione informacje o sposobie i formie informowania ludności na temat przekazywania sygnałów alarmowych (rys. 4.6) i komunikatów ostrzegawczych na terytorium Rzeczypospolitej Polskiej (rys. 4.6) [236].

Obowiązek wprowadzenia decyzji na temat sygnału alarmowego lub komunikatu ostrzegawczego spoczywa na organie administracji publicznej na danym obszarze, a tego typu sygnały mogą być zastosowane wyłącznie w sytuacji zaistnienia rzeczywistego zagrożenia. Wykorzystanie tego typu sygnałów w ramach np. treningów lub ćwiczeń możliwe jest wyłączne w sytuacji, gdy odpowiedni organ terytorialny poinformuje o nich z 24 godzinnym wyprzedzeniem w środkach masowego przekazu lub w sposób obowiązujący na danym terenie. Tego typu ogłoszenie powinno zawierać również informację na temat zasięgu terytorialnego przeprowadzanych treningów lub ćwiczeń. W celu zapewnienia bezpieczeństwa ludności istotne jest nie tylko przekazanie komunikatów, ale również odpowiednie zachowanie się w trakcie i po zakończeniu (odwołaniu) alarmu. Dlatego też należy unikać przekazywania informacji, które nie są zweryfikowane[237].

Środki masowego przekazu w procesie informowania ludności o zagrożeniach

W sytuacjach kryzysowych telewizja i radio są najczęściej używanymi środkami informowania ludności o zagrożeniach, ponieważ programy radiowe i telewizyjne są nadawane w czasie rzeczywistym, a informacje przekazywane za pośrednictwem tych środków masowego przekazu są często bezpośrednio z miejsca wystąpienia zagrożenia. Zarówno radio jak i telewizja stanowią najszybsze i najbardziej wiarygodne źródło przekazania informacji, a także dają możliwość przekazania przez ludność na żywo dodatkowych relacji o zaistniałej sytuacji[238].

W pewnych okolicznościach media zapewniają ważną rolę w zarządzaniu klęskami żywiołowymi, zwłaszcza w zakresie nadawanych alertów, ostrzeżeń i porad. Mogą też odgrywać istotną rolę w dostarczaniu potrzebnych informacji decydentom. Należy jednak pamiętać o tym, że oprócz pozytywnych aspektów wykorzystania mediów w procesie informowania ludności o zagrożeniach mogą same z sie-

[236] Tamże.
[237] Tamże.
[238] E.L., Qyarantelli, *What is a Disaster? Perscpective on the Qestion, Routledge*; 1st edition, London 1998, s. 146-159.

bie wprowadzić również chaos i dezorientację u osób podejmujących decyzje, co może skutkować zmniejszeniem wartości informacji niezbędnych do przekazania[239]. Często media zamiast skoncentrować się na procesie informowania ludności o zagrożeniach wywierają presję na decydentach i osobach podejmujących decyzje w sytuacjach kryzysowych, aby wyjaśnili i uzasadnili, co robią, aby zapobiec zagrożeniu lub zakończyć kryzys. Ponadto w przypadku gdy władze polityczne nie chcą informować opinii publicznej, media znajdą inne źródła informacji takie, jak np. ratownicy lub przypadkowi ludzie, co skutkuje często niezweryfikowanymi danymi, co może powodować chaos i dezorientację[240]. Media mogą również stanowić zachętę do tendencyjnego interpretowania obserwowanych zjawisk społeczno-gospodarczych. Ze względu na ten fakt młodsza grupa odbiorców radia i telewizji w celu zdobycia informacji o zagrożeniach preferuje skorzystanie z innych dostępnych źródeł wyszukania informacji takich jak np. media społecznościowe.

Media elektroniczne w procesie informowania o zagrożeniach

Media elektroniczne w wymiarze współczesnym to media społecznościowe oraz strony i komunikatory internetowe[241]. Kilkanaście lat temu zanim wprowadzono do powszechnego użytku telefony typu smartfon korzystanie z mediów społecznościowych w telefonie wydawało się nierealne. Obecny rozwój technologii spowodował, że większość użytkowników Smartfonów (zwłaszcza młodych) wykorzystuje telefon jako mini osobisty komputer do komunikowania się za pomocą mediów społecznościowych. Media społecznościowe i portale internetowe stanowią ważny kanał dostarczania w czasie rzeczywistym pilnych wiadomości i powiadomień o sytuacjach kryzysowych oraz ważnych informacji z kraju i ze świata. Tak więc media społecznościowe mogą odgrywać istotną rolę w procesie informowania ludności o zagrożeniach ponieważ informacje z tych mediów [242]:

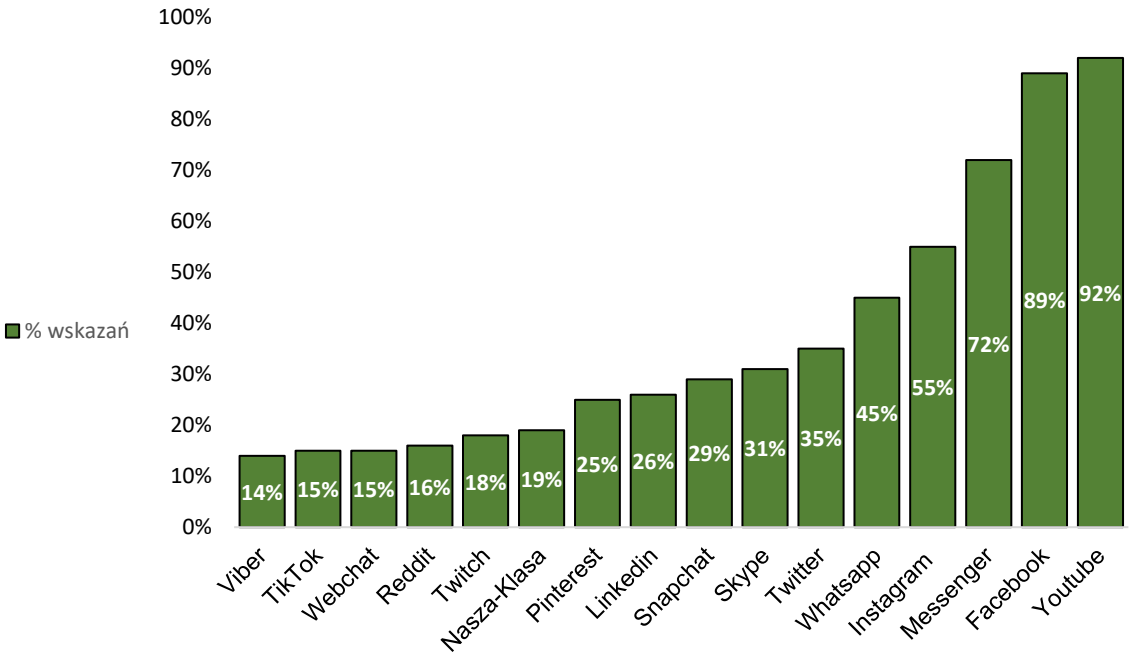
- często płyną ze źródeł pierwotnych, które mogą zostać uznane jako źródła nieoficjalne, ale mogą to być ważne informacje także dla bezpieczeństwa poszczególnych osób.

---

[239] M. Adamkiewicz, *Wokół rozważań nad bezpieczeństwem egzystencjalnym, czyli interpretacje śmierci w nauce*, Studia Bezpieczeństwa Narodowego, 2013, nr 4, s. 57.
[240] Tamże, s. 146-159.
[241] G. Hutton, M. Fosdick, *The Globalization of Social Media*, „Journal of Advertising Research" 2011, Vol. 51 s. 564-570.
[242] Tamże, s. 564-570.

- są na bieżąco komentowane a treści komunikatów szybko udostępniane i rozpowszechniane.

Media społecznościowe mogą skutecznie pomóc w procesie informowania ludności o zagrożeniach oraz w dotarciu do obywateli, ponieważ znaczna część obywateli korzysta z nich na urządzeniach mobilnych. Według raportu Hootsuite z 2020 r. za najbardziej popularne media społecznościowe w Polsce uważane są: YouTube, Facebook, FB Messenger, Instagram, Whatsapp, Twitter (wyk. 4.1)[243].



Wykres 4.1. Najpopularniejsze media społecznościowe w Polsce

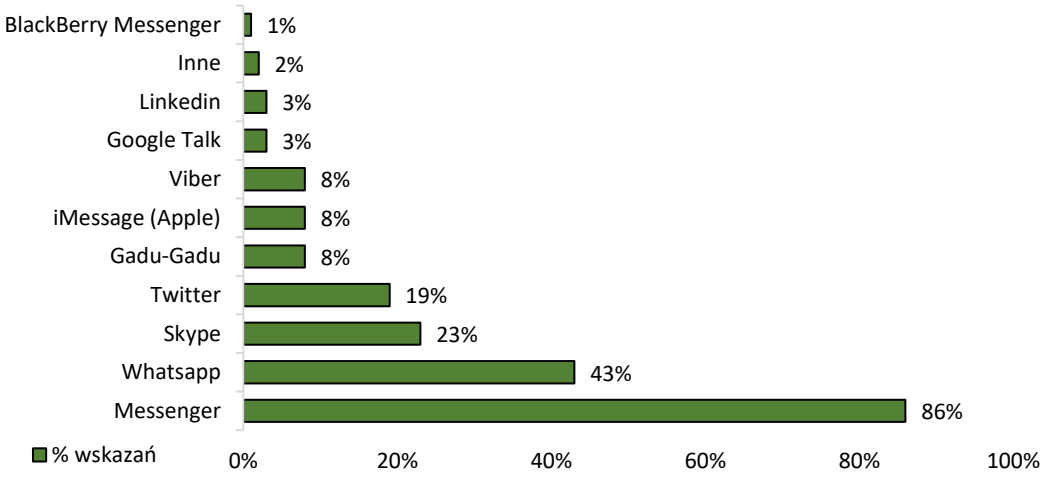
Źródło: opracowanie własne na podstawie (Digital Marketing W Polsce W 2020 Roku), https://www.ltb.pl/digital-marketing-w-polsce-w-2020-roku

Z badań przeprowadzonych przez Hootsuite wynika, że najpopularniejszym portalem społecznościowym w Polsce jest *YouTube* (92%), który pomimo tego, iż służy do udostępniania treści wideo, zaliczany jest do grona portali społecznościowych. Na kolejnych miejscach, według przeprowadzonych badań, plasują się takie portale jak *Facebook* (89%), a zaraz po nim *Facebook Messenger* – komunikator portalu społecznościowego *Facebook* (72%). Coraz większą popularnością w Polsce zyskują takie portale jak *Instagram* (55%) i *Whatsapp* (45%). Zaskakująco niskie miejsce zajmuje polski portal Nasza-Klasa (19%, praktycznie wycofany z eksploatacji)[244].

[243] https://www.ltb.pl/digital-marketing-w-polsce-w-2020-roku/ (data dostępu 03.09.2021).
[244] Tamże.

Korzystanie z portali społecznościowych w czasie sytuacji kryzysowych, podczas których społeczeństwo zmuszone jest do ograniczenia swoich codziennych kontaktów, odgrywa kluczową rolę w komunikacji międzyludzkiej, przy założeniu wiarygodności źródła. W czasie sytuacji kryzysowej takiej, jak pandemia COVID-19, rola portali społecznościowych, a także komunikatorów nabrała nowego znaczenia. Komunikacja społeczna zarówno podczas pracy zdalnej jak i podczas kontaktów z rodziną w większości przypadków przeniosła się ze świata rzeczywistego do cyberprzestrzeni. Sytuacje kryzysowe powodują, że społeczeństwo nawiązuje kontakty z wykorzystaniem komunikatorów, które często w zależności od rodzaju sytuacji stanowią jedyną formę kontaktu ze światem zewnętrznym.

W 2019 roku firma Statista przeprowadziła badania dotyczące najczęściej używanych komunikatorów internetowych w Polsce[245] (wyk. 4.2).



Wykres 4.2. Najpopularniejsze komunikatory internetowe w Polsce w 2019 roku

Źródło: opracowanie własne na podstawie (Statista) dostęp na stronie: https://www.statista.com/statistics/982664/poland-most-popular-messaging-apps/ (data dostępu 21.09.2021)

Według badań przeprowadzonych przez firmę Statista najpopularniejszym komunikatorem internetowym w Polsce jest *Messenger* (86%), który ze względu na integrację z *Facebook* sprawił, że jest to najczęściej wykorzystywany komunikator zarówno w Polsce jak i w większości krajów na świecie. Na kolejnych miejscach znajdują się takie komunikatory, jak: *Whatsapp* (43%), Skype (23%) czy *Twitter* (19%). Wśród najpopularniejszych komunikatorów w Polsce nie zabrakło również Gadu-Gadu (8%) polskiego komunikatora, który „lata świetności" ma już za sobą, pomimo

[245] https://www.statista.com/statistics/982664/poland-most-popular-messaging-apps/ (data dostępu 21.09.2021).

licznych prób jego reaktywacji[246]. Przywołane badania odnoszą się do wszystkich mieszkańców Polski, a statystyki na temat najpopularniejszych komunikatorów oraz mediów społecznościowych zostały zebrane na podstawie danych pochodzących od Dostawców telefonii komórkowej oraz Internetu.

W czasach pandemii COVID-19 wykorzystanie komunikatów internetowych nabrało nowego znaczenia i wykorzystywane są głównie do pracy zdalnej, podczas której coraz większa popularność zyskują komunikatory takie jak m.in. Microsoft Teams, Zoom, Skype itp. Ponadto sytuacja wywołana przez pandemię sprawiła, że w dalszym ciągu powstają nowe komunikatory i platformy zarówno do pracy jak i nauki zdalnej[247].

W sytuacji kryzysowej rola mediów społecznościowych, stron internetowych i komunikatorów jest znacznie większa niż kiedykolwiek. Jeden z najpopularniejszych portali społecznościowych, jakim jest Facebook, uruchomił specjalną stronę – Centrum sytuacji kryzysowych, na której na bieżąco możliwe jest śledzenie zagrożeń aktualnie występujących na świecie[248]. Funkcja utworzona przez Facebook została zintegrowana z konkurencyjnym programem – Whatsapp w celu zwiększenia potencjalnej liczby odbiorców.

W sytuacjach kryzysowych oprócz danych pozyskiwanych z takich źródeł, jak np. Rządowe Centrum Bezpieczeństwa, czy portale społecznościowe, istotną rolę w procesie informowania ludności o zagrożeniach odgrywają również strony internetowe[249]. Warto zwrócić uwagę na wszelkiego rodzaju portale informacyjne, których zadaniem jest przekazywanie najświeższych informacji zarówno z kraju, jak i ze świata. Tego typu strony stanowią źródło sprawdzonych i zweryfikowanych informacji na temat zagrożeń. Strony internetowe zawierające najświeższe informacje na temat sytuacji w kraju można skategoryzować ze względu na źródła informacji lokalnych – zawierające informacje na temat wydarzeń na obszarze, którego bezpośrednio dotyczą, jak i krajowych – zawierające informacje na temat wydarzeń, których obszar obejmuje całe państwo. Tak jak w przypadku portali społecznościowych, czy też innych form informowania ludności o zagrożeniach strony te zawierają dodatkowo wytyczne jak postępować na wypadek materializacji zagrożenia, a także najnowsze in-

[246] http://web.archive.org/web/20110 (data dostępu 21.09.2021).
[247] J. Woźniak, M. Staruch, M. Jurek, W. Wereda, P. Zaskórski, *Jak uczyć (się) zdalnie?*, Wydawnictwo CeDeWu, Warszawa 2020, s. 87.
[248] https://www.facebook.com/crisisresponse/?source=crisis_bookmark (data dostępu 23.09.2021).
[249] Tamże.

formacje o skali zagrożenia i wytycznych poszczególnych władz na temat obostrzeń itp.

Korzystanie z mediów społecznościowych, komunikatorów internetowych czy też stron internetowych umożliwia nie tylko dostęp do informacji, ale daje również możliwość szerszego informowania o zaistniałych zagrożeniach. Dla zapewnienia bezpieczeństwa ludności w sytuacjach kryzysowych niektóre firmy ubezpieczeniowe po skorzystaniu z ich oferty w momencie wystąpienia zagrożenia wysyłają alerty pogodowe mające na celu ostrzeżenie przed niebezpiecznymi zjawiskami pogodowymi. Jedną z firm, która uruchomiła tego typu inicjatywę, jest LINK4. Firma ta od 2019 roku wysyła swoim klientom komunikaty pogodowe w formie *SMS*. Według statystyk podawanych przez firmę LINK4, od momentu uruchomienia usługi wysłanych zostało 190 tys. alertów pogodowych[250]. Treść wysyłanych komunikatów zbliżona jest do tych wysyłanych przez Rządowe Centrum Bezpieczeństwa i informuje o prognozowanym na danym obszarze zagrożeniu atmosferycznym. Ponadto wysyłany jest link przekierowujący na stronę internetową w wersji mobilnej, która zawiera wskazówki, jak radzić sobie w sytuacji zaistniałego zagrożenia. Alerty wprowadzone przez LINK4 niewątpliwie można uznać za użyteczne niemniej jednak forma ich przekazu wymaga modernizacji z uwagi z uwagi na to, że pośród potencjalnych klientów są również osoby korzystające z klasycznych telefonów komórkowych, na których wysłana strona internetowa nie może zostać uruchomiona.

4.5. Ocena procesu informowania ludności w sytuacjach kryzysowych w RP

Proces informowania ludności powinien być postrzegany przez pryzmat wartości informacji. Informacja bowiem to wiadomość, którą otrzymuje człowiek poprzez obserwację lub przemyślenia, podlegająca przekazowi w układzie nadawca-odbiorca i może być postrzegana w dwóch perspektywach jako [251]:

- informacja jednostkowa, opisującą pojedynczy obiekt, proces, zdarzenie w formie (O, C, W) gdzie: O – oznacza nazwę obiektu lub zdarzenia, C oznacza nazwę mierzonej cechy, W oznacza wartość cechy jako wynik pomiaru,

[250] https://www.link4.pl/biuro-prasowe/aktualnosci-link4/alerty-pogodowe-od-link4-teraz-takze-dla-kierowcow (data dostępu 23.09.2021).
[251] J. Oleński, *Ekonomika informacji*: *Metody,* Wydawnictwo PWE, Warszawa 2003, s. 208-220.

- informacja uogólniona, która odnosi się do zbiorów obiektów jednostkowych, a także zbiorów cech, przy czym proces łączenia obiektów można przeprowadzić w przestrzeni obiektów i ich cech za pomocą sumowania, translacji i transformacji algorytmicznej.

Ciągłe monitorowanie i przekazywanie danych na temat zagrożeń spełnia istotną rolę w ich interpretacji oraz w kształtowaniu świadomości sytuacyjnej ludności. Analiza aktualnie wykorzystywanych rozwiązań dotycząca informowania ludności w sytuacjach kryzysowych wskazuje na luki w obecnym procesie informowania o zagrożeniach, które należy uzupełnić przy wykorzystaniu zarówno tradycyjnych jak i współczesnych technologii.

Całość tego rozdziału jest profilowana potrzebą weryfikacji dwóch założonych hipotez, że:

H2: W funkcjonującym systemie informowania ludności o zagrożeniach poziom świadomości sytuacyjnej ludności nie jest determinowany złożonością tego systemu.

H3: Skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej a sprawnością systemu informowania w warunkach zagrożeń i kryzysów.

W dalszej części podrozdziału zostanie podjęta próba oceny procesów informowania ludności w sytuacjach kryzysowych w aspekcie złożoności tych procesów oraz w aspekcie skuteczności i wydajności systemu informacyjnego, a w szczególności systemu wymiany informacji dla zapewnienia ciągłości działania i kształtowania pożądanego poziomu świadomości sytuacyjnej. Podstawą weryfikacji hipotez H.2 i H.3 jest analiza odpowiedzi na pytania ankietowe od reprezentatywnej grupy respondentów, przy czym dotyczy to obywateli (załącznik nr. 2), w których ocenie został poddany stopień realizacji działań przez administrację publiczną (wyk. 4.3) oraz pytanie ankietowe skierowane do ZZK (załącznik nr. 3) nt. istotności i możliwości najważniejszych działań w kontekście skuteczności funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń (wyk. 4.4) oraz świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów (wyk. 4.5). Badanie przeprowadzone zostało na próbie 112 obywateli. Do oceny stopnia realizacja działań przez administrację publiczną przyjęto 5-cio stopniową skalę określającą stopień zgody z poszczególnym stwierdzeniem (1 – bardzo niski, 2 –

niski, 3 – umiarkowany, 4 – wysoki, 5 – bardzo wysoki). Ankietowani dokonali oceny poszczególnych stwierdzeń określając, w jakim stopniu się z nimi zgadzają. Ocenie poddane zostały aktualne i możliwe do wykorzystania narzędzia i technologie w procesie informowania ludności o zagrożeniach. Na wykresie 4.3 przedstawiono rozkład odpowiedzi obywateli wg zawartych w ankiecie stwierdzeń.

Wykres 4.3. Ocena stopnia realizacji działań przez administrację publiczną (N=112)

Źródło: opracowanie własne

W celu określenia stopnia zgody z ocenianymi stwierdzeniami utworzone zostały 3 przedziały zgodne ze schematem. zaprezentowanym w rozdziale metodyczne podstawy badań (rys. 2.1). Przedziały te posłużyły do oceny poziomu zgodności ze

stwierdzeniami zawartymi w ankiecie (tab. 4.2.), przy czym ankietowanym zostały przedstawione następujące stwierdzenia:

1. *Rozpowszechniać informację o zagrożeniach w miejscach publicznych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 33 osoby oceniają przydatność rozpowszechniania informacji o zagrożeniach w miejscach publicznych na bardzo wysokim poziomie, a 36 na wysokim poziomie, co pokazuje, że 61% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność rozpowszechniania informacji o zagrożeniach na niskim poziomie stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (12) oraz bardzo niski (9). Na tej podstawie stwierdzono, że przydatność informacji o zagrożeniach w miejscach publicznych kształtuje się na akceptowalnym poziomie (średnia ocena poziomu i wynosi 3,73).

2. *Rozpowszechniać informacje o zagrożeniach w środkach transportu publicznego i prywatnego*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 34 osoby oceniły przydatność rozpowszechniania informacji o zagrożeniach w środkach transportu publicznego i prywatnego na bardzo wysokim poziomie, a 27 na wysokim poziomie, co pokazuje, że 55% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność rozpowszechniania informacji o zagrożeniach na niskim poziomie stanowią 45% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (31), niski (10) oraz bardzo niski (10). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność informacji o zagrożeniach w środkach transportu publicznego i prywatnego kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,62.

3. *Stworzyć audycje radiowo-telewizyjne o zagrożeniach w Polsce w celu zwiększenia świadomości o nich*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 35 osób oceniło przydatność audycji radiowo-telewizyjnych na bardzo wysokim poziomie, a 22 na wysokim poziomie, co pokazuje, że 50% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność rozpo-

wszechniania tego typu informacji na niskim poziomie stanowią 50% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (35), niski (12) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność stworzenia tego typu audycji kształtuje się na akceptowalnym, ale niskim poziomie i wynosi 3,52.

4. *Udostępniać więcej informacji o zagrożeniach w mediach społecznościowych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 41 osób oceniło przydatność udostępniania informacji o zagrożeniach w mediach społecznościowych na bardzo wysokim poziomie, a 37 na wysokim poziomie, co pokazuje, że 69% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność udostępniania tego typu informacji na niskim poziomie stanowią 31% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (20), niski (6) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność informacji o zagrożeniach w mediach społecznościowych na akceptowalnym (dość wysokim) poziomie i wynosi 3,87.

5. *Wykorzystać symulatory do modelowania scenariuszy zagrożeń*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 27 osób oceniło przydatność wykorzystania symulatorów do modelowania scenariuszy zagrożenia bardzo wysokim poziomie, a 41 na wysokim poziomie, co pokazuje, że 60% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność rozpowszechniania tego typu informacji na niskim poziomie stanowią 40% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (25), niski (12) oraz bardzo niski (7). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność modelowania scenariuszy o zagrożeniach na akceptowalnym (średnim) poziomie i wynosi 3,62.

6. *Rozszerzyć tradycyjne środki informowania o zagrożeniach o współczesne technologie*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 40 osób oceniło rozszerzenia tradycyjnych środków informowania o zagrożeniach o współczesne technologie na bardzo wysokim poziomie, a 33 na wysokim poziomie, co pokazuje, że 65% uważa za przydatne wykorzystanie tego

typu rozwiązania. Osoby, które oceniły przydatność rozpowszechniania tego typu informacji na niskim poziomie stanowią 35% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (24), niski (7) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność rozszerzenia tradycyjnych środków informowania ludności o zagrożeniach o współczesne technologie kształtuje się na bardzo wysokim poziomie i wynosi 3,80.

7. *Wykorzystać nowoczesne technologie w celu zwiększenia poziomu bezpieczeństwa*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 41 osób oceniło przydatność wykorzystania nowoczesnych technologii w celu zwiększenia poziomu bezpieczeństwa na bardzo wysokim poziomie, a 35 na wysokim poziomie, co pokazuje, że 67% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność rozpowszechniania tego typu informacji na niskim poziomie stanowią 33% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (6) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność wykorzystania nowoczesnych technologii kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,85.

8. *Przygotować poradniki o zagrożeniach dla ludności*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 37 osób oceniło przydatność poradników o zagrożeniach na bardzo wysokim poziomie, a 34 na wysokim poziomie, co pokazuje, że 63% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu poradników na niskim poziomie stanowią 37% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (19), niski (11) oraz bardzo niski (11). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność poradników o zagrożeniach kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,67.

9. *Zwiększyć nacisk na poprawię świadomości ludności o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 33 osoby oceniło przydatność zwiększenia świadomości sytuacyjnej ludności o zagrożeniach na bardzo wysokim poziomie, a 41 na wysokim poziomie, co pokazuje, że 66% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby,

które oceniły przydatność tego typu poradników na niskim poziomie stanowią 34% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (23), niski (7) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę poziomu przydatności. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,76.

10. *Zmodernizować aktualne alerty wysyłane przez Rządowe Centrum Bezpieczeństwa*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 28 osób oceniło potrzebę zmodernizowania aktualnych alertów RCB na bardzo wysokim poziomie, a 32 na wysokim poziomie, co pokazuje, że 53% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę ,modyfikacji poradników na niskim poziomie stanowią 47% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (31), niski (13) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę modernizacji aktualnych alertów RCB. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym, ale niskim poziomie i wynosi 3,53.

11. *Zmienić formę aktualnego sposobu informowania ludności o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 29 osób oceniło potrzebę zmiany aktualnego sposobu informowania ludności o zagrożeniach na bardzo wysokim poziomie, a 40 na wysokim poziomie, co pokazuje, że 61% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (27), niski (7) oraz bardzo niski (9). Dane zawarte w tabeli 4.2 umożliwiają zmiany aktualnego sposobu informowania ludności o zagrożeniach. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,65.

12. *Zacieśnić współpracę między* podmiotami *zarządzania kryzysowego*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 31 osób oceniło potrzebę współpracy między podmiotami zarządzania kryzysowego na bardzo wysokim poziomie, a 38 na wysokim poziomie, co pokazuje, że 61% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły

potrzebę współpracy na niskim poziomie stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (27), niski (8) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności. współpracy między podmiotami zarządzania kryzysowego. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (wysokim) poziomie i wynosi 3,71.

13. *Organizować konferencje i seminaria informacyjne*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 37 osób oceniło potrzebę organizacji konferencji i seminariów informacyjnych na bardzo wysokim poziomie, a 36 na wysokim poziomie, co pokazuje, że 61% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę konferencji i seminariów na niskim poziomie stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (19), niski (10) oraz bardzo niski (10). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności konferencji oraz seminariów informacyjnych. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,68.

14. *Uświadamiać ludność w zakresie zagrożeń oraz ochrony przed nimi*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 35 osób oceniło potrzebę uświadamiania ludności o zagrożeniach na bardzo wysokim poziomie, a 45 na wysokim poziomie, co pokazuje, że 71% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność uświadamiania na niskim poziomie stanowią 29% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (16), niski (8) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności uświadamiania w zakresie zagrożeń oraz ochrony przed nimi. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (wysokim) poziomie i wynosi 3,81.

15. *Przeprowadzać więcej zajęć w szkołach o tematyce zarządzania kryzysowego*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 31 osób oceniło potrzebę przeprowadzania zajęć w szkołach o tematyce zarządzania kryzysowego na bardzo wysokim poziomie, a 41 na wysokim poziomie, co pokazuje, że 64% uważa za przydatne wykorzystanie tego typu rozwiązania.

Osoby, które oceniły przydatność zajęć w szkole na niskim poziomie stanowią 36% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (20), niski (12) oraz bardzo niski (8). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności uświadamiania w zakresie zagrożeń oraz ochrony przed nimi. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (wysokim) poziomie i wynosi 3,67.

16. *Przeprowadzać coroczne szkolenia, ćwiczenia dla zespołów zarządzania kryzysowego*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 31 osób oceniło przeprowadzania corocznych szkoleń ZZK na bardzo wysokim poziomie, a 41 na wysokim poziomie, co pokazuje, że 64% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność szkoleń na niskim poziomie stanowią 36% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (20), niski (11) oraz bardzo niski (9). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności uświadamiania w zakresie zagrożeń oraz ochrony przed nimi. Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,67.

17. *Stworzyć większą liczbę etatów odpowiedzialnych za zarządzanie kryzysowe*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 30 osób oceniło potrzebę stworzenia większej liczby etatów na bardzo wysokim poziomie, a 34 na wysokim poziomie, co pokazuje, że 57% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność stworzenia większej liczby etatów na niskim poziomie stanowią 43% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (25), niski (10) oraz bardzo niski (10). Dane zawarte w tabeli 4.2 umożliwiają ocenę przydatności uświadamiania w zakresie zagrożeń Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (niskim) poziomie i wynosi 3,33.

Warto w tym miejscu zauważyć, że w skali 3-stopniowej oceny akceptacji określonych stwierdzeń nie można potwierdzić oceny w pełni zadowalającej, ale również nie ma wskazań statystycznie negatywnych.

W celu weryfikacji powyższych stwierdzeń przy pomocy oprogramowania PS IMAGO PRO wyznaczone zostały statystki pozycji (tab. 4.2).

Tabela 4.2. Oceny respondentów wg zidentyfikowanych czynników

Symbol czynnika	Nazwa czynnika	Średnia arytmetyczna (ocena)
C1	Rozpowszechniać informację o zagrożeniach w miejscach publicznych	3,73
C2	Rozpowszechniać informacje o zagrożeniach w środkach transportu publicznego i prywatnego	3,62
C3	Stworzyć audycje radiowo-telewizyjne o zagrożeniach w Polsce w celu zwiększenia świadomości o nich	3,52
C4	Udostępniać więcej informacji o zagrożeniach w mediach społecznościowych	3,87
C5	Wykorzystać symulatory do modelowania scenariuszy zagrożeń	3,62
C6	Rozszerzyć tradycyjne środki informowania o zagrożeniach o współczesne technologie	3,8
C7	Wykorzystać nowoczesne technologie w celu zwiększenia poziomu bezpieczeństwa	3,85
C8	Przygotować poradniki o zagrożeniach dla ludności	3,67
C9	Zwiększyć nacisk na poprawię świadomości ludności o zagrożeniach	3,76
C10	Zmodernizować aktualne alerty wysyłane przez Rządowe Centrum Bezpieczeństwa	3,53
C11	Zmienić formę aktualnego sposobu informowania ludności o zagrożeniach	3,65
C12	Zacieśnić współpracę między podmiotami zarządzania kryzysowego	3,71
C13	Organizować konferencje i seminaria informacyjne	3,68
C14	Uświadamiać ludność w zakresie zagrożeń oraz ochrony przed nimi	3,81
C15	Przeprowadzać więcej zajęć w szkołach o tematyce zarządzania kryzysowego	3,67
C16	Przeprowadzać coroczne szkolenia, ćwiczenia dla zespołów zarządzania kryzysowego	3,67
C17	Stworzyć większą liczbę etatów odpowiedzialnych za zarządzanie kryzysowe	3,33

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

Następnie oszacowano wartości średniej dla próby badawczej. W tym celu wykorzystany został wzór 2.1., który przyjmuje następującą formułę:

$$ZSIL^{252} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.2.)$$

Następnie obliczono średnią całej próby (tab. 4.5), która wynosi 3,676882.

Tabela 4.3. Statystyki opisowe dla wskaźnika ZSIL

Statystyka	Wartość
N	112
Rozstęp	4,00
Minimum	1,00
Maksimum	5,00
Średnia	**3,676882**
Odchylenie standardowe	0,92970
Wariancja	0,864
Skośność	-1,034
	0,228
Kurtoza	1,317
	0,453

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

W celu weryfikacji hipotezy H.2 określono poziom świadomości sytuacyjnej ludności zgodnie ze schematem zaprezentowanym w rozdziale II (rys. 2.1).

W kolejnym kroku dokonano analizy skupień (metodą k-średnich) w oparciu wystandaryzowaną zmienną ZSILL (tab. 4.4).

Tabela 4.4 ukazuje, że spośród 112 badanych 8 osób (8%) oceniło złożoność systemu informowania ludności na niskim poziomie, 60 osób (53%) - poziomie umiarkowanym, a 44 (39%) poziomie wysokim.

[252] ZSIL – złożoność systemu informowania ludności.

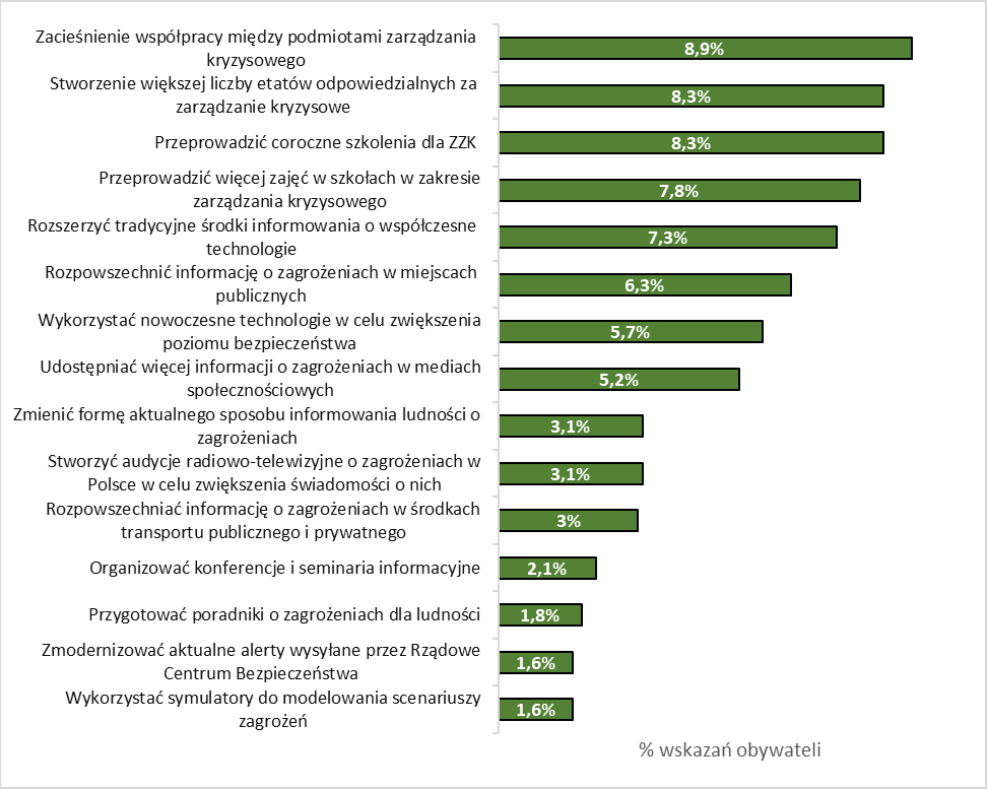
Tabela 4.4. Skupienie odchyleń pod kątem poziomu świadomości sytuacyjnej (N=112)

	Skupienie		
	1	2	3
	Niski poziom złożoność systemu informowania ludności	Średni poziom złożoność systemu informowania ludności	Wysoki złożoność systemu informowania ludności
Stand: złożoność systemu informowania ludności	-2,55967	-0,31511	0,89510
Liczba obserwacji w każdym ze skupień	8	60	44

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

Wysoki poziom systemu informowania ludności ma kluczowe znaczenie dla bezpieczeństwa publicznego, dlatego wymaga wysokiego poziomu odpowiedzialności i zaufania ze strony instytucji i władz odpowiedzialnych za zarządzanie kryzysowe.

Następnie określone zostały najważniejsze działania w kontekście funkcjonowania systemu informowania ludności o zagrożeniach w momencie zaistnienia sytuacji kryzysowych (wyk. 4.4).



Wykres 4.4. Najważniejsze działania w kontekście funkcjonowania systemu informowania ludności o zagrożeniach w momencie zaistnienia sytuacji kryzysowych (N=112)

Źródło: opracowanie własne

Analiza odpowiedzi wykazała, że dla ankietowanych najważniejszymi działaniami są:

- zacieśnienie współpracy między podmiotami zarządzania kryzysowego (8,9%),

- stworzenie większej liczby etatów odpowiedzialnych za zarządzanie kryzysowe (8,3%),
- przeprowadzić coroczne szkolenia dla ZZK (8,3%).
- przeprowadzić więcej zajęć w szkołach w zakresie zarządzania kryzysowego (7,8%),
- rozszerzyć tradycyjne środki informowania o współczesne technologie (7,3%).
- rozpowszechnić informację o zagrożeniach w miejscach publicznych (6,3%)

Na podstawie analizy odpowiedzi można zatem przyjąć, że w procesie skutecznego informowania ludności o zagrożeniach główną rolę odgrywa przekaz informacji, a więc szkolenie z wykorzystywania tradycyjnej technologii oraz jej rozszerzenie, i przeprowadzanie szkoleń zarówno dla ZZK jak i obywateli, co pokazuje, że istnieje silna potrzeba zwiększania metod przekazywania informacji na temat zagrożeń. W ocenie ankietowanych działania takie, jak modyfikacja aktualnych rozwiązań np. Alertów RCB oraz wykorzystanie symulatorów odgrywają, drugorzędną rolę w procesie informowania ludności o zagrożeniach oraz w kreowaniu świadomości sytuacyjnej na temat zagrożeń.

W celu weryfikacji hipotezy H.2 określono ocenę poziomu złożoności systemu informowania ludności wyrażoną liczbą dodatkowych aktywności (działań/podprocesów) zgodnie ze schematem zaprezentowanym w Rozdziale II (rys. 2.2). Analiza danych zawartych w tabeli 4.5 falsyfikuje hipotezę 2, ponieważ statystycznie złożoność systemu informowania ludności plasuje się na średnim poziomie i może wg ankietowanych dodatnio wpływać na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów. Dla pełnej oceny procesu informowania ludności w sytuacjach kryzysowych w RP podjęto próbę zweryfikowana hipotezy H.3. W tym celu ocenie poddane zostały odpowiedzi na pytanie ankietowe skierowane do obywateli (załącznik nr. 2), w którym oceniono stopień realizacji działań przez administrację publiczną (wyk. 4.5) oraz pytanie ankietowe skierowane do ZZK (załącznik nr. 3), w którym ocenie poddana została istotność najważniejszych działań w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń (wyk. 4.5). Do oceny stopnia realizacja działań przez administrację publiczną przyjęto 5-cio stopniową skalę określającą stopień zgody z poszczególnym stwierdzeniem (1 –bardzo niski, 2 – niski, 3 – umiarkowany, 4 – wysoki, 5 – bardzo wysoki). Ankietowani dokonali oceny poszczególnych stwierdzeń

określając, w jakim stopniu się z nimi zgadzają. Ocenie poddane zostały aktualne i możliwe do wykorzystania narzędzia i technologie w procesie informowania ludności o zagrożeniach.

Wykres 4.5. Ocena stopnia realizacji działań przez administrację publiczną w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń (N=112)
Źródło: opracowanie własne

Na wykresie 4.5 przedstawiono rozkład odpowiedzi obywateli na zawarte w ankiecie stwierdzenia.

W celu określenia stopnia zgody z powyższymi stwierdzeniami utworzone zostały 3 przedziały zgodne z modelem zaprezentowanym w rozdziale metodyczne podstawy badań (rys. 2.1), które posłużyły do oceny poziomu statystycznej zgody ze stwierdzeniami zawartymi w ankiecie (tab. 4.5).

Do oceny stopnia realizacja działań przez administrację publiczną sformułowano następujące stwierdzenia:

1. *Utworzenie grup reagowania kryzysowego spośród mieszkańców może przyczynić się do poprawy świadomości o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 34 osoby oceniają przydatność utworzenia grup reagowania kryzysowego spośród mieszkańców na bardzo wysokim poziomie, a 36 na wysokim poziomie, co pokazuje, że 62% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność utworzenia grup reagowania kryzysowego spośród mieszkańców na niskim poziomie stanowią 38% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (12) oraz bardzo niski (8). Na tej podstawie stwierdzono, że przydatność utworzenia grup reagowania kryzysowego spośród mieszkańców może przyczynić się do poprawy świadomości o zagrożeniach kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,74.

2. *Zwiększenie poziomu świadomości ludności o zagrożeniach jest niezbędne do poprawy poziomu bezpieczeństwa (obniżenia ryzyka ich materializacji)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 36 osób oceniło przydatność zwiększenia poziomu świadomości ludności o zagrożeniach na bardzo wysokim poziomie, a 44 na wysokim poziomie, co pokazuje, że 71% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 29% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (19), niski (5) oraz bardzo niski (8). Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości ludności o zagrożeniach kształtuje się na zadowalającym (wysokim) poziomie i wynosi 3,85.

3. *Dostosowanie systemu informowania ludności do aktualnych rozwiązań techniczno- technologicznych może przyczynić się do poprawy świadomości o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 27 osób oceniło potrzebę dostosowania systemu informowania ludności do aktualnych rozwiązań techniczno- technologicznych w celu poprawy świadomości o zagrożeniach na bardzo wysokim poziomie, a 45 na wysokim poziomie, co pokazuje, że 64% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 36% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (21), niski (12) oraz bardzo niski 6). Na tej podstawie stwierdzono, że przydatność dostosowania systemu informowania ludności do aktualnych rozwiązań techniczno- technologicznych kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,76.

4. *Wprowadzenie dla ludności szkoleń e-learningowych na temat zagrożeń może przyczynić się do poprawy poziomu bezpieczeństwa (obniżenia ryzyka ich materializacji)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 29 osób oceniło przydatność *szkoleń e-learningowych na temat zagrożeń* na bardzo wysokim poziomie, a 42 na wysokim poziomie, co pokazuje, że 63% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 37% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (27), niski (10) oraz bardzo niski (4). Na tej podstawie stwierdzono, że przydatność wprowadzenia dla ludności szkoleń e-learningowych na akceptowalnym (dość wysokim) poziomie i wynosi 3,73.

5. *Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do obiektywizacji oceny i uproszczenia procesu postępowania w trakcie zagrożenia*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 34 osoby oceniły wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach w celu uproszczenia procesu postępowania w trakcie zagrożenia na bardzo wysokim poziomie, a 34 na wysokim poziomie, co pokazuje, że 60% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 40% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (26), niski (12) oraz bardzo niski (6). Na tej podstawie stwierdzono, że przydatność wykorzystania sztucznej inteligencji kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,62.

6. *Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do zmniejszenia czasu reakcji na wypadek wystąpienia zagrożenia*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 40 osób oceniło przydatność wykorzystania sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach na bardzo wysokim poziomie, a 33 na wysokim poziomie, co pokazuje, że 65% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 35% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (24), niski (7) oraz bardzo niski (8). Na tej podstawie stwierdzono, że przydatność wykorzystania sztucznej inteligencji kształtuje się kształtuje się na akceptowalnym (dość wysokim) poziomie i wynosi 3,75.

7. *Wykorzystanie nowoczesnych technologii w środkach transportu publicznego może przyczynić się do zwiększenia poziomu bezpieczeństwa (obniżenia ryzyka materializacji zagrożeń z tym związanych)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 44 osoby oceniły przydatność wykorzystanie nowoczesnych technologii w środkach transportu publicznego na bardzo wysokim poziomie, a 35 na wysokim poziomie, co pokazuje, że 70% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 30% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (23), niski (6) oraz bardzo niski (4). Na tej podstawie stwierdzono, że przydatność wykorzystania nowoczesnych technologii kształtuje się na zadowalającym (bardzo wysokim) poziomie i wynosi 3,97.

8. *Wykorzystanie mediów społecznościowych w procesie informowania ludności o zagrożeniach może zwiększyć poziom bezpieczeństwa (obniżenia ryzyka ich materializacji)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 40 osób oceniło przydatność mediów społecznościowych w procesie informowania ludności o zagrożeniach na bardzo wysokim poziomie, a 38 na wysokim poziomie, co pokazuje, że 69% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 31% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (21), niski (7) oraz bardzo niski (6). Na tej podstawie stwierdzono, że przydat-

ność mediów społecznościowych kształtuje się na zadowalającym (wysokim) poziomie i wynosi 3,88.

9. *Wysyłanie przez RCB komunikatów o zagrożeniach oraz procedur postępowania w trakcie jego wystąpienia może przyczynić się do zmniejszenia jego skutków*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 35 osób oceniło przydatność wysyłania przez RCB komunikatów o zagrożeniach oraz procedur postępowania na bardzo wysokim poziomie, a 46 na wysokim poziomie, co pokazuje, że 72% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie stanowią 28% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (20), niski (6) oraz bardzo niski (5). Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na zadowalającym (wysokim) poziomie i wynosi 3,89.

10. *Zmiana formy komunikatów przesyłanych przez RCB na tekstowo-graficzne może przyczynić się do poprawy poziomu świadomości ludności*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 31 osób oceniło potrzebę zmodernizowania aktualnych komunikatów RCB na bardzo wysokim poziomie, a 47 na wysokim poziomie, co pokazuje, że 69% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę modyfikacji poradników na niskim poziomie stanowią 31% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (22), niski (6) oraz bardzo niski (6). Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (wysokim) poziomie i wynosi 3,81.

11. *Wdrożenie do systemu informowania ludności możliwości przesyłania informacji o zagrożeniach na współczesne urządzenia (smartfon, smartwatch komputery tablety itp.) w formie graficznej może przyczynić się do podwyższenia poziomu rozumienia i tym samym do zwiększenia poziomu świadomości ludności*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 31 osób oceniło potrzebę wdrożenia do systemu informowania ludności możliwości przesyłania informacji o zagrożeniach na współczesne urządzenia na bardzo wysokim poziomie, a 32 na wysokim poziomie, co pokazuje, że 56% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę

wdrożenia tego typu rozwiązania na niskim poziomie stanowią 44% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (30), niski (11) oraz bardzo niski (8). Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,60.

12. *Organizowanie spotkań mających na celu uświadomienie ludności o zagrożeniach może przyczynić się do zwiększenia poziomu bezpieczeństwa (obniżenia ryzyka ich materializacji)*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 32 osoby oceniły potrzebę organizowanie spotkań mających na celu uświadomienie ludności o zagrożeniach na bardzo wysokim poziomie, a 45 na wysokim poziomie, co pokazuje, że 68% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę współpracy na niskim poziomie stanowią 32% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (27), niski (8) oraz bardzo niski (8). Na tej podstawie stwierdzono, że przydatność organizowania spotkań mających na celu uświadomienie ludności o zagrożeniach kształtuje się na zadowalającym (wysokim) poziomie i wynosi 3,81.

13. *Poinformowanie ludności o sposobie postępowania w trakcie wystąpienia zagrożenia może przyczynić się do racjonalnego (optymalnego) działania służb ratowniczych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 30 osób oceniło potrzebę poinformowania ludności o sposobie postępowania w trakcie wystąpienia zagrożenia na bardzo wysokim poziomie, a 39 na wysokim poziomie, co pokazuje, że 61% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę konferencji i seminariów na niskim poziomie stanowią 39% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (24), niski (14) oraz bardzo niski (5). Na tej podstawie stwierdzono, że przydatność zwiększenia poziomu świadomości sytuacyjnej kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,68.

14. *Niezwłoczne informowanie ludności w momencie ryzyka wystąpienia sytuacji kryzysowych może przyczynić się do zniwelowania jego skutków*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 36 osób oceniło potrzebę niezwłocznego informowanie ludności w momencie ryzyka wystąpienia sytuacji kryzysowych na bardzo wysokim poziomie, a 37 na

wysokim poziomie, co pokazuje, że 65% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły potrzebę niezwłocznego informowania na niskim poziomie stanowią 35% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (28), niski (6) oraz bardzo niski (5Na tej podstawie stwierdzono, że przydatność niezwłocznego informowania ludności kształtuje się na zadowalającym (wysokim) poziomie i wynosi 3,81.

15. *Informowanie ludności o zagrożeniach odgrywa kluczową rolę w procesie kreowania świadomości o zaistniałych zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 obywateli 34 osoby oceniły, że informowanie ludności o zagrożeniach odgrywa kluczową rolę w procesie kreowania świadomości o zaistniałych zagrożeniach na bardzo wysokim poziomie, a 33 na wysokim poziomie, co pokazuje, że 59% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność informowania ludności na niskim poziomie stanowią 41% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowany (28), niski (9) oraz bardzo niski (8). Na tej podstawie stwierdzono, że informowanie ludności kształtuje się na akceptowalnym (średnim) poziomie i wynosi 3,59.

W tabeli 4.5 zawarte są średnie arytmetyczne oceny respondentów dla czynników związanych z oceną przydatności w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń.

Tabela 4.5. Średnie oceny respondentów dla czynników związanych z oceną przydatności w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń

Symbol czynnika	Nazwa czynnika	Średnia arytmetyczna (ocena)
1	Utworzenie grup reagowania kryzysowego spośród mieszkańców może przyczynić się do poprawy świadomości o zagrożeniach	3.74
2	Zwiększenie poziomu świadomości ludności o zagrożeniach jest niezbędne do poprawy świadomości o nich	3.85
3	Dostosowanie systemu informowania ludności do aktualnych rozwiązań techniczno- technologicznych może przyczynić się do poprawy świadomości o zagrożeniach	3.76
4	Wprowadzenie dla ludności szkoleń e-learningowych na temat zagrożeń może przyczynić się do poprawy ich świadomości o nich	3.73
5	Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do uproszczenia procesu postępowania w trakcie zagrożenia	3.62
6	Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do zmniejszenia czasu reakcji na wypadek wystąpienia zagrożenia	3.75
7	Wykorzystanie nowoczesnych technologii w środkach transportu publicznego może przyczynić się do zwiększenia poziomu świadomości o nich	3.97
8	Wykorzystanie mediów społecznościowych w procesie informowania ludności o zagrożeniach może zwiększyć poziom świadomości o nich	3.88
9	Wysyłanie przez RCB komunikatów o zagrożeniach oraz procedur postępowania w trakcie jego wystąpienia może przyczynić się do zmniejszenia jego skutków	3.89
10	Zmiana formy komunikatów przesyłanych przez RCB na tekstowo-graficzne może przyczynić się do poprawy poziomu świadomości ludności	3.81

Tabela 4.5. cd.. Średnie oceny respondentów dla czynników związanych z oceną przydatności w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń

11	Wdrożenie do systemu informowania ludności możliwości przesyłania informacji o zagrożeniach na współczesne urządzenia (smartfon, smartwatch komputery, tablety itp.) w formie graficznej może przyczynić się do zwiększenia poziomu świadomości ludności	3.6
12	Organizowanie spotkań mających na celu uświadomienie ludności o zagrożeniach może przyczynić się do zwiększenia świadomości o nich	3.81
13	Poinformowanie ludności o sposobie postępowania w trakcie wystąpienia zagrożenia może przyczynić się do optymalnego działania służb ratowniczych	3.68
14	Niezwłoczne informowanie ludności w momencie ryzyka wystąpienia sytuacji kryzysowych może przyczynić się do zniwelowania jego skutków	3.83
15	Informowanie ludności o zagrożeniach odgrywa kluczową rolę w procesie kreowania świadomości o zaistniałych zagrożeniach	3.68

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

Następnie oszacowano wartości średniej dla próby badawczej. W tym celu wykorzystany został wzór 2.1, który przyjmuje następującą formułę:

$$WSIL^{253} = \frac{C1 + C2 + C3 + C4 + C5 + C6 + C7 + C8 + C9 + C10 + C11 + C12 + C13 + C14 + C15}{15} \quad (2.3)$$

Następnie przy wykorzystaniu *PS IMAGO PRO* została obliczona średnia z całej próby badawczej (N=112) – średnia wskaźnika dla wszystkich respondentów (tabela 4.6.).

Tabela 4.6. Statystyki opisowe dla wskaźnika WSIL (N=112).

Statystyka	Wartość
Rozstęp	4,00
Minimum	1,00
Maksimum	5,00
Średnia	**3,773333**
Odchylenie standardowe	0,82299
Wariancja	0,677
Skośność	0,228

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

W celu weryfikacji hipotezy H.3 określono poziom świadomości sytuacyjnej ludności zgodnie ze schematem zaprezentowanym w rozdziale II (rys. 2.1).

Następnie dokonano analizy skupień (metodą k-średnich) w oparciu wystandaryzowaną zmienną WSIL (tab. 4.7).

Tabela 4.7. Ostateczne centra skupień

	Skupienie		
	1	2	3
	Niski poziom wydajności systemu informowania ludności	Średni poziom wydajnośc systiemu informowania ludności	Wysoki poziom wydajności systemu informowania ludności
Stand: złożoność systemu informowania ludności	-2,41425	-0,32792	0,98827
Liczba obserwacji w każdym ze skupień	7	66	39

Źródło: opracowanie własne przy wykorzystaniu oprogramowania PS IMAGO PRO

[253] WSIL - wydajność systemu informowania ludności.

Tabela 4.7. ukazuje, że spośród 112 badanych 7 osób (6%) oceniło wydajność systemu informowania na niskim poziomie, 66 osób (59%) na umiarkowanym poziomie, a 39 osób (35%) na wysokim poziomie.

Analiza tabeli 4.7. falsyfikuje hipotezę, ponieważ skuteczność i wydajność systemu informowania ludności w sytuacji kryzysowej są na akceptowalnym (średnim) poziomie, zgodnie z przyjętym wcześniej 3 – poziomowym modelem (rys. 2.1). Ostatecznie hipoteza H.3 została sfalsyfikowana, ponieważ wydajność i skuteczność systemu informowania ludności oraz jego sprawność dodatnio wpływają na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów.

4.6. Podsumowanie rozdziału czwartego

Sprawne i skuteczne komunikowanie to niezbędny czynnik sukcesu we wszelkich relacjach społecznych, politycznych i biznesowych, a ich znaczenie przejawia się szczególnie w różnego rodzaju sytuacjach kryzysowych. Zdarzenia tego typu wymagają określonych sposobów działania, dlatego proces komunikowania się wymaga odpowiedniego zarządzania. Należy przyjąć, że proces uczenia się to wymiana informacji, pomysłów i uczuć za pomocą środków werbalnych i niewerbalnych, dostosowanych do kontekstu sytuacyjnego lub środowiska społecznego[254]. Należy nim zarządzać, aby osiągnąć akceptowalne rezultaty. Ważnym czynnikiem sukcesu jest zrozumienie przekazywanych informacji (komunikatów). Dotyczy to w szczególności różnego rodzaju sytuacji kryzysowych, które wymagają określonych metod i narzędzi oraz stosowania wydajnych strategii komunikacyjno-informacyjnych[255]. Społeczne postrzeganie złożoności i ryzyka sytuacji kryzysowej, a także zaufanie do interesariuszy i decydentów odpowiedzialnych za rozwiązywanie kryzysów w dużej mierze zależy od ich umiejętności w zakresie doboru treści, formy i sposobu zarządzania procesem komunikowania się. Podobnie jak wszystkie inne rodzaje umiejętności, zdolności komunikacyjne muszą być doskonalone. Posiadanie dobrych umiejętności komunikowania się w rzeczywistości oznacza wiedzę, jak sformułować wiadomość w kontekście procesu komunikacyjnego i jak przekazać tę wiadomość tym, dla których jest przeznaczona, przy jak najmniejszym szumie komunikacyjnym, co mogłoby mieć wpływ na zrozumienie wiadomości oraz na jej formę i treść z podkreśleniem wartości informacyjnej i wiarygodności. Sytuacje kryzysowe wymagają szybkiego

[254] T.J. Dąbrowski, *Komunikacja kryzysowa jako narzędzie kształtowania reputacji,* "Marketing i Rynek" 2010, 8, s.15.
[255] D. Domalewska, *Wielowymiarowość komunikacji w kontekście bezpieczeństwa*. Komunikacja w sytuacjach kryzysowych i komunikacja strategiczna, Warszawa 2020, s.90-135.

reagowania i wysokiej jakości przekazu do wszystkich grup docelowych w ramach ogółu społeczeństwa przed, w trakcie i po kryzysie[256].

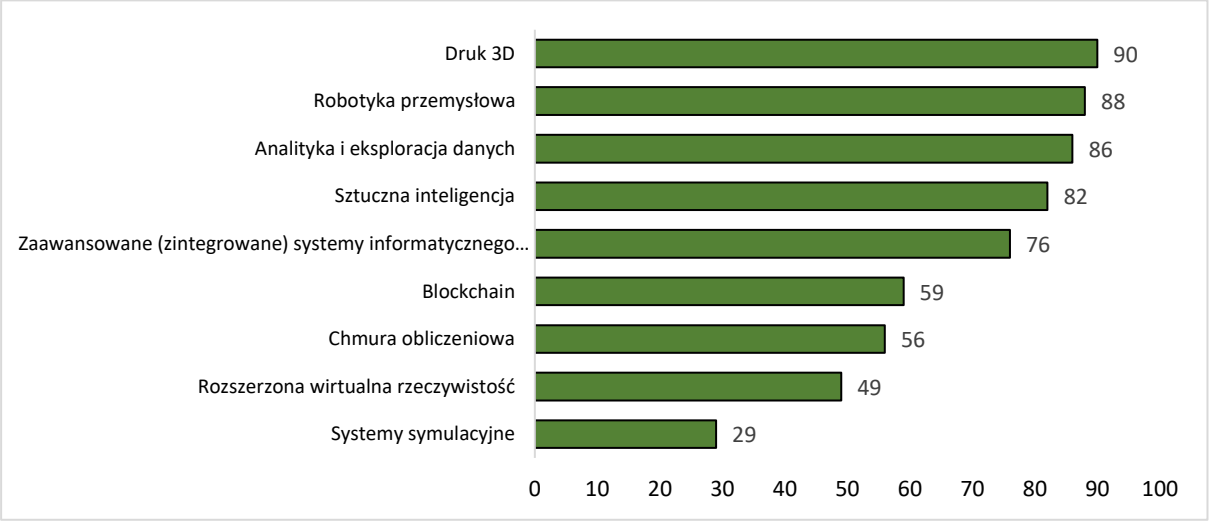
W rozdziale tym przedstawiono uwarunkowania kreowania świadomości sytuacyjnej w istniejącym systemie i określono determinanty wzrostu jej poziomu. Weryfikacja hipotezy H2 potwierdza, że w badanym systemie informowania ludności o zagrożeniach - poziom świadomości sytuacyjnej ludności jest dość silnie determinowany złożonością zadaniową tego systemu i możliwością wykorzystywania dodatkowych aktywności w doskonaleniu procesu postrzegania i oceny oraz rozumienia zagrożeń. Ważne przy tym jest, że (H3) - skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest akceptowalna, ale wymaga doskonalenia w zakresie podnoszenia sprawności systemu informowania w warunkach zagrożeń i kryzysów. Drogą do ulepszania tego stanu może być szersze wykorzystanie narzędzi i nowoczesnych platform technologii IT/ICT.

Rozwój współczesnych technologii IT/ICT spowodował, że dla obywateli korzystających na co dzień z urządzeń takich jak np. smartfon niektóre tradycyjne technologie mogą wydawać się niezrozumiałe lub przestarzałe. W obecnych czasach część współczesnych technologii IT/ICT może nie tylko zastąpić tradycyjne środki, ale wprowadzić nową jakość do realizacji tej klasy procesów. Niemniej jednak nie należy ograniczać się wyłącznie do współczesnych (nowoczesnych) technologii, ponieważ wśród potencjalnych odbiorców wiadomości istnieją również osoby, które ze względu na swój wiek lub też inne ograniczenia uważają tradycyjne metody komunikowania się jako najskuteczniejsze nie tylko w procesie pozyskiwania informacji o zagrożeniach, ale także jako źródło przesyłania informacji. Zidentyfikowane aktualne rozwiązania dotyczące informowania ludności w sytuacjach kryzysowych w połączeniu z prowadzonymi badaniami jednoznacznie wskazują, że pomimo względnie dobrej funkcjonalności systemu informacji publicznej należy go doskonalić poprzez rozbudowę istniejących środków i metod informowania o zagrożeniach. Dotyczy to przede wszystkim takiego modelu komunikacyjnego, aby możliwe było dotarcie do jak największej grupy odbiorców, niezależnie od tego, gdzie mieszkają i jakich technologii używają[257]. W tym celu niezbędne jest dokonanie oceny przydatności współczesnych technologii IT/ICT i ich potencjału w zarządzaniu kryzysowym. Przeprowadzone badania ukazują, że istnieje potrzeba udoskonalenia również tradycyjnych

[256] Tamże, s.90-135.
[257] Tamże, s. 90-135.

rozwiązań, z których korzysta znaczna część społeczeństwa. Technologie te mogą istotnie wspomagać funkcjonowanie systemu zarządzania kryzysowego oraz procesu informowania ludności i poprawią poziom świadomości sytuacyjnej. Dlatego też kluczowe jest uwzględnienie zarówno współczesnych technologii jak i tradycyjnych rozwiązań co zostanie wykazane w kolejnych rozdziałach rozprawy i w rozdziale koncepcyjnym. Warto również dodać, że kształtowanie odpowiedniego poziomu bezpieczeństwa stanowi wyzwanie zarówno dla państwa i Zespołów Zarządzania Kryzysowego w celu zapewnienia odpowiedniego poziomu świadomości sytuacyjnej oraz usprawnienia funkcjonowania w momencie wystąpienia kryzysu.

Jako uzupełnienie dotychczasowych rozważań przywołane zostały badania z artykułu pt. *Implications of Industry 4.0 for Security in Contemporary Organizations – Perspective of Information Strategies* z 2020 roku[258] (wyk. 4.6 i wyk.4.7). Wskazano w nich rozwiązania IT/ICT szczególnie ważne dla organizacji, a ich potencjał możliwy jest do zastosowania w zarządzaniu kryzysowym. Badanie zostało przeprowadzone na próbie N=225.



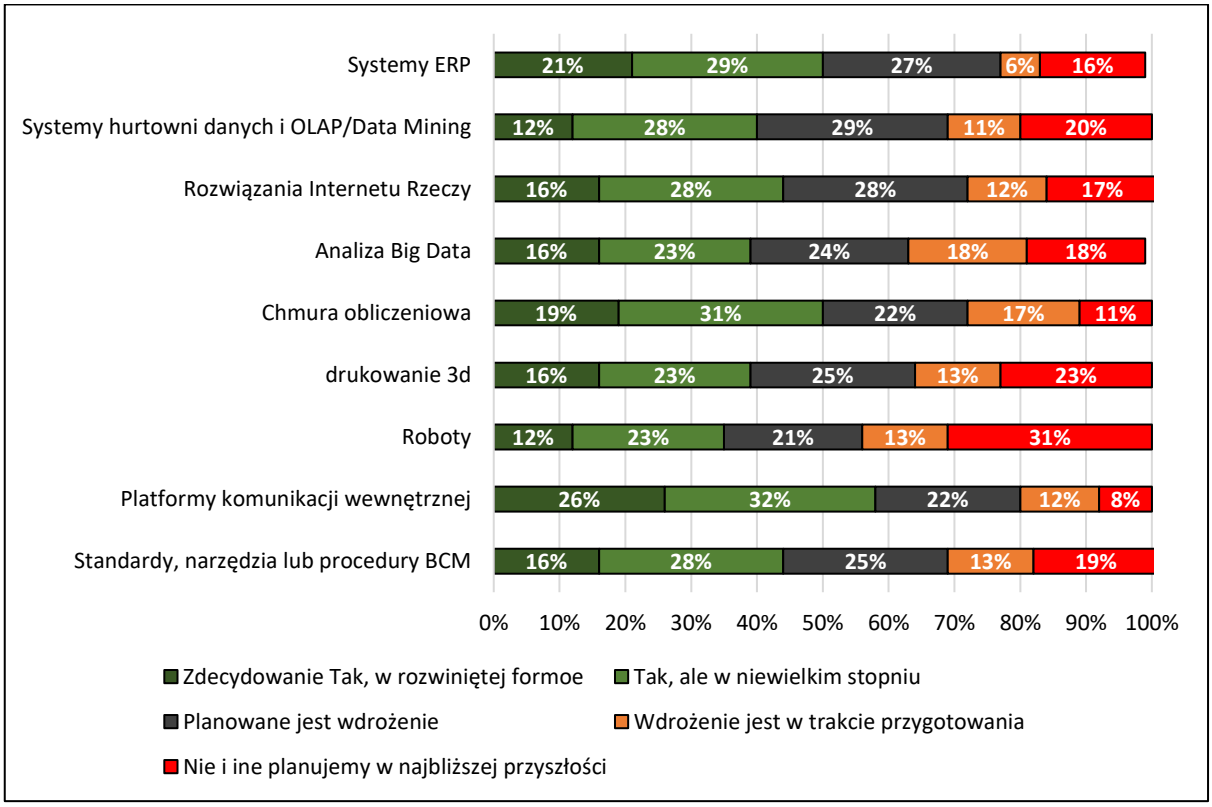
Wykres 4.6. Rozwiązania Przemysłu 4.0 szczególnie istotne dla organizacji możliwe do wykorzystania w zarządzaniu kryzysowym

Źródło opracowanie własne na podstawie badania z artykułu pt. Implications of Industry 4.0 for Security in Contemporary Organizations – Perspective of Information Strategies z 2020 roku.

Wśród odpowiedzi respondenci wskazali na: druk 3D (90 wskazań), robotyka przemysłowa (88 wskazań), analityka i *Data Minning* (86 wskazań), sztuczna inteligencja (82 wskazania) oraz Zintegrowane Systemy Informatycznego Zarządzania

[258] P. Zaskorski, J. Wozniak, *Implications of Industry 4.0 for Security in Contemporary Organizations – Perspective of Information Strategies*, European Research Studies Journal, Volume XXV, Issue 1, 2022.

i Produkcji (76 wskazań). Najmniej istotne w ocenie respondentów są: systemy symulacyjne (29 wskazań), rozszerzona i wirtualna rzeczywistość (49 wskazań), a także *Cloud Computing* (56 wskazań) i *Blockchain* (59 wskazań). (wyk. 4.6). Niskie wskazania dla *VR/AR*, *CC*, *Blockchain* oraz systemów symulacyjnych może wskazywać na nieznajomość tych technologii przez co respondenci nie dostrzegli ich potencjału w zarządzaniu kryzysowym i w procesie kształtowania świadomości sytuacyjnej.



Wykres 4.7. Zakres zastosowania wybranych rozwiązań informatycznych w organizacji (N=225)
Źródło: opracowanie własne na podstawie badania z artykułu pt. Implications of Industry 4.0 for Security in Contemporary Organizations – Perspective of Information Strategies z 2020 roku.

Warto tu również zwrócić uwagę na fakt, że badane organizacje w różnym stopniu i zakresie wykorzystują takie rozwiązania, jak platformy komunikacji wewnętrznej (58% wskazań), systemy *ERP* i usługi *Cloud Computing* (oba 50% wskazań) oraz Internetu Rzeczy (40% wskazań). Przyszłe plany wdrożeniowe współczesnych organizacji związane są z systemami hurtowni danych oraz *OLAP/Data Mining* z mechanizmami generowania wiedzy (*DM*, 29% wskazań), rozwiązaniami Internetu Rzeczy (28% wskazań) a także z systemami klasy *ERP* (27% wskazań). Ponadto w badanych organizacjach planowane jest wdrożenie takich technologii jak systemy *Big Data* (18% wskazań) oraz usługi *Cloud Computing* (17% wskazań), przy czym zastanawiające jest to, że rozwiązania takie jak roboty (31% wskazań) i druk 3D

(23% wskazań) nie są powszechnie wykorzystywane i nie są planowane do szerokiego wdrożenia w badanych organizacjach (wyk. 4.7).
Wyniki tego badania odnoszą się do przedsiębiorstw, jednakże w pewnym uproszczeniu można je odnieść do Zespołów Zarządzania Kryzysowego.

Analiza przywołanych badań miała na celu ukazanie potencjału technologii IT/ICT, które coraz częściej są wykorzystywane lub planowane jest ich wykorzystanie w organizacjach. Na podstawie zebranych informacji o technologiach, możliwa jest ich analiza pod kątem wykorzystania w zarządzaniu kryzysowym oraz w procesie kształtowania świadomości sytuacyjnej ludności na temat zagrożeń. Zaprezentowane technologie zostały poddane ocenie przydatności oraz potencjalnych sposobów wykorzystania ich w celu usprawnienia całego procesu zarządzania kryzysowego.

ROZDZIAŁ V
IDENTYFIKACJA I OCENA PRZYDATNOŚCI WSPÓŁCZESNYCH TECHNOLOGII TELEINFORMATYCZNYCH W SZK

5.1. Identyfikacja wybranych technologii użytecznych w kreowaniu świadomości sytuacyjnej

Istnieje wiele metod i narzędzi (służących zapobieganiu materializacji ryzyka oraz łagodzeniu jego negatywnych skutków dzięki ich prognozowaniu i opracowywaniu scenariuszy przebiegu możliwych zdarzeń np. symulatory zagrożeń, analiza danych historycznych, urządzenia pomiarowe itp.). Prognozy te mogą być podstawą skutecznego planowania sytuacji kryzysowych, powstałych z różnorodnych zagrożeń. Mogą temu służyć np. modele symulacyjne propagacji skutków klęsk żywiołowych oraz wielowariantowe prognozowanie skutków i planowanie przeciwdziałania tym skutkom. W każdym tego typu rozwiązaniu współczesne technologie IT/ICT stanowią istotne wsparcie wzmacniające generowanie rzetelnej wiedzy na podstawie analizy symptomów różnych zagrożeń i poszukiwania analogii do zdarzeń z przeszłości przy wieloaspektowych uwarunkowaniach. Może to być ważny czynnik kreowania świadomości sytuacyjnej.

Technologie IT/ICT można traktować jako zespół systemów technicznych, urządzeń (serwery, komputery tablety itp.), środków komunikacji (Internet, telefonia komórkowa, satelitarna, sieci *Bluetooth* i sieci bezprzewodowe) oraz profesjonalne oprogramowanie do realizacji usług informacyjnych a w tym gromadzenia i przetwarzania danych oraz dystrybucji wyników udostępnianych w elektronicznej formie[259].

Brak ścisłych regulacji prawnych w kontekście doboru technologii możliwych do wykorzystania w procesie informowania w SZK i kształtowania mechanizmów zapewniania świadomości sytuacyjnej ludności daje w pewnym stopniu swobodę wyboru form przekazywania informacji. Stąd do komunikowania się wykorzystywane są powszechnie dostępne media (radio, telewizja), Internet (komunikatory, portale społecznościowe itp.) i sieci komórkowe. Coraz powszechniej jednak eksploatowane są systemy dziedzinowe np. ISOK (Informatyczny System Osłony Kraju) obejmujący na dziś tylko obszar zagrożeń powodziowych. Tak więc z jednej strony brak odpowiednich regulacji może stanowić zaletę, a z drugiej strony mogą pojawić się problemy

[259] K. Warzecha, *Technologie informacyjno-komunikacyjne wykorzystywane przez młodzież - szanse i zagrożenia, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach,* Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2018 nr 13, s. 1-5.

z integracją z innymi systemami (w tym komercyjnymi, sprawdzonymi np. w biznesie) wykorzystywanymi współcześnie także w zarządzaniu sytuacjami kryzysowymi.

Wobec braku ogólnokrajowych, jednolitych rozwiązań informatycznych wspierających szeroko rozumiane zarządzanie kryzysowe[260], należy sięgać zarówno po standardy technologiczne, jak i rozwiązania dedykowane, które mogą znaleźć zastosowanie w zarządzaniu kryzysowym a w tym narzędzia[261]:

- gromadzące i aktualizujące dane o zdarzeniach obrazujących sytuację na szczeblu gminnym, powiatowym oraz wojewódzkim (np. Arcus 2015. NET, CAR),
- systemy reagowania kryzysowego (np. Alaska – opracowany przez resortowe Centrum Zarządzania Projektami Informatycznymi),
- dziedzinowo – funkcjonalne (np. ABAKUS – wielomodułowy system przeznaczony dla Komendy Głównej Państwowej Straży Pożarnej, DART – przeznaczony do wspomagania zarządzanie Centrum Zarządzania Kryzysowego),
- zobrazowania zagrożeń zaistniałych na terenie województwa na podkładzie mapy cyfrowej (np. CorelDRAW Graphics Suite 2021, QGIS),
- system C3M, wykorzystywany przez Wielkopolski Urząd Wojewódzki w Poznaniu oraz powiaty i gminy, jak również podmioty administracji zespolonej i niezespolone,
- obsługi magazynowej (np. MOC),
- obsługi rastrowanych map wojskowych (Pakiet Grafiki Operacyjnej 2003),
- szybkiej wymiany informacji pomiędzy jednostkami medycznymi, a koordynatorem ratownictwa medycznego (infoMed),
- kontroli funkcjonowania jednostek Państwowego Ratownictwa Medycznego (GPS Monitor Rejestr, SWD PRM),
- analizy geoprzestrzennej do wspomagania procesów decyzyjnych (Arcus-Geo, ArcGis, InterGraf),
- tworzenia georeferencyjnych baz danych i przeprowadzania analizy oraz importowania i eksportowania danych itp. (GBDOT),

[260] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 23.01.2023).
[261] P. Zaskórski, W. Zaskórski, J. Woźniak, *Świadomość sytuacyjna, a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, Wydawnictwo. CeDeWu, Warszawa 2021, s. 53.

- zintegrowanego zarządzania różnymi obszarami w SZK począwszy od systemów transakcyjnych, poprzez systemy analityczno-decyzyjne, a w tym wykorzystanie sztucznej inteligencji, Internetu Rzeczy i systemów eksploracji bardzo dużej kolekcji wielopostaciowych danych (Big_Data) z wykorzystaniem usług w modelach chmurowych.

Zastosowanie współczesnych technologii IT/ICT może znacznie ułatwić, przyspieszyć i rozszerzyć dostęp do odpowiedniej informacji w czasie rzeczywistym. Jest to jeden z powodów, dla którego należy wykorzystywać zaawansowane technologie informacyjno-komunikacyjne dla podniesienia skuteczności funkcjonowania różnych podmiotów zaangażowanych w daną sytuację kryzysową poprzez zwiększenie świadomości sytuacyjnej w przypadku materializacji skutków określnego zagrożenia. Tak więc wdrożenie współczesnych technologii do procesów informowania o zagrożeniach może ograniczać lub wręcz likwidować lukę w sprawnym przepływie informacji i szybszą identyfikację zagrożeń oraz podejmowanie działań i procedur możliwych do wykorzystania w danej sytuacji[262] przy pożądanym poziomie świadomości sytuacyjnej różnych grup interesariuszy, co istotnie może obniżać ryzyko strat związanych z występującym zagrożeniem.

W celu usprawnienia tego procesu każdy podmiot powinien mieć dostęp do zaawansowanej technologii IT/ICT. Oznacza to, że każdy proces zarządzania oraz reagowania kryzysowego wymaga wsparcia odpowiednimi narzędziami techniczno-technologicznymi ze szczególnym uwzględnieniem platform teleinformatycznych na różnych poziomach struktury (regionalnym, centralnym, lokalnym np. wojewódzkim, powiatowym, gminnym)[263].

W ustawie o zarządzaniu kryzysowym[264] nie są określone narzędzia, które mogą lub powinny być wykorzystane w celu zapewnienia wsparcia organów realizujących proces zarządzania kryzysowego. Nie określono również systemów łączności, jakie powinno się przygotować. W ustawie jest jedynie mowa o tym, że plan zarzadzania kryzysowego w swojej strukturze powinien zawierać organizację łączności bez określenia za pomocą jakich środków i w jaki sposób ma funkcjonować.

---

[262] Tamże, s. 53.
[263] P. Zaskórski, W. Zaskórski, J. Woźniak, *Świadomość sytuacyjna, a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, Wydawnictwo CeDeWu, Warszawa 2021, s. 53.
[264] Ustawa z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r., Nr 89, poz. 590).

Jednym z głównych zadań Zespołów Zarządzania Kryzysowego jest zagwarantowanie skutecznego przepływu informacji w celu wsparcia procesu informowania i przekazywania poleceń, co zostało zapisane w Rozporządzeniu Rady Ministrów w sprawie określenia zadań organów administracji rządowej[265]. W rozporządzeniu nałożono na Centra obowiązek zapewnienia ciągłości działania i łączności w sytuacjach kryzysowych (§ 4.1, pkt 1 i 2).

Należy zatem zwrócić uwagę na fakt, że obecnie szerzej wykorzystywane są systemy wspierające zarządzanie kryzysowe na szczeblu wojewódzkim, które wspomagają działania terenowych organów administracyjnych. W przypadku zagrożeń, które swoim zasięgiem obejmują większe obszary należy zatem liczyć się z możliwością wystąpienia problemów w zakresie sprawnej wymiany informacji oraz zarzadzania zasobami. Można również zauważyć, że większość systemów pełni funkcje zbierania danych i ich zobrazowania, a zautomatyzowane formy przekazu i wymiana informacji są realizowane w ograniczonym zakresie[266].

5.2. Analiza funkcjonalności istniejących rozwiązań teleinformatycznych w Systemie Zarządzania Kryzysowego RP

Różnorodność systemów i stosowanych narzędzi jednoznacznie pokazuje, że administracja publiczna nie posiada w swojej strukturze kompleksowego systemu łączności integrującego rożne rodzaje usług. Wymienione w poprzednim podrozdziale systemy teleinformatyczne realizują zadania, które wspomagają zarządzanie kryzysowe w wybranym obszarze, ale powiązane są z podmiotami (poszczególnymi służbami), dla których zostały utworzone. Narzędzia te mają w większości status autonomicznych rozwiązań, które nie są w całości zintegrowane i nie tworzą kompleksowego rozwiązania w formie systemu funkcjonującego na skalę całego państwa. Brak takiego systemu nie wynika z błędnego zaprojektowania wspomnianych podsystemów lecz z zaplanowanego zakresu ich wdrożenia i działania[267].

Pomimo, iż podjęte zostały próby zintegrowania i wykorzystania ogólnokrajowego systemu informatycznego, którego celem było wspomaganie zarządzania SZK,

[265] Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania (Dz. U. Nr 226 poz. 1810).
[266] Tamże.
[267] Tamże.

to potencjał wdrożonego w 2012 systemu Euromaster[268], ułatwiającego zarządzanie imprezą masową, jaką był turniej Euro 2012, po jego zakończeniu nie został wykorzystany. Do zadań tego systemu należało dostarczanie czytelnych i aktualnych informacji na temat bieżącej sytuacji na danym obszarze (w tym monitorowania zagrożeń i wspierania procesu kształtowania świadomości sytuacyjnej nie tylko decydentów, ale także zwykłych obywateli). Dostęp do tych danych przydzielony był wszystkim pracownikom podmiotów publicznych, którzy uczestniczyli w organizacji Euro 2012. Odpowiedzialność za zasilanie systemu danymi spoczywała na Krajowym Sztabie Operacyjnym, Sztabach Miejsko-Wojewódzkich, Sztabie MSW/MAiC (Ministerstwo Spraw Wewnętrznych/Ministerstwo Administracji i Cyfryzacji), Sztabie MTBiGM (Ministerstwo Transportu, Budownictwa i Gospodarki Wodnej) oraz Sztabie MZ (Ministerstwo Zdrowia). Zadaniem systemu było zbieranie i raportowanie danych o zdarzeniach za pośrednictwem przeglądarki internetowej i aplikacji zainstalowanej na smartfonie. Pomimo bardzo znaczących możliwości tego systemu, rozwiązania te nie zostały jednak przetestowane w skali kraju, a obecnie nadal wykorzystywanym podstawowym sposobem przekazywania informacji pozostają klasyczne już środki telekomunikacyjne oraz poczta elektroniczna[269]. Powstają tu jednak nowe zagrożenia dla bezpieczeństwa informacyjnego, co wiąże się z bezpieczeństwem cyberprzestrzeni w kontekście wiarygodności i niezawodności/pewności przekazu informacji.

W Polsce ważnym komponentem Systemu Zarządzania Kryzysowego, jednostek administracji publicznej i Ministerstwa Resortu Obrony Narodowej jest SZK JAŚMIN. System ten stanowi rozwiązanie, które dedykowane jest strukturom krajowego Systemu Zarządzania Kryzysowego NATO oraz UE. SZK JAŚMIN wspiera działanie organów administracji publicznej i Sił Zbrojnych RP oraz jednostek Obrony Terytorialnej w czasie prowadzonych akcji ratowniczych i/lub kryzysowych oraz działań prewencyjnych. Zadaniem systemu jest wspieranie procesu zarządzania, planowanie dowodzenia, kierowania oraz monitorowania zagrożeń o charakterze niemilitarnym i polityczno-militarnym.

---

[268] Przygotowanie i realizacja policyjnego zabezpieczenia turnieju finałowego mistrzostw Europy w piłce nożnej UEFA Euro 2012 - https://kpk.policja.gov.pl/download/18/17418/Raport_UEFA_EURO_2012.pdf

[269] Sprawozdanie z realizacji przedsięwzięć EURO 2012 oraz z wykonanych działań dotyczących realizacji przygotowań Polski do finałowego turnieju Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 (styczeń–grudzień 2012 r.), s. 7–8. Dostęp na stronie: https://bip.msit.gov.pl/download/2/3062/Sprawozdanie_EURO_2012-styczen_2013_r.pdf (data dostępu 23.01.2023).

Warto pamiętać, że SZK RP bezpośrednio współdziała z SWD C3IS JAŚMIN[270]. System ten wspiera procesy zarządzania, planowania, dowodzenia, kierowania, a także monitorowania (obrazowania) rzeczywistych zagrożeń o różnym charakterze[271]. Użytkownikami systemu JAŚMIN mogą być takie jednostki jak[272]:

- Policja;
- Straż Pożarna;
- Ratownictwo Medyczne;
- Centra Zarządzania Kryzysowego;
- Resort Obrony Narodowej.

SZK JAŚMIN składa się z oprogramowania o bogatej funkcjonalności oraz dedykowanego sprzętu IT, co umożliwia wsparcie procesów zarządzania kryzysowego w wymiarze globalnym przy współdziałaniu z agendami międzynarodowi (NATO, UE itp.). Do głównych funkcji systemu należą: planowanie i wsparcie procesów decyzyjnych oraz kontrolno-ocenowych, a w tym gromadzenie, przetwarzanie oraz dystrybucja informacji na temat akcji ratowniczych w zakresie [273]:

- incydentów,
- zdarzeń i zagrożeń,
- informacji o terenie i zasobach,
- danych o ludności,
- automatyczne oraz bieżące raportowanie,
- przekazywania informacji i współpracy z systemami innych resortów,
- przetwarzania informacji,
- obrazowania i monitorowania rzeczywistych sytuacji kryzysowych,
- integracja z bezzałogowymi statkami powietrznymi,
- monitorowanie osób przebywających na kwarantannie,
- współpraca z systemami symulacyjnymi.

Na rysunku 5.1 przedstawiono zobrazowanie wybranych aspektów sytuacji kryzysowych w SZK JAŚMIN. Z kolei na rysunku 5.2 przedstawiono możliwości zastosowania SZK JAŚMIN w strukturze zarządzania kryzysowego RP.

---

[270] https://www.teldat.com.pl/oferta/produkty/systemy/96-c3is.html (data dostępu 03.10.2021)
[271] Tamże.
[272] Tamże.
[272] Tamże.
[273] Tamże.

Rysunek 5.1. Zobrazowanie wybranych aspektów sytuacji kryzysowych z wykorzystaniem SZK JAŚMIN.

Źródło:https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html data dostępu 23.01.2022)

Rysunek 5.2. Możliwości zastosowania SZK JAŚMIN w strukturze zarządzania kryzysowego RP

Źródło: https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html (data dostępu 23.01.2022)

Analiza systemu SZK JAŚMIN pokazuje, że jest to w miarę kompleksowe rozwiązanie, dedykowane głównie dla organizacji administracji publicznej odpowiedzialnej za zarządzanie kryzysowe[274]. Rozwiązanie to ma jednak wiele luk głównie z punktu widzenia zakresu zasobów informacyjnych i możliwości przetwarzania analitycznego.

W 2019 roku Najwyższa Izba Kontroli (NIK) poddała analizie dostępne w Polsce systemy ochrony ludności na wypadek zagrożenia. W przedstawionym raporcie NIK zwrócono uwagę na to, że „nieprzygotowanie odpowiednich planów i procedur oraz niezapewnienie warunków do odpowiedniej koordynacji działań, może obniżać skuteczność działań służb odpowiedzialnych za ochronę ludności, zwłaszcza w momencie wystąpienia sytuacji kryzysowej[275]". Z raportu wynika również, że pomimo wieloletnich zapowiedzi w Polsce nie został uchwalony akt prawny, którego zadaniem byłaby regulacja całokształtu zagadnień związanych z ochroną ludności. Informacje tego typu rozporoszone zostały w różnych aktach prawnych. Zdaniem NIK główną tego przyczyną są przede wszystkim ustawicznie zmieniające się koncepcje rozwiązań prawnych[276].

Najwyższa Izba Kontroli poddała też badaniu funkcjonalność systemu ochrony ludności w ramach struktury zarządzania kryzysowego i obrony cywilnej, a wśród nich takie podmioty, jak m.in.[277]:

- Ministerstwo Spraw Wewnętrznych i Administracji,
- Komenda Główna Państwowej Straży Pożarnej,
- Rządowe Centrum Bezpieczeństwa,
- Urzędy Wojewódzkie,
- Starostwa Powiatowe,
- Urzędy Gmin/Miast.

Jak podaje, NIK kontrola wykazała zróżnicowany stan przygotowania struktur administracji samorządowej i rządowej w zakresie zarzadzania kryzysowego oraz ochrony ludności, a nieprawidłowości stwierdzono na każdym przebadanym szczeblu. Według raportu na szczeblu centralnym zastrzeżenia dotyczyły niekompletnego i niewłaściwego raportowania sytuacyjnego, a także niepełnej analizy i cząstkowych

[274] https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html (data dostępu 23.01.2022).
[275] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 11.10.2021).
[276] Tamże.
[277] Tamże.

prognoz rozwoju sytuacji kryzysowej oraz niewłaściwej lub nieprawidłowej formy komunikowania się pomiędzy wojewódzkimi centrami zarządzania kryzysowego. Ponadto z badań Najwyższej Izby Kontroli wynikało, że proces informowania o sytuacjach kryzysowych podmiotów wskazanych w siatce bezpieczeństwa jest nieefektywny. Co ważniejsze zwrócono również uwagę na fakt, że w przypadku niedoboru energii elektrycznej funkcjonowanie WCZK[278] może zostać sparaliżowane ze względu na brak zasilania awaryjnego[279].

Od 2007 roku w polskich regulacjach prawnych został określony obowiązek utworzenia Centrów Zarządzania Kryzysowego, funkcjonujących całodobowo[280] na terenie powiatów. Z raportu NIK wynika, że zadanie to nie zawsze było realizowane i zdarzyły się przypadki, w których pracownicy zatrudnieni na stanowiskach nie mieli odpowiedniej świadomości sytuacyjnej na temat zagrożeń[281], czyli stwierdzono braki w dostępie do właściwej informacji o zagrożeniu.

W raporcie zwrócono również uwagę na fakt, że w sporządzonych planach zarządzania kryzysowego występują nieprawidłowości, a możliwość ich wykorzystania jest bardzo ograniczona, ponieważ nie zawierają aktualnych informacji, co również wskazuje na lukę w aktualizacji danych o zagrożeniach i aktualnych możliwościach działania (zasobach, w tym zasobach informacyjnych). Ponadto pomimo nałożonego obowiązku na wszystkie organy zarządzania kryzysowego na szczeblu lokalnym odnośnie organizowania ćwiczeń i szkoleń powinność ta realizowana jest w małym stopniu[282].

W dalszej części raportu wzmiankuje się, że błędna interpretacja pojęcia sytuacja kryzysowa powoduje, że „nie jest możliwe jednoznaczne ustalenie liczby sytuacji kryzysowych objętych kontrolą”[283]. Istotnym problemem związanym z sytuacją kryzysową i radzeniem sobie z nią w trakcie jej zaistnienia było dopasowanie niezbędnego sprzętu, do przeprowadzania akcji ratowniczej. Raport NIK „obnaża” funkcjonowanie zarządzania kryzysowego w Polsce, co pokazują praktyczne ćwiczenia epizod prze-

[278] WCZK – Wojewódzkie Centrum Zarządzania Kryzysowego.
[279] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 11.10.2021).
[280] ROZPORZĄDZENIE RADY MINISTRÓW z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania.
[281] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 11.10.2021).
[282] Tamże.
[283] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 11.10.2021).

prowadzone na terenie woj. Dolnośląskiego. Scenariusz działań opierał się na podejmowaniu decyzji bezpośrednio po informacji o zaistnieniu awarii przemysłowej. Stwierdzono, że zarówno Wójt Gminy Krotoszyce, jak i członkowie Sztabu Kryzysowego Wójta nie dokonali weryfikacji informacji otrzymanej z Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu o skali zagrożenia (skażenie powietrza). W rezultacie spowodowało to wysyłanie do przeprowadzenia akcji ewakuacyjnej pracowników urzędu gminy i funkcjonariuszy niewyposażonych w środki ochrony osobistej stosownych w warunkach zaistniałego zagrożenia. Ponadto, pierwotnie ewakuacja odbywała się na terenie Krotoszyc, tj. skażonej miejscowości, której mieszkańców także należało ewakuować, a do ewakuacji przeznaczono pojazdy nieprzystosowane do transportu osób w terenie skażonym (np. ciągniki z przyczepami, samochody ciężarowe)”[284]. Ćwiczenia przeprowadzone w innych województwach również wykazały bardzo duże nieprawidłowości, a podejmowane decyzje nie były realne do wykonania. Oprócz wyżej wspomnianych problemów w raporcie NIK zwrócono uwagę na problemy związane z procesami komunikowania się pomiędzy Rządowym Centrum Bezpieczeństwa i Wojewódzkimi Centrami Bezpieczeństwa. Według raportu przesyłane komunikaty odczytywane są dużym opóźnieniem, przez co procedury reagowania są opóźnione[285]. Niezbędne jest zatem opracowanie koncepcji której celem będzie poprawa obecnej sytuacji umożliwiającej skuteczny obieg informacji w zespołach zarządzania kryzysowego oraz w procesie kształtowania świadomości sytuacyjnej ludności na temat zagrożeń przy wykorzystaniu współczesnych technologii, a także dotychczas stosowanej bazy narzędziowej do realizacji procesów informacyjno-decyzyjnych i komunikowania się współdziałających podmiotów.

5.3. Funkcjonalność i użyteczność współczesnych technologii możliwych do wykorzystania w procesie informowania ludności w sytuacjach kryzysowych

Każda współczesna technologia możliwa do zastosowania w zarządzaniu kryzysowym czy sytuacji kryzysowej, której zadaniem jest pomoc bądź ratowanie życia niezależnie od tego, czy jest to sztuczna inteligencja *Blockchain* czy IoT, jest warta analizy. Zarówno Internet Rzeczy (*IoT*) jak i *Blockchain* czy sztuczna inteligencja (*AI*), *Cloud Computing* (*CC*) - stanowią szczególne wyzwanie w zarządzaniu kryzy-

[284] Tamże.
[285] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 11.10.2021).

sowym. Zastosowanie tych technologii może spowodować usunięcie różnego typu luk stwierdzonych w funkcjonującym SZK i w sposobie realizacji w nim procesów informacyjnych służących wzmocnieniu poziomu świadomości sytuacyjnej i skuteczności działań. Technologie te mogą zatem poprawić jakość reakcji na zagrożenia. Każdą z tych technologii można stosować autonomicznie lub wykorzystując zjawisko synergii dążyć do łączenia ich potencjałów, co może istotnie wzmacniać funkcjonalność i użyteczność rozwiązań doskonalących procesy informowania ludności. Jednym z rozwiązań zapewniających wiarygodność i aktualność danych o bieżącej sytuacji może być platforma Internetu rzeczy.

5.3.1. Funkcjonalność Internetu Rzeczy (IoT)

Internet Rzeczy można zdefiniować jako sposób, w jaki urządzenia (analogowe, tradycyjnie odłączone) "rzeczy" komunikują się ze sobą w dedykowanych sieciach obliczeniowych, w których współdzielone przetwarzanie danych w chmurze i ich bieżąca analiza mogą dostarczyć aktualnej informacji na temat sytuacji zgodnie z celem uruchomionych operacji i procesów, w których biorą udział. To odróżnia IoT jako koncepcję i paradygmat organizacyjny od tradycyjnych sieciowych inteligentnych urządzeń, takich jak telefon lub komputer[286].

Termin Internet Rzeczy odnosi się do architektury internetowej, która ułatwia wymianę usług, informacji i danych między miliardami obiektów, głównie inteligentnymi. Termin ten został po raz pierwszy wprowadzony przez Kevina Ashtona w 1998 roku[287]. W niektórych publikacjach i literaturze wprowadza się określenie rozszerzające jako Internet wszystkiego (IoE[288]), aby podkreślić wszechobecne wykorzystanie obiektów z dostępem do Internetu, a przede wszystkim łączenia różnych urządzeń ludźmi. Platforma ta zapewnia połączenie między wszystkimi tymi obiektami z zapewnieniem współpracy rozwiązań sprzętowych i programowych ze sobą, aby zrealizować paradygmat Internetu Rzeczy[289].

Internet Rzeczy jest w stanie łączyć miliardy (docelowo praktycznie nieograniczoną liczbę) heterogenicznych urządzeń przez Internet. Domena IoT obejmuje szeroką gamę standardowych lub niestandaryzowanych technologii, platform oprogra-

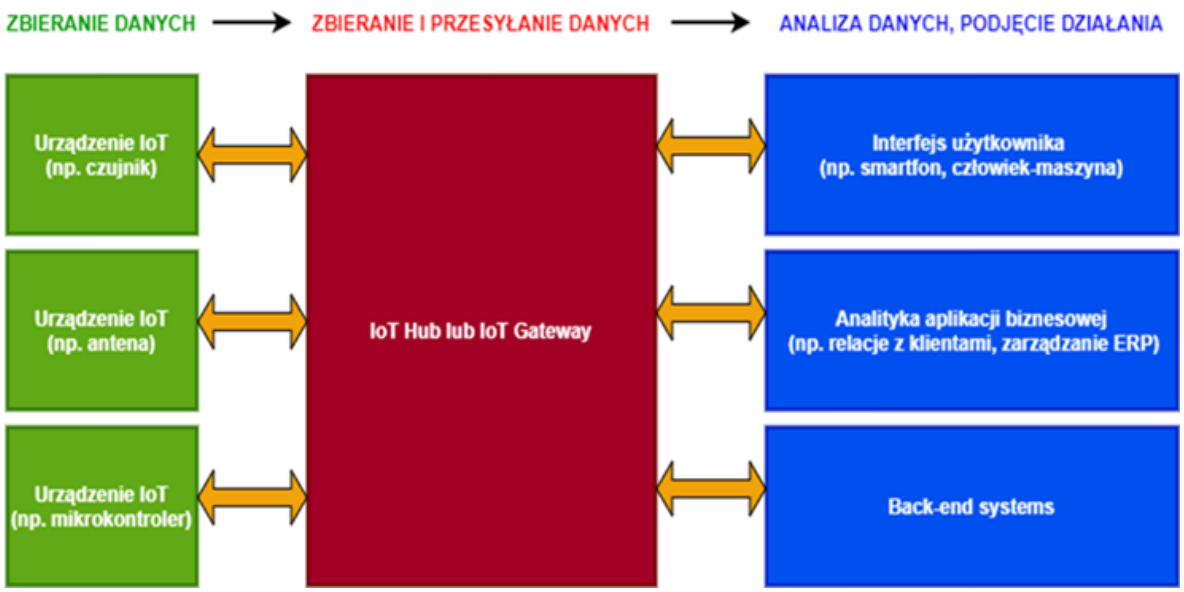
[286] https://www.rfidjournal.com/that-internet-of-things-thing (data dostępu 11.10.2021).
[287] G. Santucci, "*From Internet of Data to Internet of Things*," in International Conference on Future Trends of the Internet, 2009.
[288] Internet wszystkiego (IoE) to koncepcja, która rozszerza nacisk Internetu Rzeczy (IoT) na komunikację maszyna-maszyna(M2M),aby opisać bardziej złożony system, który obejmuje również ludzi i procesy.
[289] https://ec.europa.eu/digital-single-market/en (data dostępu 11.11.2021).

mowania i różnorodnych aplikacji. Dlatego jedna architektura referencyjna nie może być używana jako układ dla wszystkich możliwych konkretnych realizacji. Chociaż można rozważyć model referencyjny w przypadku IoT najprawdopodobniej będzie współistnieć kilka architektur referencyjnych. Architekturę należy definiować jako strukturę, w której rzeczy, usługi i ludzie w chmurze są łączone w celu wspólnego działania głównie z założeniem rejestracji, pomiaru i gromadzenia danych[290].

IoT to system (rys. 5.3) urządzeń i prostych obiektów, a także powiązanych ze sobą urządzeń komputerowych, wyposażonych w oprogramowanie i czujniki, które zbierają (np. odczytują wyniki pomiarów), gromadzą i przesyłają dane. Technologia ta, wykorzystywana do zarządzania kryzysowego, może przykładowo gromadzić i rozpowszechniać dane o zjawiskach znamionujących zagrożenia w mieście lub powodzie, tornada, huragany i inne katastrofy związane z pogodą, które wymagają bezpośrednich obserwacji w różnych miejscach, a dotarcie człowieka do tych miejsc byłoby trudne lub niemożliwe. Ta przeszkoda ogranicza zdolność zespołów do szybkiego reagowania, powiadamiania ludzi o aktualnych danych pogodowych i śledzenia uszkodzeń spowodowanych przez zaistniałe zjawiska[291].

Rozwój zaawansowanych czujników bezprzewodowych i narzędzi sieciowych, umożliwia zbieranie i gromadzenie dużej ilości danych w czasie rzeczywistym[292]. Jak już wspomniano w systemach Zarządzania Kryzysowego *IoT* może zostać wykorzystane do monitorowania klęski żywiołowej poprzez śledzenie aktualnego stanu zagrożenia przy wykorzystaniu czujników, dronów, kamer itp. Zasoby te można uznać za „inteligentne" urządzenia *IoT*, jeśli zostały zaprojektowane i zbudowane z myślą o generowaniu (zbieraniu) danych o wybranym obiekcie i bezpośredniej łączności. Istotną rolę w tym procesie odgrywa miniaturyzacja czujników oraz odpowiednia integracja ich z urządzeniami codziennego użytku np. telefon komórkowy, tablet, kamera, dron itp[293].

[290] Tamże.
[291] https://www.coolfiresolutions.com/blog/what-is-the-internet-of-things/ (data dostępu 01.10.2021).
[292] G. Santucci, "*From Internet of Data to Internet of Things*," in International Conference on Future Trends of the Internet, 2009.
[293] Tamże.



Rysunek 5.3. Architektura systemu IoT

Źródło: opracowanie własne na podstawie https://www.coolfiresolutions.com/blog/what-is-the-internet-of-things/ (data dostępu 23.02.2023)

Pomimo, że nie można powstrzymać pewnych katastrof, to można się lepiej przygotować do radzenia sobie z nimi. Internet rzeczy może pomóc w przezwyciężeniu nieefektywnych działań warunkowanych trudnością w dostępie do aktualnych danych i niewystarczającym poziomem świadomości sytuacyjnej. Urządzenia IoT mogą pomóc lub całkowicie zapobiec kryzysowi spowodowanemu np. błędami ludzi. Władze wszystkich państw muszą zwiększyć możliwości wykorzystania IoT w zarządzaniu klęskami żywiołowymi i sytuacjami kryzysowymi.

Doskonalenie technologii, takich jak sztuczna inteligencja, robotyka, wizualizacja komputerowa, analiza danych i uczenie maszynowe, może wzmocnić możliwości IoT w zakresie zarządzania klęskami żywiołowymi, a głównie podnieść skuteczność reakcji (przeciwdziałania) i zminimalizować straty powstałe na skutek zagrożeń. Wszędzie tam, gdzie wykorzystywany jest Internet Rzeczy, pojawia się koncepcja sztucznej inteligencji oraz *Blockchain* i *Cloud Computing*[294].

Urządzenia końcowe IoT można zintegrować z urządzeniami takimi jak komputer, tablet, smartfon, a ich rozmiar pozwala na umieszczenie wewnątrz dowolnego materiału, takiego jak odzież, wodowskazy itp. Wykorzystanie czujników IoT pozwala na gromadzenie danych w czasie rzeczywistym na temat: poziomu wody, odczytów barometrycznych, pożarów, oberwań chmury, trzęsień ziemi, a także umożliwia podgląd wybranych lokalizacji za pomocą kamer umieszczonych w miejscach publicznych itp.

[294] B. Shah,.H. Choset, "*Survey on Urban Search and Rescue Robotics",* CMU, Pittsburgh, 2003.

Ponadto wykorzystanie technologii IoT umożliwia ochronę infrastruktury krytycznej poprzez zastosowanie czujników do monitorowania zanieczyszczeń lub skażeń radioaktywnych. Ponadto dane gromadzone przez IoT umożliwiają zarządcom miast ustalać priorytety napraw oraz stosować zapobiegawczą konserwację. Połączone ze sobą urządzenia rozmieszczone w budynkach, na mostach drogach oraz innej infrastrukturze mogą zostać wykorzystane również do poprawy komunikacji. Co więcej wykorzystanie technologii *IoT* umożliwia monitorowanie aktualnego stanu rezerw strategicznych żywności, wody, odzieży, sprzętu medycznego i innych niezbędnych zapasów możliwych do wykorzystania w sytuacjach kryzysowych wykorzystując takie technologie jak kody kreskowe, RFID itp. Technologia *IoT* w infrastrukturze miejskiej, na obszarach leśnych lub gdziekolwiek indziej może zostać ponownie przydzielona do identyfikacji zagrożeń, osób uwięzionych lub np. stanu energetycznej (*postrzeganie*). Dzięki zastosowaniu technologii IoT służby ratownicze mają dostęp do przydatnych informacji, co może ułatwić planowanie reakcji i działań za pomocą czujników do monitorowania ruchu służb ratowniczych, a także kamer obsługujących *IoT* na miejscu zdarzenia co znacznie może zwiększyć poziom świadomości sytuacyjnej. Ponadto służby ratownicze mogą być wyposażone w czujniki audio i wideo lub wspierane przez autonomiczne drony i pojazdy, umożliwiając monitorowanie i ocenę niebezpiecznych sytuacji z bezpiecznej odległości.

Oprócz wymienionych funkcji technologia IoT umożliwia wysyłanie alertów, wiadomości oraz innych zasobów cyfrowych w celu poinformowania członków ZZK oraz obywateli w czasie rzeczywistym. Urządzenia mobilne takie jak smartfony, tablety smartwatche itp. mogą dostarczać informacji na temat bezpiecznych lokalizacji, zasobów, schronów lub zasobów niezbędnych do ratowania życia. Ponadto cyfrowe rozkłady jazdy na przystankach autobusowych mogą być wykorzystywane do szybkiego rozpowszechniania krytycznych informacji.

Każdy smartfon z dostępem do Internetu połączony z urządzeniami i czujnikami IoT za pomocą dedykowanej aplikacji jest w stanie odbierać powiadomienia oraz sterować czujnikiem IoT.

W tabeli 5.1 dokonano analizy SWOT dla technologii IoT (SWOT opisano w Rozdziale II).

Tabela 5.1. Analiza SWOT dla technologii IoT

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Monitorowanie zagrożeń i aktualnego stanu	5	W1	Nieznajomość technologii	3
S2	Udostępnianie informacji	5	W2	Ograniczenia czasowe	5
S3	Pobieranie danych	5	W3	Koszt wdrożenia	3
S4	Wykrywanie zagrożeń i otrzymywanie alertów	5	W4	Brak przeszkolonego personelu	3
S5	Monitoring niezbędnych zasobów	5	W5	Zależność od instalacji elektrycznej	5
S6	Identyfikacja zagrożeń	5	W6	Zależność od sieci komputerowej (Internet)	5
S7	Poszukiwanie poszkodowanych	5	W7	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	5
S8	Sprawdzanie statusu siec np. energetycznej	5	W8	Bezpieczeństwo urządzeń	4
S9	Sprawdzanie parametrów życiowych	5			
S10	Wysyłanie alertów	5			
S11	Odbieranie alertów	5			
S12	Wysyłanie komunikatów	5			
S13	Odbieranie komunikatów	5			
S14	Możliwość oszacowania prędkości rozprzestrzeniania się zagrożenia	5			
S15	Zmniejszenie emisji dwutlenku węgla, a tym samym pomoc w ochronie środowiska	5			
S16	Łatwość użycia	5			
	Suma wag:	**80**		**Suma wag:**	**33**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Zwiększenie poziomu świadomości sytuacyjnej na temat zagrożeń poprzez transfer danych w czasie rzeczywistym	5	T1	Utrata funkcjonalności na skutek awarii sieci elektrycznej	5
O2	Przyśpieszenie czasu reakcji na zagrożenia	5	T2	Utrata funkcjonalności na skutek awarii sieci komputerowej (Internet)	5
O3	Możliwość monitorowania zagrożeń z dowolnego miejsca bez potrzeby narażania ludzi na zagrożenia	5	T3	Podatność na cyberataki	3
O4	Usprawnienie procesu reagowania na zagrożenia	5	T4	Fałszywe powiadomienia (na skutek czynników pogodowych)	4
O5	Usprawnienie działań służb ratowniczych	5	T5	Luki w oprogramowaniu układowym	4
O6	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	5	T6	Koszt urządzeń	3
	Suma wag:	**30**		**Suma wag:**	**24**

Źródło opracowanie własne

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników[295]. W tym celu zastosowano pomocniczo następujące pytania:

1) Z perspektywy SWOT:

- Czy mocne strony IoT mogą wykorzystać szanse? (tab. 5.27 – Załącznik nr 5: Analiza SWOT/TOWS IoT),
- Czy mocne strony IoT przeważają nad zagrożeniami? (tab. 5.28 – Załącznik nr 5: Analiza SWOT/TOWS IoT,
- Czy słaba strona IoT ogranicza wykorzystanie szansy? (tab. 5.29 – Załącznik nr 5: Analiza SWOT/TOWS IoT),
- Czy słaba strona IoT może mieć wpływ na zagrożenia? (tab. 5.30 – Załącznik nr 5: Analiza SWOT/TOWS IoT).

[295] Czynniki rozumiane są jako mocne i słabe strony oraz szanse i zagrożenia.

2) Z perspektywy TOWS:

- Czy szanse IoT wpływają na mocne strony? (tab. 5.31 – Załącznik nr 5: Analiza SWOT/TOWS IoT),
- Czy zagrożenia IoT wpływają na mocne strony ? (tab. 5.32 – Załącznik nr 5: Analiza SWOT/TOWS IoT),
- Czy szanse IoT wpływają na słabe strony? (tab. 5.33 – Załącznik nr 5: Analiza SWOT/TOWS IoT),
- Czy zagrożenia IoT wpływają na słabe strony? (tab. 5.34 – Załącznik nr 5: Analiza SWOT/TOWS IoT)

Tabela 5.27 przedstawia wyniki interakcji pomiędzy mocnymi stronami i szansami. Suma interakcji wyniosła 77, co stanowi 80% maksymalnej liczby interakcji, jakie mogą wystąpić w badanym systemie. Suma wag i iloczynów wag oraz interakcji wynosi 770. Wysoka liczba interakcji wskazuje na bardzo duży potencjał rozważanej technologii w procesie zarządzania kryzysowego. Duża liczba interakcji pomiędzy mocnymi stronami i szansami jest ważnym argumentem za zastosowaniem określonej technologii, a funkcje takie jak np. takie jak monitorowanie zagrożeń, pobieranie informacji o nich oraz otrzymywanie i wysyłanie komunikatów i ostrzeżeń, daje realną szansę na zwiększenie świadomości sytuacyjnej zagrożeń, usprawnienie działań służb ratowniczych i przygotowanie się na zagrożenia.

Tabela 5.28 pokazuje związek pomiędzy mocnymi stronami, a zagrożeniami. Suma interakcji wyniosła 9, co stanowi 9% maksymalnej liczby interakcji, jaka może wystąpić. Suma wag i iloczynów wag oraz interakcji wynosi 77. Mała liczba interakcji sugeruje, że mocne strony i zagrożenia danej technologii nie są powiązane z procesem zarządzania kryzysowego, co oznacza, że zagrożenia takie jak m.in. koszty wdrożenia, podatność na cyberataki czy fałszywe powiadomienia nie obniżają znacząco walorów użytkowych technologii IoT.

Tabela 5.29 przedstawia zależności pomiędzy szansami i słabymi stronami. Duża liczba interakcji występująca między nimi, wskazuje przydatność technologii IoT w rozwijaniu świadomości sytuacyjnej na temat zagrożeń. Suma interakcji wyniosła 16, co stanowi 33% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Suma wag i iloczynów wag i interakcji wynosi 143. Mała liczba interakcji wskazuje na niską korelację pomiędzy szansami i słabymi stronami rozważanej technologii, a ukazane słabe strony, takie jak m.in. nieznajomość technologii, brak

odpowiedniej infrastruktury czy koszty wdrożenia to tymczasowe ograniczenia, które po pewnym czasie znikają całkowicie.

Tabela 5.30 przedstawia zależności pomiędzy słabymi stronami a zagrożeniami. Występująca słaba interakcja między nimi wskazuje na przydatność technologii IoT w budowaniu świadomości sytuacyjnej na temat zagrożeń. Suma interakcji wyniosła 17, co stanowi 35% maksymalnej liczby interakcji, jaka może wystąpić w zaproponowanym systemie. Suma wag i iloczynów wag i interakcji wynosi 132. Mała liczba interakcji wskazuje na niewielki wpływ słabych stron na zagrożenia. Potencjalne zagrożenia obejmują podatność na ataki cybernetyczne, które mogą być spowodowane niewłaściwym użyciem i nieznajomością technologii. Przedstawione w tabeli słabe strony i zagrożenia można jednak wyeliminować wdrażając odpowiednie zabezpieczenia i szkoląc osoby korzystające z urządzeń IoT.

Następnie za pomocą pytań pomocniczych (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.31 pokazuje zależności pomiędzy szansami i mocnymi stronami, które wchodzą ze sobą w bardzo silną interakcję, pokazując przydatność technologii IoT w rozwijaniu świadomości sytuacyjnej na temat zagrożeń. Suma interakcji wyniosła 96, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Suma wag i iloczynów wag i interakcji wynosi 960. Liczba interakcji wskazuje na bardzo duży wpływ szans na mocne strony, co wzmacnia zasadność stosowania technologii IoT. Podnoszenie poziomu świadomości sytuacyjnej, upraszczanie procesu zarządzania kryzysowego i działań ratowniczych zależy od mocnych stron, takich jak otrzymywanie powiadomień i ostrzeżeń, ciągłe monitorowanie zagrożeń oraz przesyłania danych.

Tabela 5.32 pokazuje zależności pomiędzy zagrożeniami i mocnymi stronami, między którymi nie występują powiązania. Suma interakcji wyniosła 0, co stanowi 0% maksymalnej liczby interakcji, jakie mogą wystąpić. Suma wag oraz iloczynów wag i interakcji wynosi 0, co oznacza, że zagrożenia nie wpływają na mocne strony technologii IoT.

W tabeli 5.33 przedstawiono powiązania pomiędzy oddziałującymi na siebie mocnymi i słabymi stronami. Suma interakcji wyniosła 17, co stanowi 35% maksymalnej liczby interakcji, jaka może wystąpić. Suma wag oraz iloczynów wag i interakcji wynosi 146, co oznacza, że zaprezentowane słabe strony mogą znacząco wpływać na zastosowanie technologii. Należy jednak zaznaczyć, że zaprezentowane uchybienia

dotyczą m.in. kosztów wdrożenia, nieznajomości technologii, brak odpowiedniej infrastruktury i to są ograniczenia, które pojawiają się na początku adaptacji nowej technologii.

Tabela 5.34 pokazuje zależności pomiędzy zagrożeniami i słabymi stronami, które na siebie oddziałują. Suma interakcji wyniosła 21, co stanowi 46% maksymalnej liczby interakcji, jaka może wystąpić. Suma wag oraz iloczynów wag i interakcji wynosi 165, co oznacza, że przedstawione zagrożenia mogą nie mają dużego wpływu na słabe strony technologii. Jednakże nieznajomość technologii może zwiększyć jej podatność na ataki lub szkody.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.2).

Tabela 5.2. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	173	1730
Mocne strony/Zagrożenia	9	77
Słabe strony/Szanse	33	289
Słabe strony/Zagrożenia	38	297

Źródło: opracowanie własne

Analiza zawartości tabeli 5.2 wskazuje na bardzo duży potencjał technologii IoT, której zastosowanie może usprawnić cały proces zarządzania kryzysowego pod kątem wypracowania pożądanego poziomu świadomości sytuacyjnej. Z przeprowadzonej analizy możliwości wykorzystania technologii IoT można wywnioskować (na podstawie analizy SWOT-TOWS), że istnieje przewaga mocnych stron nad słabymi oraz szans nad zagrożeniami. Przedstawione w tabeli słabe strony oraz zagrożenia takie jak, m.in. nieznajomość technologii, brak przeszkolonego personelu, zależność od poziomu niezawodności systemu zasilania oraz samej sieci komputerowej, brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych, a także bezpieczeństwo urządzeń - są możliwe do wyeliminowania poprzez wdrożenie odpowiednich procedur oraz technologii wspomagających. Działania tego typu powinny być ukierunkowane na zwiększenie wiedzy na temat funkcjonowania technologii oraz procedur bezpieczeństwa z nią związanych, tj. wdrożenie polityki bezpieczeństwa, która powinna regulować procedury postępowania z danymi oraz możliwości ich zabezpieczenia poprzez stosowanie środków zapobiegawczych takich, jak m.in. przetwarzanie danych na komputerach oraz urządzeniach do tego przeznaczonych, zastosowanie bezpiecznych haseł (duże litery, małe litery cyfry znaki specjalne) dla wy-

korzystywanych urządzeń, przetwarzanie danych wyłącznie przez osoby przeszkolone i upoważnione, zapoznanie pracowników z zasadami działania wdrażanej technologii. Ponadto, należy rozważyć wdrożenie alternatywnych źródeł zasilania na wypadek utraty dostępu do sieci energetycznej, np. energia wiatrowa lub panele fotowoltaiczne. Można zatem stwierdzić, że zagrożenia nie wynikają z działania technologii, ale z jej nieznajomości. Przed wdrożeniem technologii należy poddać się gruntownemu przeszkoleniu, aby uniknąć tego typu zagrożeń. Ponadto, warto pamiętać, że proces wdrożenia technologii IoT to dość kosztowne wieloetapowe przedsięwzięcie rozłożone w czasie.

5.3.2. Modele i narzędzia sztucznej Inteligencji

Sztuczna inteligencja (AI) to nauka i inżynieria tworzenia inteligentnych maszyn, zwłaszcza inteligentnych programów komputerowych”[296] oraz generowania wiedzy poprzez naśladowanie niejako pracy myślowej człowieka (w tym wnioskowania na bazie eksploracji dostępnych zasobów informacyjnych). *AI* to sposób na inteligentne myślenie komputera, robota sterowanego komputerowo lub oprogramowania. Uczenie maszynowe osiąga się poprzez badanie sposobu myślenia ludzkiego mózgu oraz sposobu, w jaki ludzie uczą się, podejmują decyzje i pracują nad rozwiązaniem problemu, a następnie wykorzystują wyniki tych badań jako podstawę do opracowywania inteligentnych programów i systemów[297]. Alan Turing uważał, że maszyna może zostać uznana za inteligentną w momencie, gdy człowiek (tester) nie jest w stanie odróżnić odpowiedzi udzielanych przez maszynę od odpowiedzi udzielanych przez człowieka – gra w imitację, czyli Test Turinga[298].

Sztuczna inteligencja rozwijała się wraz z rozwojem komputerów ogólnego przeznaczenia, które stały się dostępne do użytku niewojskowego w latach pięćdziesiątych XX wieku. Nowo dostępna moc obliczeniowa pozwoliła na stworzenie symbolicznych programów *AI*, czyli algorytmów, które stosują zestaw reguł w celu naśladowania rozumowania i podejmowania decyzji. Przykładami takich programów są te dedykowane do warcabów i gier w szachy, które już w latach 70 XX wieku osiągały bardzo dobre wyniki oraz pierwsze chatboty, które w pewnym stopniu symulowały

---

296 https://news.stanford.edu/news/2011/october/john-mccarthy-obit-102511.html (data dostępu 03.10.2021).

297 A. Turing, *Maszyny myślące a inteligencja*, Maszyny matematyczne i myślenie, tłum. D. Gajkowicz, Warszawa 1972, s. 24–47.

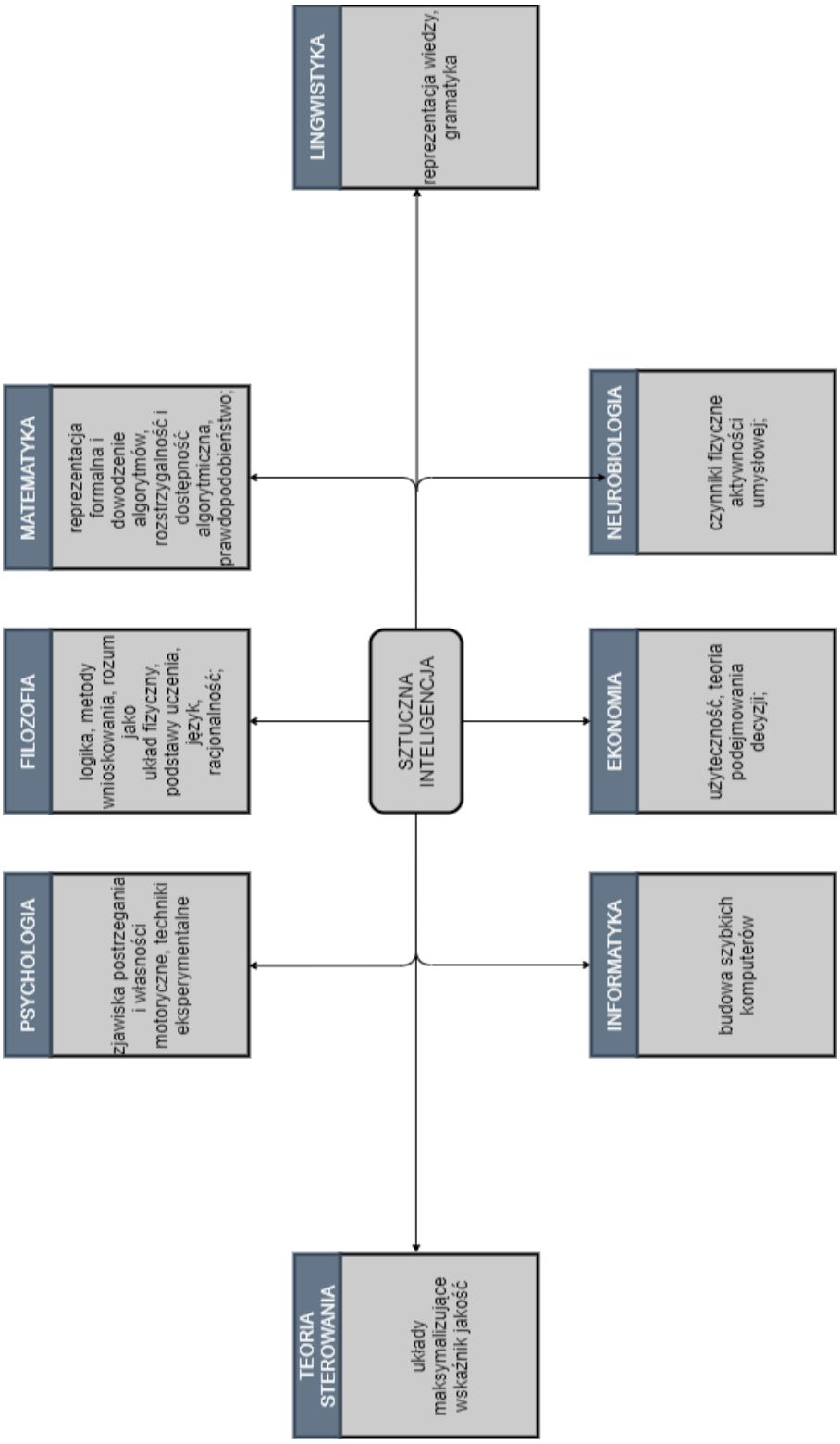
298 https://www.britannica.com/technology/artificial-intelligence/Alan-Turing-and-the-beginning-of-AI (data dostepu 03.10.2021).

rozmowę w języku naturalnym[299]. W ostatniej dekadzie XX wieku nastąpił duży wzrost wykorzystania sztucznej inteligencji (*AI*), zwłaszcza technologii uczenia maszynowego (*ML*). Na przykład osobiści asystenci, którzy potrafią rozumieć głosowy język naturalny i wykonywać proste zadania, takie jak pobieranie informacji z kalendarza, zarządzanie urządzeniami automatyki domowej i składanie zamówień online, są obecnie wykorzystywani na wielu smartfonach.

Pomimo, iż sztuczna inteligencja i uczenie maszynowe używane są zamiennie to uczenie maszynowe jest tylko gałęzią sztucznej inteligencji, która zajmuje się metodami pozwalającymi maszynie „uczyć się", czyli poprawiać jej wydajność w określonych zadaniach w oparciu o wcześniejsze doświadczenia lub dane.[300]. Maszyny wyposażone w sztuczną inteligencję mogą poprawić komfort życia poprzez pomoc ludziom w przemieszczaniu się z jednego obszaru do drugiego, zmienić sposób pracy jednostek itp. Wykorzystanie AI w zarządzaniu kryzysowym może pomóc w przewidywaniu, ocenie i symulacji incydentów i procesów takich, jak np. klęski żywiołowe. Daje to ratownikom i innym służbom możliwość skrócenia czasu reakcji i optymalizacji dostaw zasobów dla dotkniętych obszarów[301].

Sztuczna inteligencja to nauka i technologia oparta na dyscyplinach takich, jak informatyka, biologia, psychologia, filozofia, matematyka i socjologia. Głównym celem sztucznej inteligencji jest rozwój funkcji komputerowych związanych z ludzką inteligencją takich, jak rozumowanie, uczenie się (w tym automatyczne wnioskowanie) oraz rozwiązywanie problemów (rys. 5.4)[302].

[299] Tamże.
[300] AL. Samuel, *Some studies in machine learning using the game of checkers*. *IBM J Res Dev.* 1959, s. 210-229.
[301] A. Hosny, C. Parmar, J. Quackenbush, LH Schwartz, HJ. Aerts, *Artificial intelligence in radiology*. Nat Rev Cancer*,* 2018, s. 510-518.
[302] Tamże, s. 510-518.



Rysunek 5.4. Możliwości zastosowania sztucznej inteligencji

Źródło: opracowanie własne na podstawie (G. Senthilvel - Exploring the concepts of Artificial Intelligence: https://www.codeproject.com/*AR*ticles/1182210/*AR*tificial-Intelligence)

Możliwości sztucznej inteligencji są nieograniczone. Technologia ta może być stosowana w wielu różnych sektorach i branżach. *AI* jest wykorzystywana coraz czę-

ściej w branży medycznej przy skomplikowanych operacjach. Inne przykłady maszyn ze sztuczną inteligencją to komputery, które mogą automatycznie realizować różne procesy (np. gry w szachy) i samochody autonomiczne itp. Każda z tych maszyn musi przewidywać konsekwencje wszelkich podejmowanych przez siebie działań, ponieważ każde działanie będzie miało wpływ na wynik końcowy. W szachach efektem końcowym jest wygranie gry. W przypadku samochodów autonomicznych system komputerowy musi uwzględniać wszystkie dane zewnętrzne i obliczać je, aby działały w sposób zapobiegający kolizji[303].

Sztuczna inteligencja osiągnęła obecnie wystarczająco wysoki poziom dojrzałości jako technologia, aby możliwe było wykorzystanie jej do usprawnienia całego procesu zarządzania kryzysowego, a w szczególności w procesie kształtowania kompetencji w rozpoznawaniu zagrożeń przez jednostkę i całe społeczności. W wysoko rozwiniętych krajach administracje rządowe coraz częściej wykorzystują inteligentne technologie cyfrowe w swoich codziennych działaniach, mających na celu zwalczanie sytuacji kryzysowych[304].

Rozwój i wdrażanie nowych technologii zwykle budzi pewien strach i niechęć wśród ludzi, którzy są przeciwni tego typu rozwiązaniom. Niechęć ta w głównej mierze wynika z braku wiedzy lub znajomości cech i potencjalnych korzyści płynących z wdrożenia danej technologii. Sztuczna inteligencja powoduje pewien stopień „wrogości" w niektórych społecznościach, np. ze względu na poczucie, że jej szerokie zastosowanie może wywołać nieznane zmiany w codziennym życiu człowieka, a także przejąć część jego obowiązków[305]. Niemniej jednak wykorzystanie sztucznej inteligencji umożliwia automatyzację, identyfikowalność i optymalizację działań człowieka w taki sposób, że część zadań związanych z ratowaniem ludzi bez potrzeby narażania służb ratowniczych mogą wykonać inteligentne roboty. Ponadto sztuczna inteligencja dzięki zastosowaniu odpowiednich algorytmów i dużej mocy obliczeniowej jest w stanie wykonać obliczenia dla wielu wariantów scenariuszy przebiegu sytuacji kryzysowej znacznie szybciej niż mógłby to wykonać człowiek[306].

Szeroka gama zastosowań sztucznej inteligencji pozwala na sprawniejsze przygotowanie się na zagrożenia poprzez monitorowanie zagrożeń, zbieranie da-

[303] https://www.techtarget.com/searchenterpriseai/definition/driverless-car (data dostępu 23.02.2023).
[304] K. Grace, J. Salvatier, A. Dafoe, B. Zhang, O. Evans, When Will AI Exceed Human Performance? Evidence from AI Experts, https://arxiv.org/pdf/1705.08807.pdf (data dostępu 23.02.2023).
[305] Tamże.
[306] Tamże.

nych, opracowywanie prognoz możliwych do wystąpienia zarówno aktualnych jak i przyszłych wydarzeń, a także analizując te dane. AI daje także możliwość stworzenia scenariuszy różnych zagrożeń bazujących na rzeczywistych odniesieniach i danych. W tabeli 5.3 dokonano analizy SWOT dla technologii sztucznej inteligencji w aspekcie jej użyteczności w kreowaniu poziomu świadomości sytuacyjnej.

Tabela 5.3. Analiza SWOT dla technologii sztucznej inteligencji

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Robotyka akcje - akcje poszukiwawczo ratownicze	5	W1	Nieznajomość technologii	3
S2	Wymiana informacji	5	W2	Ograniczenia czasowe	5
S3	Pobieranie danych	5	W3	Koszt wdrożenia	3
S4	Symulowanie zagrożeń	5	W4	Brak przeszkolonego personelu	3
S5	Analiza zagrożeń na podstawie zebranych danych	5	W5	Zależność niektórych urządzeń od Internetu	5
S6	Identyfikacja zagrożeń	5	W6	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	5
S7	Tworzenie chatbotów	5			
S8	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	5			
S9	Komunikacja z dowolnego miejsca	5			
S10	Oszacowanie możliwości wystąpienia zagrożenia	5			
S11	Przetwarzanie danych	5			
S12	Generowanie scenariuszy zagrożeń	5			
	Suma wag:	**60**		**Suma wag:**	**24**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Usprawnienie działania służb ratowniczych	5	T1	Utrata funkcjonalności niektórych urządzeń na skutek awarii sieci komputerowej (Internet)	5
O3	Możliwość przygotowania się na zagrożenia	5	T3	Podatność na cyberataki	3
O4	Symulacje przyszłych zagrożeń	5	T4	Luki w oprogramowaniu układowym	4
O5	Usprawnienie procesu komunikacji (chatboty - źródło informacji o zagrożeniach)	5	T5	Bezpieczeństwo danych	3
	Prowadzenie ćwiczeń i scenariuszy zagrożeń	5			
O6	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	5			
	Suma wag:	**30**		**Suma wag:**	**15**

Źródło: opracowanie własne

Pomimo, iż systemy sztucznej inteligencji są w stanie nauczyć się wykonywać zadania oparte na danych wejściowych, często wymagają wsparcia innych technologii w celu pozyskiwania, przechowywania, przetwarzania i przesyłania danych takich jak m.in. Internet Rzeczy (*IoT*),technologie 3D, *Blockchain*, infrastruktura komunikacyjna 5G.

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu zastosowano pomocniczo następujące pytania:

1) Dla perspektywy SWOT:
   - Czy mocna strona sztucznej inteligencji może wykorzystać szanse? (tab. 5.35 – Załącznik nr 5: Analiza SWOT/TOWS sztucznej inteligencji),

- Czy mocne strony sztucznej inteligencji przeważają nad zagrożeniami? (tab. 5.36 – Załącznik nr 5: Analiza SWOT/TOWS sztucznej inteligencji,
- Czy słaba strona sztucznej inteligencji ogranicza wykorzystanie szansy? (tab. 5.37 – Załącznik nr 5: Analiza SWOT/TOWS sztucznej inteligencji),
- Czy słaba strona sztucznej inteligencji może mieć wpływ na zagrożenia? (tab. 5.38 – Załącznik nr. 5: Analiza SWOT/TOWS sztucznej inteligencji).

2) Dla perspektywy TOWS:
    - Czy szanse sztucznej inteligencji wpływają na mocne strony? (tab. 5.39 – Załącznik nr. 5: Analiza SWOT/TOWS sztucznej inteligencji),
    - Czy zagrożenia sztucznej inteligencji wpływają na mocne strony? (tab. 5.40 – Załącznik nr 5: Analiza SWOT/TOWS sztucznej inteligencji),
    - Czy szanse sztucznej inteligencji wpływają na słabe strony? (tab. 5.41 – Załącznik nr. 5: Analiza SWOT/TOWS sztucznej inteligencji),
    - Czy zagrożenia sztucznej inteligencji wpływają na słabe strony? (tab. 5.42 – Załącznik nr. 5: Analiza SWOT/TOWS sztucznej inteligencji).

Tabela 5.35 przedstawia zależności pomiędzy mocnymi stronami a szansami, między którymi występuje bardzo silna korelacja, co wskazuje na przydatność sztucznej inteligencji w kształtowaniu świadomości sytuacyjnej na temat zagrożeń. Na podstawie odpowiedzi na pytanie. Suma interakcji wyniosła 61, co stanowi 92% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 610, co oznacza, że wymienione mocne strony takie jak m.in. robotyka, symulacja zagrożeń, oszacowanie możliwości ich wystąpienia czy integracja z urządzeniami mobilnymi mogą znacznie usprawnić działanie służb ratowniczych, lepiej przygotować się na zagrożenia i usprawnić komunikację w czasie zagrożeń.

Tabela 5.36 przedstawia zależności pomiędzy oddziałującymi mocnymi stronami zagrożeniami. Suma interakcji wyniosła 18, co stanowi 37,5% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz wag i interakcji wynosi 150, co oznacza, że zagrożenia takie jak luki w oprogramowaniu lub ataki mają niewielki wpływ na mocne strony, takie jak robotyka, symulacja zagrożeń, szacowane prawdopodobieństwo wystąpienia czy integracja z urządzeniami mobilnymi.

Tabela 5.37 pokazuje relacje pomiędzy słabymi stronami i szansami. Na podstawie odpowiedzi na pytanie. Suma interakcji wyniosła 24, co stanowi 67% maksy-

malnej liczby interakcji, jaka może wystąpić. Łączna suma wag i iloczynów wag oraz interakcji wynosi 214. Słabe strony mogą tymczasowo ograniczać możliwości i potencjał sztucznej inteligencji, niemniej jednak w miarę wzrostu wiedzy na temat technologii ostatecznie zidentyfikowane słabe strony są możliwe do wyeliminowania.

W tabeli 5.38 przedstawiono zależności pomiędzy słabymi stronami oraz zagrożeniami ,między którymi występuje słaba interakcja. W przebadanym układzie uzyskano sumę interakcji równą 10, co stanowi 42% maksymalnej liczby interakcji które mogą wystąpić. Łączna suma wag i iloczynów wag oraz interakcji wynosi 73. Z analizy tabeli można wyciągnąć wniosek, że słabe strony mogą stwarzać zagrożenia.

Następnie za pomocą pytań pomocniczych (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.39 pokazuje relacje pomiędzy szansami i mocnymi stronami. Suma interakcji wyniosła 70, co stanowi 97% maksymalnej liczby interakcji, jaka może wystąpić. Suma wag i iloczynów wag oraz interakcji wynosi 700. Na podstawie analizy tabeli można stwierdzić, że szanse takie jak Poprawa efektywności służb ratunkowych, lepsze przygotowanie na zagrożenia oraz poprawa komunikacji w chwilach zagrożenia mogą przyczynić się do efektywności zarządzania kryzysowego poprzez wykorzystanie mocnych stron technologii takich jak m.in. ocena możliwości wystąpienia zagrożenia, opracowanie scenariuszy zagrożeń, skuteczna analiza zagrożeń na podstawie zebranych informacji i ich identyfikacji.

Tabela 5.40 pokazuje, że między zagrożeniami i mocnymi stronami nie stwierdzono interakcji. Na tej podstawie można zauważyć, że zagrożenia nie ograniczają potencjału sztucznej inteligencji i mocnych stron tej technologii.

Tabela 5.41 pokazuje zależności szansami i słabymi stronami, które wzajemnie na siebie oddziałują. Na podstawie odpowiedzi na pytanie Suma interakcji wyniosła 21, co stanowi 58% maksymalnej liczby interakcji, jaka może wystąpić w przebadanym układzie. Suma wag i iloczynów wag oraz interakcji wynosi 191. Z analizy tabeli można wyciągnąć wniosek, że słabe strony mogą mieć wpływ na szansę poprawy świadomości sytuacyjnej i możliwości usprawnienia zarządzania kryzysowego, jeśli nie zostaną pozyskane informacje o technologii i nie zostanie stworzona odpowiednia infrastruktura do jej wykorzystania.

Tabela 5.42 pokazuje zależności pomiędzy interaktywnymi zagrożeniami i słabymi stronami. Suma interakcji wyniosła 11, co stanowi 46% maksymalnej możliwej

liczby interakcji, które mogą wystąpić. Suma wag i iloczynów wag oraz interakcji wynosi 84. Z analizy tabeli można wyciągnąć wniosek, że słabe strony mogą stwarzać zagrożenia, ale i nie wynikają one z nieprawidłowości wynikających z funkcjonalności technologii, lecz mogą powstać na skutek np. braku informacji, niewłaściwego zabezpieczenia lub brak odpowiedniej infrastruktury do jej wdrożenia technologii.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.4)

Tabela 5.4. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	131	1310
Mocne strony/Zagrożenia	18	150
Słabe strony/Szanse	45	405
Słabe strony/Zagrożenia	21	157

Źródło: opracowanie własne

Analiza tabeli 5.4 wskazuje na dominacje mocnych stron i szans. Zasadne jest zatem stwierdzenie, że wielki potencjał technologii sztucznej inteligencji może usprawnić proces całego zarządzania kryzysowego.

Analiza SWOT-TOWS sztucznej inteligencji wykazała, że zarówno zagrożenia jak i słabe strony wynikają z luk w oprogramowaniu, podatności na ataki lub nieznajomości technologii. Wskazane słabe strony oraz zagrożenia są możliwe do zlikwidowania poprzez systematyczną aktualizację, odpowiednie zabezpieczenie urządzeń oraz systematyczne szkolenia pracowników z zakresu działania technologii oraz zasad jej bezpieczeństwa. Brak przeszkolonego personelu lub brak odpowiedniej infrastruktury niezbędnej do wdrożenia technologii jest w stanie zakłócić działanie każdej technologii.

5.3.3. Możliwości Virtual Reality (VR) i Augmented Reality (AR)

W przypadku sztucznej inteligencji warto również uwzględnić wykorzystanie takich technologii, jak symulatory sytuacji kryzysowych, które w połączeniu z technologią *Virtual Reality* (*VR*) i *Augmented Reality* (*AR*) są w stanie symulować wydarzenia na odpowiednim poziomie szczegółowości. Połączenie sztucznej inteligencji i technologii *VR/AR* umożliwia symulowanie wydarzeń zbliżonych do rzeczywistych sytuacji kryzysowych, dzięki czemu możliwe jest przygotowanie służb ratunkowych na te sytuacje, z którymi mogą się spotkać w czasie prawdziwego zagrożenia[307]. Jednym przykładów takiego rozwiązania jest symulator pacjenta *PerSim* stworzony

[307] F. Longo, L. Nicoletti, A. Padovano, *Emergency preparedness in industrial plants: a forward-looking solution based on industry 4.0 enabling technologies*, Comput. Ind. 105, 2019 s. 99–122.

przez *MedCognition*. Personel korzysta z usługi *Microsoft HoloLens*[308] do bardziej realistycznego szkolenia w zakresie reagowania na drgawki, niewydolność oddechową i urazy spotykane w sytuacjach kryzysowych. Instruktorzy mogą zaprogramować zmiany, które model będzie wykazywać, aby sprawdzić szybkość i dokładność uczestników podczas reagowania na sygnały wizualne. Rzeczywistość wirtualna to trójwymiarowy obraz, który został stworzony komputerowo. VR może przedstawiać różne przedmioty, obiekty, a nawet całe zdarzenia.

W zależności od koncepcji, *Virtual Reality* opiera się zarówno na elementach świata realnego, jak i abstrakcyjnego. Najprościej można więc powiedzieć, że to określenie oznacza po prostu wirtualną imitację rzeczywistości koncentrując się głównie na algorytmach wczesnego ostrzegania i oceny kryzysów np. w przestrzeni morskiej dla wsparcia decyzji[309]. Algorytmy są wyposażone w zaawansowane funkcje wizualizacji i zarządzania kryzysowego. Technologie oparte na rozszerzonej rzeczywistości (*AR*) mogą zapewnić lepszą świadomość sytuacyjną dzięki zastosowaniu wyświetlaczy *heads-up* i AR opartych na gestach. Wyświetlacze tego typu mogą ułatwić członkom zespołów ratunkowych postrzeganie najważniejszych informacji o procesie dowodzenia i kontroli bez konieczności powrotu do stanowiska pracy, aby uzyskać dostęp do ekranu[310]. W Polsce tego typu rozwiązania nie są powszechnie wykorzystywane, niemniej jednak są już stosowane na świecie. Przykładem takiego oprogramowania połączonego z AR jest *Simavi*[311].

Technologia *VR/AR* umożliwia użytkownikom przeprowadzenie wirtualnych ćwiczeń zbliżonych warunkami do rzeczywistych zagrożeń, dzięki czemu możliwe jest przygotowanie się na istniejące zagrożenia w rzeczywistym świecie bez narażenie członków służb ratowniczych[312] a potem skuteczne reagowanie.

Technologię *VR* można zdefiniować jako sztuczne środowisko cyfrowe, które jest w stanie całkowicie zastąpić środowisko rzeczywiste. Istnieją dwa rodzaje zestawów słuchawkowych dostarczających *VR* – podłączone do komputera i samodzielne. Aktualnie wśród głównych zastosowań tej technologii dominują: gry (360°) i odtwarzanie wideo. Wykorzystanie technologii wirtualnej i rozszerzonej rzeczywistości do szkoleń w zakresie zarządzania kryzysowego, a także w terenie podczas

[308] Microsoft HoloLens - gogle rozszerzonej rzeczywistości wyprodukowane przez Microsoft
[309] A. Perlman, R. Sacks, R. Barak, *Hazard recognition and risk perception in construction*, Saf. Sci. 64, 2014 s. 13–21.
[310] Tamże s. 13–21.
[311] https://www.simavi.ro/en/node/61 (data dostępu 30.09.2021).
[312] Tamże.

fazy reagowania kryzysowego jest w stanie usprawnić działanie służb w miejscach dotkniętych katastrofą. W przypadku szkoleń wirtualna i rozszerzona rzeczywistość jest skutecznym sposobem na ułatwienie i usprawnienie procesu uczenia się. W przypadku reagowania kryzysowego wirtualna i rozszerzona rzeczywistość może pomóc w wizualizacji skutków katastrof, zapewniając ekspertom więcej czasu na opracowanie alternatywnych planów działania. Technologia pomaga również podmiotom zarządzającym klęskami żywiołowymi i zainteresowanym stronom lepiej planować działania w sytuacji kryzysowej[313].

Przeprowadzona analiza SWOT ma na celu ocenę przydatności technologii *VR/AR* w zarządzaniu kryzysowym (tab. 5.5).

Tabela 5.5. Analiza SWOT dla technologii *VR/AR*

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Symulowanie realistycznych zagrożeń	5	W1	Koszt wdrożenia	3
S2	Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	5	W2	Brak przeszkolonego personelu	3
S3	Tworzenie realistycznych szkoleń dla służb ratowniczych	5	W3	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	5
S4	Wyświetlanie nazw ulic, śledzenie służb ratowniczych,	5	W4	Brak kontaktu z otoczeniem (*VR*)	1
S5	Komunikacja głosowa	5			
S6	Nanoszenie obrazów 3D na rzeczywiste środowisko	5			
	Suma wag:	**30**		**Suma wag:**	**12**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Usprawnienie działania służb ratowniczych	5	T1	Zaburzenia błędnika, choroba lokomocyjna	5
O2	Możliwość przygotowania się na zagrożenia	5	T2	Podatność na cyberataki i śledzenie	4
O3	Symulacje przyszłych zagrożeń	5	T3	Uzależnienie od technologii	3
O4	Usprawnienie procesu komunikacji	5			
O5	Prowadzenie ćwiczeń i scenariuszy zagrożeń - bez narażania życia i zdrowia	5			
O6	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	5			
	Suma wag:	**20**		**Suma wag:**	**12**

Źródło: opracowanie własne

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikację interakcji SWOT-TOWS przeprowadzono za pomocą ośmiu tabel, które są wynikiem połączenia dwóch czynników. Pomocne w tym celu okazały się następujące pytania:

W perspektywie SWOT:

- Czy mocna strona *VR/AR* mogą wykorzystać szanse? (tab. 5.43 – Załącznik nr 5: Analiza SWOT/TOWS),
- Czy mocna strona *VR/AR* przeważają nad zagrożeniami? (tab. 5.44 – Załącznik nr 5: Analiza SWOT/TOWS),

[313] https://imtech.imt.fr/en/2022/09/15/virtual-reality-to-improve-crisis-management-and-cybersecurity/ (data dostępu: 23.02.2023).

- Czy słaba strona *VR/AR* ogranicza wykorzystanie szansy? (tab. 5.45 – Załącznik nr 5: Analiza SWOT/TOWS),
- Czy słaba strona *VR/AR* może mieć wpływ na zagrożenia? (tab. 5.46 – Załącznik nr 5: Analiza SWOT/TOWS).

1) W perspektywie TOWS:
    - Czy szanse *VR/AR* wpływają na mocne strony? (tab. 5.47 – Załącznik nr 5: Analiza SWOT/TOWS),
    - Czy zagrożenia *VR/AR* wpływają na mocne strony? (tab. 5.48 – Załącznik nr 5: Analiza SWOT/TOWS),
    - Czy szanse *VR/AR* wpływają na słabe strony? (tab. 5.49 – Załącznik nr 5: Analiza SWOT/TOWS),
    - Czy zagrożenia *VR/AR* wpływają na słabe strony? (tab. 5.50 – Załącznik nr 5: Analiza SWOT/TOWS).

Tabela 5.43 pokazuje relacje pomiędzy mocnymi stronami i szansami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 36, co stanowi 100% maksymalnej możliwej liczby interakcji w badanym układzie. Suma iloczynów wag oraz interakcji wynosi 360. Z analizy tabeli można stwierdzić, że mocne strony VR/AR mogą przyczynić się usprawnienia działań zespołów zarządzania kryzysowego i służb ratowniczych, a omawiana technologia może okazać się bardzo przydatna w tworzeniu pożądanego poziomu świadomości sytuacyjnej.

Tabela 5.44 pokazuje interakcję pomiędzy mocnymi stronami i zagrożeniami. Suma interakcji wyniosła 9, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 81. Na podstawie analizy tabeli można stwierdzić, że mocne strony są w stanie eliminować zagrożenia, takie jak m.in. mała liczba dostawców technologii, ukryte koszty, gdyż technologię tę można przy pomocy odpowiednich środków dostosować do potrzeb ZZK i służb ratunkowych.

Tabela 5.45 pokazuje zależności pomiędzy słabymi stronami i szansami. Suma interakcji wyniosła 12, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić w przebadanym układzie. Suma iloczynów wag oraz interakcji wynosi 108. Z analizy tabeli można stwierdzić, że szanse są w stanie zrekompensować słabe strony omawianej technologii. Słabymi stronami ograniczającymi wykorzystanie

technologii są koszty wdrożenia technologii lub brak przeszkolonego personelu, co uniemożliwia jej efektywne wykorzystanie.

Tabela 5.46 pokazuje zależności pomiędzy oddziałującymi na siebie słabymi stronami i zagrożeniami. Suma interakcji wyniosła 2, co stanowi 16% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz wag i interakcji wynosi 16. Z analizy tabeli można wyciągnąć wniosek, że pewne słabości mogą mieć wpływ na zagrożenia. Na przykład brak przeszkolonego personelu może zwiększyć podatność na cyberataki i inwigilację.

Następnie za pomocą pytań pomocniczych (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.47 pokazuje relacje pomiędzy szansami i mocnymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 36, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić w badanym układzie. Suma iloczynów wag oraz wag i interakcji wynosi 360. Z analizy tabeli można stwierdzić, że mocne strony technologii VR/AR dają szansę na usprawnienie całego procesu zarządzania kryzysowego.

Tabela 5.48 pokazuje zależności pomiędzy zagrożeniami i mocnymi stronami, które ze sobą nie oddziałują. Suma interakcji wyniosła 0. Z analizy wynika zatem, że przedstawione zagrożenia nie wpływają na mocne strony.

Tabela 5.49 pokazuje relacje pomiędzy szansami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 15, co stanowi 62,5% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz wag i interakcji wynosi 132. Z analizy tabeli można wyciągnąć wniosek, że słabe strony, takie jak koszty wdrożenia lub nieznajomość technologii mogą ograniczyć jej zastosowanie.

Tabela 5.50 przedstawia interakcje pomiędzy zagrożeniami i słabymi stronami. Suma interakcji wyniosła 4, co stanowi 33% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz wag i interakcji wynosi 36. Zagrożenia związane z wykorzystaniem technologii obejmują jej niewłaściwe wykorzystanie, uzależnienie od technologii, choroby oraz podatność cyberataki, które mogą być spowodowane słabymi stronami, takimi jak nieznajomość technologii.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.6).

Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów i ich wag.
W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab. 5.6)

Tabela 5.6. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	72	720
Mocne strony/Zagrożenia	9	81
Słabe strony/Szanse	27	240
Słabe strony/Zagrożenia	6	52

Źródło opracowanie własne

Analiza tabeli 5.6 wskazuje na przewagę mocnych stron i szans oraz brak korelacji pomiędzy mocnymi stronami i zagrożeniami. Z analizy tabeli można wywnioskować, że słabe strony wpływają na szanse i zagrożenia, niemniej jednak słabe strony dotyczą w głównej mierze nieznajomości technologii, a zagrożenia związane są m.in. z problemami zdrowotnymi, które dotyczą nielicznej grupy odbiorców.

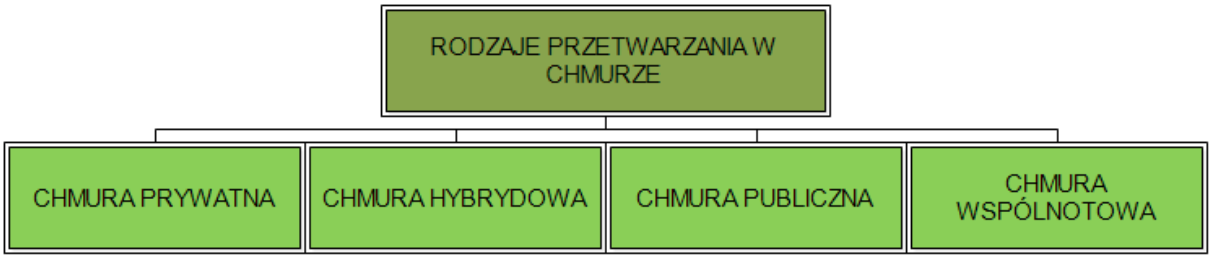
Przeprowadzona analiza SWOT-TOWS wskazuje na potencjał technologii *VR/AR*, niemniej jednak wdrożenie technologii wiąże się z pewnymi ograniczeniami. Jednym z nich jest koszt technologii i implementacja na masową skalę. Warto jednak zwrócić uwagę na fakt, że w przypadku zarządzania kryzysowego, w którym istotną rolę odgrywa bezpieczeństwo, zwiększenie świadomości sytuacyjnej na temat zagrożeń i możliwości ich materializacji nawet w warunkach ćwiczeń upoważnia do stwierdzenia, że ta technologia obniża ryzyko strat własnych i może usprawnić działania służb, co wskazuje na jej przydatność. Warto też zauważyć, że istotnym problemem związanym ze stosowaniem technologii *VR/AR* jest jej podatność na ataki oraz śledzenie, niemniej jednak problemy te powstają np. poprzez używanie aplikacji pochodzących z nieznanych źródeł, nieodpowiednie zabezpieczenie kont (bezpieczne hasła), nieodpowiednie zabezpieczenie danych. Opisane problemy nie wynikają zatem z błędów w działaniu technologii, ale z niewłaściwego jej wykorzystania. Odpowiednie szkolenia są w stanie wyeliminować opisane problemy.

5.3.4. Funkcjonalność technologii Cloud Computing *(CC)*

Ważną współcześnie technologią ICT, która umożliwia dostęp do zaawansowanych usług informacyjnych oraz eliminację lub ograniczenie wyłudzenia informacyjnego, jest przetwarzanie w chmurze (*CC*).

Technologia ta stała się szybszym, bardziej opłacalnym sposobem zarządzania, analizy i aktywacji danych, generowanych przez urządzenia IoT. Zazwyczaj nieprzetworzone dane zebrane przez czujniki są przesyłane do scentralizowanej sieci

w chmurze w celu ich analizy lub przechowywania[314]. Przetwarzanie w chmurze podkreśla synergię współczesnych technologii wspierających analizę danych i procesy decyzyjne poprzez wiele specjalizowanych usług. Można wyróżnić cztery rodzaje chmury: prywatna, hybrydowa, publiczna wspólnotowa (rys. 5.5)[315]:



Rysunek 5.5. Rodzaje chmur obliczeniowych

Źródło opracowanie własne na podstawie (https://pulpysoft.com/types-of-cloud-computing/, z dn. 13.06.2022r.

- Chmura prywatna tworzona jest dla konkretnej organizacji, wspólnoty lub grupy społecznej (np. przedsiębiorstwa, instytucji). Usługi w chmurze prywatnej dostępne są dla ograniczonej ilości użytkowników i stanowią skuteczne rozwiązanie w operowaniu danymi wrażliwymi przy zastosowaniu niezbędnych zabezpieczeń[316].

Wykorzystanie chmury prywatnej jest dedykowane dla jednego klienta/organizacji i ta usługa nie jest udostępniana innym.

- Chmura publiczna jest dostępna dla ogółu społeczeństwa, a dane są przechowywane na serwerach innych firm. Chmura ta może nie być w pełni bezpieczna do przechowywania poufnych danych[317].

W chmurze publicznej cała infrastruktura obliczeniowa znajduje się na terenie firmy, która oferuje usługę chmury. Lokalizacja pozostaje więc oddzielona od klienta i nie ma on fizycznej kontroli nad infrastrukturą. Usługi w tej chmurze bazują na współdzieleniu zasobów i wyróżniają się głównie wydajnością, ale również podatnością na różne ataki[318].

---

[314]https://www.coolfiresolutions.com/blog/5-situational-awareness-technologies/(data dostępu 30.09.2022).
[315] Tamże.
[316] A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*. Wyd. Helion, Gliwice 2011, s. 70-72.
[317] https://pulpysoft.com/types-of-cloud-computing/ (data dostępu 23.06.2022).
[318] W. K. Hon, C. Millard, I. Walden,, *Who is Responsible for 'Personal Data' in Cloud Computing?* The Cloud of Unknowing, Part 2, 2011.

- Chmura wspólnotowa to pośredni model pomiędzy chmurą prywatną, a publiczną. Podczas gdy tylko jedna firma jest właścicielem serwera chmury kilka organizacji o podobnym pochodzeniu dzieli infrastrukturę i powiązane zasoby chmury wspólnotowej[319].

Chmura wspólnotowa to infrastruktura współdzielona między organizacjami, która może należeć np. do rządu jednego kraju i może być zlokalizowana na terenie danego kraju lub poza nim[320].

- Chmura hybrydowa obejmuje najlepsze funkcje chmury publicznej, prywatnej i wspólnotowej. Pozwala firmom na wybór najlepszych funkcji i dopasowanie do potrzeb odpowiadających ich wymaganiom[321].

Chmura hybrydowa oznacza, że wykorzystuje zarówno usługi chmury prywatnej, jak i publicznej, w zależności od ich przeznaczenia[322].

Chmura obliczeniowa może realizować usługi typu: oprogramowanie jako usługa(SaaS), platforma jako usługa (*PaaS*) i infrastruktura jako usługa (*IaaS*)[323]:

- SaaS (ang. *Software-as-a-Service*) jest zdecydowanie najczęściej wykorzystywanym modelem usługi w chmurze: firmy kupują dostęp do aplikacji, ale nie ponoszą odpowiedzialności (ani nie mają kontroli nad jej wdrożeniem),
- *PaaS* (ang. *Platform-as-a-Service*) polega na dostarczeniu platformy, na której klient może uruchamiać własne aplikacje,
- *IaaS* (ang. *Infrastructure-as-a-Service*) umożliwia organizacji uruchamianie całych stosów aplikacji centrum danych, od systemu operacyjnego po aplikację, w infrastrukturze dostawcy usług.

W tabeli 5.7 przedstawiono różnice między IaaS, PaaS i SaaS.

---

[319] The National Institute of Standards and Technology: www.nit.gov/itl/-cloud/index.cfm z dn. 23.06.2022.

[320] P. Mell, T. Grance, Special Publication 800-145 (Draft): The NIST Definition of Cloud Computing (Draft) – Recommendations of the National Institute of Standards and Technology. [On-line]. National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (data dostępu 23.02.2023).

[321] R.L. Krutz, R.D. Vines Cloud Security. A comphersive Guide to Secure Cloud Computing, Indianapholis 2010, Whiley Publishing INC, s. 38.

[322] Tamże, s.38.

[323] http://bigdatariding.blogspot.com/2013/10/cloud-computing-types-of-cloud.html (data dostępu 22.09.2021).

Tabela 5.7. Różnice między IaaS, PaaS i SaaS

SaaS	PaaS	IaaS
Zapewnia wirtualne centrum danych do przechowywania informacji i tworzenia platform do tworzenia, testowania i wdrażania aplikacji.	Zapewnia wirtualne platformy i narzędzia do tworzenia, testowania i wdrażania aplikacji	Zapewnia oprogramowanie internetowe i aplikacje do wykonywania zadań biznesowych.
Zapewnia dostęp do zasobów, takich jak maszyny wirtualne, wirtualna pamięć masowa itp.	Zapewnia środowiska uruchomieniowe i narzędzia do wdrażania aplikacji.	Dostarcza oprogramowanie jako usługę dla użytkowników końcowych.
Jest używany przez architektów sieci.	Jest używany przez programistów.	Jest używany przez użytkowników końcowych
IaaS zapewnia tylko infrastrukturę.	PaaS zapewnia Infrastrukturę i platformę.	SaaS zapewnia Infrastrukturę, platformę i oprogramowanie.

Źródło opracowanie własne na podstawie https://www.javatpoint.com/cloud-service-models (data dostępu 23.01.2023)

Każdy z zawartych w tabeli 5.7 modeli jest łatwo dostępny za pośrednictwem dowolnej przeglądarki internetowej lub aplikacji. Na przykład przetwarzanie w chmurze ułatwia zespołom współpracę przy użyciu Arkuszy Google. Eliminuje to potrzebę przesyłania i wysyłania pojedynczego pliku do różnych członków zespołu[324]. Wykorzystanie chmury obliczeniowej zapewnia[325] :

- zwiększenie produktywności w miejscu pracy, co pomaga zintegrować i ujednolicić systemy robocze i procesy biznesowe w celu zwiększenia produktywności w miejscach pracy,
- redukcję kosztów, co pomaga zwiększyć rentowność działalności firmy,
- bezpieczeństwo i przywrócenie funkcjonowania po awarii,
- skalowalność i elastyczność.

Serwery oprogramowania oparte na chmurze są wygodne i łatwe w użyciu dla większości podmiotów, umożliwiając im wirtualne zarządzanie infrastrukturą techniczną organizacji, tworzenie aplikacji i dostęp do szerokiej gamy narzędzi bez konieczności zakupu danego narzędzia i utrzymywania fizycznego serwera. Usługi te mogą zwiększyć produktywność i efektywność organizacji – i w rezultacie pozytywnie wpłynąć na jej rozwój, a także przyśpieszyć i ułatwić proces zarządzania kryzysowego poprzez alternatywne możliwości dostępu do dedykowanych usług, pomocnych w przygotowaniu i rozpowszechnianiu treści przydatnych w kreowaniu świadomości

[324] L. Logeswaran, H. M. N. D. Bandara, and H. S. Bhathiya, *Performance, Resource, and Cost Aware Resource Provisioning in the Cloud*, in 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), 2016, s. 913–916.
[325] https://www.connectpos.com/major-cloud-computing-advantages/ (data dostępu 22.09.2021).

sytuacyjnej. Chmura eliminuje poniekąd ryzyko wykluczenia informacyjnego, co jest bardzo ważne z punktu widzenia dostępu do nowych technologii dla pojedynczych podmiotów o niższym statusie ekonomicznym.

W tabeli 5.8 dokonano analizy SWOT *Cloud Computing*.

Tabela 5.8. Analiza SWOT dla technologii *Cloud Computing*

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Niski koszt wdrożenia	4	W1	awarie techniczne	3
S2	Dostęp do zasobów za pośrednictwem Internetu	5	W2	wymagany dostęp do internetu	5
S3	Komunikacja z dowolnego miejsca	5	W3	brak przeszkolonego personelu	3
S4	Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	5	W4	zróżnicowany poziom bezpieczeństwa	3
S5	Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	5	W5	zależność od dostawców usług	5
S6	Tworzenie kopii zapasowych	5	W6	trudna integracja z aktualnymi rozwiązaniami	4
S7	Oszczędność energii	5	W7	ograniczenia transferu danych	3
S8	Łatwe odzyskiwanie danych po awariach	5	W8	brak możliwości wyboru fizycznej lokalizacji danych	5
S9	skalowalność i elastyczność	5	W9	dostęp do wydajnego internetu	5
S10	opłata jedynie za wykorzystane zasoby	5			
	Suma wag:	**49**		**Suma wag:**	**36**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Duża ilość przechowywanych danych i dostępność zasobów	5	T1	bezpieczeństwo danych	5
O2	nieograniczona skalowalność	5	T2	zależność od technologii	4
O3	najnowsze technologie oraz oprogramowanie	4	T3	Uzależnienie od zewnętrznego dostawcy	3
O4	Usprawnienie procesu komunikacji	5	T4	ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych)	2
O5	zwiększenie efektywności działań	5	T5	mała liczba dostawców	2
O6	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	5			
	Suma Wag:	**19**		**Suma Wag:**	**16**

Źródło: opracowanie własne.

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu zastosowano pomocniczo następujące pytania:

1) W perspektywie SWOT

- Czy mocna strona *Cloud Computing* pozwoli wykorzystać szanse? (tab. 5.51 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy mocna strona *Cloud Computing* zniweluje zagrożenia? (tab. 5.52 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy słaba strona *Cloud Computing* ogranicza wykorzystanie szansy? (tab. 5.53 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy słaba strona *Cloud Computing* może przyczynić się do wystąpienia zagrożenia? (tab. 5.54 – Załącznik nr. 5 Analiza SWOT/TOWS).

2) W perspektywie TOWS

- Czy szanse *Cloud Computing* wpływają na mocne strony? (tab. 5.55 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy zagrożenia *Cloud Computing* wpływają na mocne strony? (tab. 5.56 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy szanse *Cloud Computing* wpływają na słabe strony? (tab. 5.57 – Załącznik nr. 5 Analiza SWOT/TOWS),

Czy zagrożenia *Cloud Computing* wpływają na słabe strony? (tab. 5.58 – Załącznik nr 5. Analiza SWOT/TOWS).

W tabeli 5.51 przedstawiono zależności pomiędzy mocnymi stronami oraz szansami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy mocna strona *Cloud Computing* wpływa na szanse?" uzyskano sumę interakcji równą 49, co stanowi 81% maksymalnej liczby interakcji, które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz liczby interakcji wynosi 477. Z analizy tabeli można wywnioskować, że mocne strony takie jak m.in. niski koszt wdrożenia, dostęp do zasobów za pośrednictwem Internetu, komunikacja z dowolnego miejsca czy np. komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer) dają szansę na usprawnienie procesu komunikacji, zwiększenie efektywności działań zespołów zarządzania kryzysowego oraz służb ratowniczych.

W tabeli 5.52 przedstawiono zależności pomiędzy mocnymi stronami oraz zagrożeniami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy mocna strona *Cloud Computing* zniweluje zagrożenie?" uzyskano sumę interakcji równą 25, co stanowi 83% maksymalnej liczby interakcji, które mogą wystąpić. Łączna suma iloczynów wag oraz liczby interakcji wynosi 185. Z przeprowadzonej analizy można zatem wywnioskować, że mocne strony są w stanie zniwelować zagrożenia takie jak m.in. ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych),mała liczba dostawców.

W tabeli 5.53 przedstawiono zależności pomiędzy słabymi stronami oraz szansami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy słaba strona *Cloud Computing* ogranicza wykorzystanie szansy?" uzyskano sumę interakcji równą 35, co stanowi 65% maksymalnej liczby interakcji, które mogą wystąpić. Łączna suma iloczynów wag oraz interakcji wynosi 441. Z przeprowadzonej analizy można zatem wywnioskować, że słabe strony takie jak m.in. brak prze-

szkolonego personelu, zróżnicowany poziom bezpieczeństwa, zależność od dostawców usług, dostęp do wydajnego internetu są w stanie ograniczyć szansę wykorzystania potencjału technologii jeśli nie zostanie przygotowane odpowiednie zaplecze teleinformatyczne niezbędne do jej wdrożenia.

W tabeli 5.54 przedstawiono zależności pomiędzy słabymi stronami oraz zagrożeniami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy słaba strona *Cloud Computing* wpływa na możliwość wystąpienia zagrożenia?" uzyskano sumę interakcji równą 34, co stanowi 75,5% maksymalnej liczby interakcji, które mogą wystąpić. Łączna suma iloczynów wag oraz interakcji wynosi 250. Z przeprowadzonej analizy można zatem wywnioskować, że słabe strony mogą przyczynić się do wystąpienia zagrożeń takich jak m.in. ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych) i bezpieczeństwo danych.

Następne przeanalizowane zostały interakcje między zagrożeniami, szansami, słabymi i mocnymi stronami za pomocą pytań pomocniczych (Analiza TOWS).

W tabeli 5.55 przedstawiono zależności pomiędzy szansami oraz mocnymi stronami, między którymi występuje bardzo silna interakcja. Na podstawie odpowiedzi na pytanie „Czy szanse *Cloud Computing* wpływają na mocne strony?" uzyskano sumę interakcji równą 53, co stanowi 88% maksymalnej liczby interakcji które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 517. Na tej podstawie można stwierdzić, że poprzez usprawnienie procesu komunikacji oraz zwiększenie efektywności działań możliwa jest komunikacja z dowolnego miejsca, komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer), dostęp przez Internet do współdzielonej puli zasobów obliczeniowych, tworzenie kopii zapasowych, oszczędność energii oraz łatwe odzyskiwanie danych po awariach co nie wątpliwie stanowi mocne strony technologii *Cloud Computing*.

W tabeli 5.56 przedstawiono zależności pomiędzy zagrożeniami oraz mocnymi stronami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy zagrożenia *Cloud Computing* wpływają na mocne strony?" uzyskano sumę interakcji równą 21, co stanowi 70% maksymalnej liczby interakcji, które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 187. Z analizy tabeli można wywnioskować, zagrożenia takie jak m.in. zależność od technologii, uzależnienie od zewnętrznego dostawcy, ukryte koszty (archiwizacja danych,

rozwiązywania problemów, odzyskiwania danych) oraz mała liczba dostawców mogą wpłynąć na mocne strony technologii.

W tabeli 5.57 przedstawiono zależności pomiędzy szansami oraz słabymi stronami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy szanse *Cloud Computing* wpływają na słabe strony ?" uzyskano sumę interakcji równą 25, co stanowi 52% maksymalnej liczby interakcji, które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 223. Z analizy tabeli można wywnioskować, że usprawnienie procesu komunikacji, zwiększenie efektywności działań możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch) może zostać ograniczone poprzez awarie techniczne, wymagany dostęp do Internetu, brak przeszkolonego personelu, zróżnicowany poziom bezpieczeństwa, zależność od dostawców usług, trudna integracja z aktualnymi rozwiązaniami, ograniczenia transferu danych, brak możliwości wyboru fizycznej lokalizacji danych oraz dostęp do wydajnego Internetu.

W tabeli 5.58 przedstawiono zależności pomiędzy zagrożeniami oraz słabymi stronami, między którymi występuje interakcja. Na podstawie odpowiedzi na pytanie „Czy zagrożenia *Cloud Computing* wpływają na słabe strony?" uzyskano sumę interakcji równą 37, co stanowi 92,5% maksymalnej liczby interakcji, które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 266. Z analizy tabeli można wywnioskować, że zagrożenia takie jak bezpieczeństwo danych, zależność od technologii, uzależnienie od zewnętrznego dostawcy, ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych) oraz mała liczba dostawców mogą wpłynąć na takie aspekty jak m.in. brak przeszkolonego personelu, zróżnicowany poziom bezpieczeństwa, zależność od dostawców usług, trudna integracja z aktualnymi rozwiązaniami, ograniczenia transferu danych oraz brak możliwości wyboru fizycznej lokalizacji danych.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.9). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów ich wag.
W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab.5.9)

Tabela 5.9. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	102	994
Mocne strony/Zagrożenia	21	372
Słabe strony/Szanse	60	664
Słabe strony/Zagrożenia	71	516

Źródło: opracowanie własne

Analiza tabeli 5.9 wskazuje na przewagę mocnych stron i szans niemniej jednak warto zwrócić uwagę na zagrożenia, które mogą powstać w efekcie wykorzystywania chmury obliczeniowej. W przypadku zastosowania *CC* w procesie zarządzania kryzysowego istotny jest stały dostęp do danych oraz określona lokalizacja serwera na którym te dane są gromadzone, ponieważ mogą być objęte klauzulą poufności. Dlatego też bezpiecznym rozwiązaniem jest gromadzenia danych w chmurze obliczeniowej, która nie będzie uzależniona od zewnętrznego dostawcy. Zastosowanie tego typu rozwiązania może zmniejszyć ryzyko utraty danych na skutek awarii zewnętrznych serwerów, bądź ataków cybernetycznych. Ponadto stworzenie prywatnej chmury obliczeniowej w ramach zarządzania kryzysowego wymusza w pewnym stopniu na organach państwowych stworzenie alternatywnych źródeł zasilania i dostępu do Internetu tak, aby zapewnić ciągłość działania i przesyłanie danych w czasie rzeczywistym.

5.3.5. Technologia Blockchain

Blockchain odnosi się do rosnącej listy porcji danych (rekordów) połączonych ze sobą z uwzględnieniem procedur kryptografii. Osoby fizyczne mogą zaprogramować *Blockchain* do cyfrowego rejestrowania transakcji i tę technologię można zatem określić jako cyfrową księgę transakcji, która jest odpowiednikiem papierowej księgi rachunkowej umożliwiającej rejestrowanie kompletnych i bezpiecznych transakcji dokonywanych w ramach sieci. Pierwsze zastosowanie technologii *Blockchain* związane było z uruchomieniem krypto waluty *bitcoin*, której wartość bazuje na mocy obliczeniowej[326]. *Bitcoin* (system płatności i krypto waluta) jest najbardziej skalowalną aplikacją *Blockchain*. Technologia ta może być bardzo korzystna do poprawy przejrzystości i interoperacyjności działu zarządzania kryzysowego. Organizacje mogą wdrożyć *Blockchain* do koordynowania funduszy, pomocy i innych zasobów w nagłych wypadkach. System ten umożliwia bardziej efektywne reagowanie kryzysowe, a jego użytkownicy mogą monitorować swoje transakcje. Korupcja i nieautoryzowane przekierowanie zasobów staje się zatem mało prawdopodobne [327].

Technologia *Blockchain* i związana z nią wiedza może być wykorzystywana w zarządzaniu kryzysowym, ponieważ spełnia wszystkie wymagania dotyczące bezpieczeństwa informacji przekazywanej w sytuacjach kryzysowych. Potrzeba termi-

[326] https://businessinsider.com.pl/poradnik-finansowy/blockchain-na-czym-polega/fdctpsb (data dostępu 29.09.2021).
[327] https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/ (data dostępu 30.09.2021).

nowych, dokładnych i wiarygodnych informacji wydaje się być zaspokajana przez technologię *Blockchain*. Problemy, które mogą pojawić w sytuacjach kryzysowych, to m.in. trudności w znalezieniu najbliższego centrum pomocy, przerwy w dostawie prądu, nierównomierny rozkład wody i żywności, znajdowanie zaginionych osób, liczenie rannych osób i szkód, transport i zabezpieczenie dobra ludzi[328]. *Blockchain* ma potencjał, aby skutecznie wspomagać rozwiązywanie tej klasy problemów bez opóźnień. *Blockchain* jest w stanie zapewnić silne wsparcie dla zarządzania kryzysowego dzięki swoim zaletom technicznym, takim jak rozproszone przechowywanie, decentralizacja, algorytmy konsensusu, zabezpieczenie przed manipulacją czy identyfikowalność. Wdrożenie technologii *Blockchain* może m.in. przyspieszyć akcje ratownicze oraz zwiększyć świadomość sytuacyjną, ale wdrożenie tej technologii jest złożonym procesem wymagającym współpracy wszystkich służb[329]. W tabeli 5.10 zaprezentowano wyniki analizy SWOT dla technologii *Blockchain*.

Tabela 5.10. Analiza SWOT technologii *Blockchain*

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Łatwość dostępu	4	W1	Brak wykwalifikowanych osób	3
S2	Kontrola zasobów	5	W2	Wysokie zużycie energii	5
S3	Stanowi własność użytkownika	5	W3	Dostęp wyłącznie za pośrednictwem Internetu	3
S4	Szyfrowanie danych	5	W4	wymaga wysokowydajnościowego sprzętu	3
S5	Transakcje bez osób trzecich	5	W5	zależność od Internetu	5
S6	Weryfikacja tożsamości	5	W6	trudna integracja z innymi systemami	4
	Suma Wag:	**29**		**Suma Wag:**	**23**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	usprawnienie zarządzania kryzysowego	5	T1	utrata dostępu przy braku klucza prywatnego	5
O2	zwiększenie świadomości sytuacyjnej na temat zagrożeń	5	T2	brak dostępu do Internetu czyni technologię bezużyteczną	4
O3	najnowsze technologie oraz oprogramowanie	4	T3	podatność na ataki i kradzież danych	3
O4	Zabezpieczenie danych	5			
O5	zwiększenie efektywności działań	5			
	Suma Wag:	**14**		**Suma Wag:**	**12**

Źródło: opracowanie własne

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu sformułowano dodatkowe pytania:

1) W perspektywie SWOT:

- Czy mocna strona *Blockchain* może wykorzystać szanse? (tab. 5.59 – Załącznik nr. 5 Analiza SWOT/TOWS *Blockchain*),

[328] X. Yue, H. Wang, D. Jin, M. Li ,W. Jiang, *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,* J Med Syst 2016; 40(10): s. 1-8.
[329] S. Alsalamah, E. Nuzzolese, *Promising blockchain technology applications and use case designs for the identification of multinational victims of mass disasters*. Front Blockchain 2020; 3: s. 34.

- Czy mocna strona *Blockchain* przeważają nad zagrożenia? (tab. 5.60 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy słaba strona *Blockchain* ogranicza wykorzystanie szansy? (tab. 5.61 – Załącznik nr. 5 Analiza SWOT/TOWS *Blockchain*),
- Czy słaba strona *Blockchain* może mieć wpływ na wystąpienie zagrożenia? (tab. 5.62 – Załącznik nr 5 Analiza SWOT/TOWS *Blockchain*).

2) W perspektywie TOWS:

- Czy szanse *Blockchain* wpływają na mocne strony? (tab. 5.63 – Załącznik nr 5 Analiza SWOT/TOWS *Blockchain*),
- Czy zagrożenia *Blockchain* wpływają na mocne strony? (tab. 5.64 – Załącznik nr. 5 Analiza SWOT/TOWS *Blockchain*),
- Czy szanse *Blockchain* wpływają na słabe strony? (tab. 5.65 – Załącznik nr. 5 Analiza SWOT/TOWS *Blockchain*),
- Czy zagrożenia *Blockchain* wpływają na słabe strony? (tab. 5.66 – Załącznik nr. 5 Analiza SWOT/TOWS).

Tabela 5.59 pokazuje związki pomiędzy mocnymi stronami a szansami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 30, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 289. Na podstawie analizy tabeli można stwierdzić, że potencjał technologii Blockchain może sprzyjać doskonaleniu całego procesu zarządzania kryzysowego, a wykorzystanie mocnych stron takich jak m.in. łatwość dostępu, szyfrowanie danych, transakcje bez stron trzecich, kontrola tożsamości mogą usprawnić zarządzanie kryzysowe, zwiększyć świadomość sytuacyjną na temat zagrożeń, zabezpieczyć dane i zwiększyć efektywność operacyjną.

Tabela 5.60 pokazuje relacje pomiędzy mocnymi stronami a zagrożeniami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 18, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić w danym układzie. Suma iloczynów wag oraz interakcji wynosi 159. Z analizy tabeli można wyciągnąć wniosek, że mocne strony technologii mogą eliminować potencjalne zagrożenia, jeśli zostaną właściwie wdrożone i wykorzystane.

Tabela 5.61 pokazuje relacje pomiędzy słabymi stronami a szansami.?” suma interakcji wyniosła 24, co stanowi 80% maksymalnej liczby interakcji możliwych do wystąpienia. Suma iloczynów wag oraz interakcji wynosi 206. Z analizy tabeli można stwierdzić, że słabe strony takie jak. brak wykwalifikowanego personelu, dostęp wy-

łącznie za pośrednictwem Internetu, wysokowydajnościowy sprzęt, zależność od Internetu i skomplikowana integracja z innymi systemami wpływają na możliwości wykorzystania szans.

Tabela 5.62 pokazuje zależności pomiędzy słabymi stronami i zagrożeniami. Suma interakcji wyniosła 9, co stanowi 50% maksymalnej liczby interakcji, jaka może. Całkowita suma iloczynów wag oraz interakcji wynosi 69. Z analizy tabeli można wyciągnąć wniosek, że słabe strony takie jak m.in. brak wykwalifikowanej kadry, skomplikowana integracja z innymi systemami i dostęp wyłącznie przez Internet może prowadzić do zagrożeń powodujących utratę dostępu w przypadku braku klucza prywatnego, brak połączenia z Internetem, co sprawia, że technologia jest bezużyteczna i podatna na ataki i kradzież danych.

Następne przeanalizowane zostały interakcje między zagrożeniami, szansami, słabymi i mocnymi stronami za pomocą pytań pomocniczych (Analiza TOWS)

Tabela 5.63 pokazuje relacje pomiędzy szansami i mocnymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 24, co stanowi 80% maksymalnej liczby interakcji, jaka może wystąpić. Całkowita suma iloczynów wag oraz interakcji wynosi 299. Z analizy tabeli można wyciągnąć wniosek, że szanse takie jak m.in. doskonalenie zarządzania kryzysowego, podnoszenie świadomości sytuacyjnej na temat zagrożeń, najnowsze technologie i oprogramowanie, bezpieczeństwo danych, efektywność operacyjna mogą poprawić zarządzanie kryzysowe dzięki m.in. łatwości obsługi, kontroli zasobów i szyfrowaniu danych.

Tabela 5.64 pokazuje zależności pomiędzy zagrożeniami oraz mocnymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 14, co stanowi 77% maksymalnej liczby interakcji, jaka może wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 125. Na tej podstawie można stwierdzić, że zagrożenia takie jak m.in. Przerwa w połączeniu internetowym, brak klucza prywatnego mogą wpłynąć na mocne strony technologii, jednakże zbudowanie odpowiednich zasobów IT może wyeliminować tego typu zagrożenia.

W tabeli 5.65 zaprezentowano relacje pomiędzy szansami i słabymi stronami między, którymi występuje bardzo silna interakcja wynosząca 29, co stanowi 97%. Łączna suma iloczynów wag oraz interakcji wynosi 251. Na podstawie analizy tabeli można stwierdzić, że możliwości technologii Blockchain, takie jak m.in. łatwość obsługi, zarządzanie zasobami, szyfrowanie danych, lepsze zarządzanie kryzysowe,

zwiększona świadomość sytuacyjna na temat zagrożeń, najnowsze technologie oraz bezpieczeństwo oprogramowania i informacji mogą ograniczyć zagrożenia.

Tabela 5.66 pokazuje zależności pomiędzy zagrożeniami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 18, co stanowi 100% maksymalnej możliwej liczby interakcji badanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 153. Z analizy tabeli można stwierdzić, że zagrożenia technologii Blockchain wpływają na słabe strony technologii.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.11). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów i ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab.5.11)

Tabela 5.11. Zestawienie interakcji

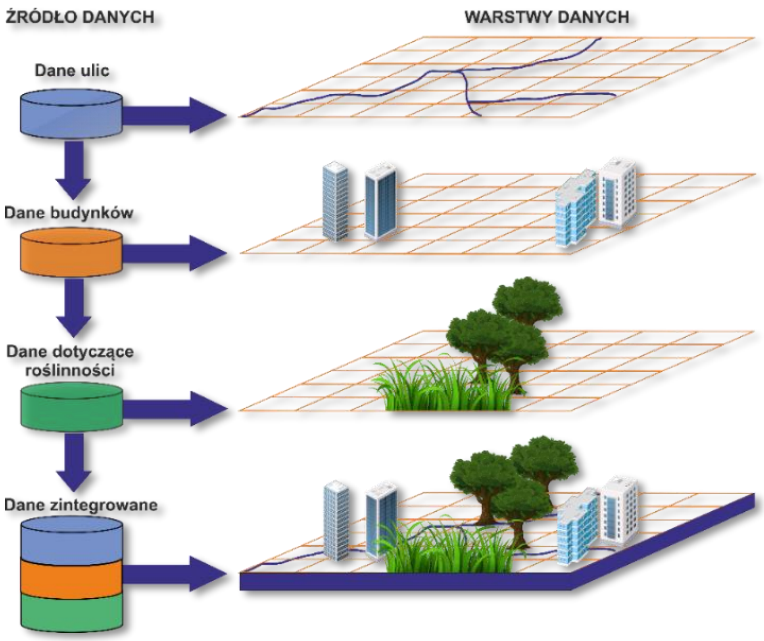
Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	54	588
Mocne strony/Zagrożenia	32	284
Słabe strony/Szanse	53	457
Słabe strony/Zagrożenia	27	222

Źródło: opracowanie własne

Z analizy tabeli 5.11 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabości mogą te szanse ograniczać, a także stwarzać zagrożenia. Wynika to z nieznajomości technologii, braku odpowiedniego sprzętu np. wysokowydajnościowych komputerów do gromadzenia i przetwarzania danych, a także z braku alternatywnego dostępu do sieci internetowej lub z błędów ludzkich takich jak np. utrata klucza szyfrującego. Można zatem stwierdzić, że wskazane słabe strony i zagrożenia są możliwe do ograniczania i technologia *Blockchain* może stać się skutecznym narzędziem możliwym do wykorzystania w zarządzaniu kryzysowym.

5.3.6. Możliwości Systemów Informacji Geoprzestrzennej (GIS)

System Informacji Geoprzestrzennej (GIS) to komputerowy system przechwytywania, przechowywania, sprawdzania i wyświetlania danych związanych z pozycjami różnych obiektów na powierzchni Ziemi. GIS może wyświetlać wiele różnych rodzajów danych na jednej mapie związanych z takimi obiektami, jak ulice, budynki, zbiory flory, fauny itp. (rys 5.6). Oprócz informacji o poszczególnych obiektach, systemy informacyjne przechowują również relacje między tymi obiektami. Mogą to być relacje informacyjne lub przestrzenne lub obie kategorie relacji mogą zostać zmapowane.



Rysunek 5.6. Modele i warstwy danych w systemach GIS – warstwy tematyczne

Źródło: opracowanie własne na podstawie http://www.nationalgeographic.org (data dostępu 03.01.2023)

Można zatem przyjąć, że Systemy Informacji Geoprzestrzennej przeznaczone są do analizowania i prezentowania wszystkich typów danych, a kluczową rolę w tej technologii odgrywa atrybut lokalizacji przestrzennej na Ziemi. Dane atrybutów można ogólnie zdefiniować jako dodatkowe informacje o każdym z elementów przestrzennych. Przykładem tego mogą być szkoły ze swoją rzeczywistą lokalizacją a dodatkowe dane takie, jak nazwa szkoły, poziom nauczania i liczba uczniów, to dane atrybutów obiektu[330]. Powiązanie tych dwóch typów danych sprawia, że GIS może stać się skutecznym narzędziem analizy sytuacyjnej z wykorzystaniem parametrów lokalizacji geoprzestrzennej. Technologia GIS umożliwia więc analizę i zarządzanie dużymi zbiorami danych oraz zobrazowanie sytuacji z wykorzystaniem mapy/grafiki[331] w wielu dziedzinach, w tym m.in. w kartografii, urbanistyce, kryminologii (mapy przestępczości), logistyce, zarządzaniu zasobami, opiece zdrowotnej i ogólnie w zarządzaniu kryzysowym. Na przykład za pomocą GIS funkcjonariusze służb ochrony ludności mogą gromadzić informacje odnośnie ewakuacji z uwzględ-

[330] J. Gaździcki, *Technologie i infrastruktury informacji przestrzennej w zastosowaniu do zarządzania kryzysowego,* Warszawa: Roczniki Geomatyki, tom IV, zeszyt 1.,2006, s. 22.
[331] https://www.gislounge.com/ (data dostępu 7.11.2022).

nieniem np. dróg ewakuacji na obszarach zagrożonych (podmokłych) i szczególnie wrażliwych[332].

Wraz z rosnącą liczbą danych coraz ważniejsze staje się efektywne zarządzanie geodanymi i ciągła aktualizacja metadanych. Niektóre narzędzia GIS mają wbudowaną obsługę metadanych, podczas gdy inne systemy pozostawiają użytkownikowi swobodę zarządzania za pomocą innych programów[333].

W celu oceny możliwości wykorzystania technologii GIS w kreowaniu świadomości sytuacyjnej, szczególnie w aspekcie lepszego rozumienia sytuacji i zagrożeń, które mogą zaistnieć - dokonano analizy SWOT (tab. 5.12).

Tabela 5.12. Analiza SWOT dla technologii Systemów Informacji Geoprzestrzennej

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Szybkie i proste przeglądanie dużych zbiorów danych	5	W1	Duże koszty wdrożenia	4
S2	Pobieranie danych	5	W2	Brak znajomości technologii	4
S3	Analiza, monitorowanie, raportowanie danych w systemie	5	W3	Potrzeba przeszkolenia pracowników	3
S4	Lokalizacja ważnych punktów z perspektywy ZK	5	W4	Ograniczenia czasowe	4
S5	Tworzenie planu odbudowy	5	W5	Brak dostępu do danych	3
S6	Analiza danych	5			
S7	Opracowywanie scenariuszy planów ZK	5			
S8	Opracowywanie przyszłych działań dla ZK	5			
	Suma wag:	**40**		**Suma wag:**	**18**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Ułatwiony przekaz informacji	5	T1	Awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych	5
O2	Zwiększenie świadomości sytuacyjnej na temat zagrożeń	5	T2	Awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych	3
O3	Możliwość wizualizacji zagrożeń	4	T3	Błędna wizualizacja danych	3
O4	Możliwość opracowywania scenariuszy przyszłych zagrożeń	5	T4	Poleganie wyłącznie na technologii może wygenerować zagrożenia dla życia lub zdrowia	3
O5	Zwiększenie efektywności działań	5			
O6	Usprawnienie działania służb ratowniczych	4			
	Suma wag:	**18**		**Suma wag:**	**14**

Źródło: opracowanie własne

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu sformułowano następujące pytania:

1) W perspektywie SWOT:

- Czy mocne strony GIS mogą wykorzystać szanse? (tab. 5.67 – Załącznik nr. 5 Analiza SWOT/TOWS),

[332] Tamże.

[333] A. Magnuszewski, *Zastosowanie techniki GIS w ocenie zagrożeń naturalnych – dawnych i przyszłych,* [w:] Ciupa T., Suligowski R. (red.) *Woda w badaniach geograficznych*, Instytut Geografii Uniwersytet Jana Kochanowskiego, Kielce 2010, s. 33.

- Czy mocne strony GIS przeważają nad zagrożeniami? (tab. 5.68 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy słaba strona GIS ogranicza wykorzystanie szansy? (tab. 5.69 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy słaba strona GIS może mieć wpływ na zagrożenia? (tab. 5.70 – Załącznik nr. 5 Analiza SWOT/TOWS).

2) W perspektywie TOWS:

- Czy szanse GIS wpływają na mocne strony? (tab. 5.71 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy zagrożenia GIS wpływają na mocne strony? (tab. 5.72 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy szanse GIS wpływa na słabe strony? (tab. 5.73 – Załącznik nr. 5 Analiza SWOT/TOWS),
- Czy zagrożenia GIS wpływają na słabe strony? (tab. 5.74 – Załącznik nr. 5 Analiza SWOT/TOWS).

Tabela 5.67 pokazuje relacje pomiędzy mocnymi stronami i szansami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 48, co stanowi 100% maksymalnej możliwej liczby interakcji jaka może wstąpić w przebadanym układzie. . Łączna suma iloczynów wag oraz interakcji wynosi464. Na podstawie analizy tabeli można stwierdzić, że potencjał technologii GIS pozwala na usprawnienie całego procesu zarządzania kryzysowego.

Tabela 5.68 pokazuje relacje pomiędzy mocnymi stronami i zagrożeniami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 20, co stanowi 83% maksymalnej liczby interakcji, jaka może wystąpić w przedstawionym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 172. Z analizy tabeli można wyciągnąć wniosek, że mocne strony technologii takie jak m.in. szybkie i łatwe przeglądanie dużych zbiorów danych, przesyłanie danych, analiza, monitorowanie, raportowanie, lokalizacja ważnych punktów w systemie dla zarządu, tworzenie planu przebudowy, analiza danych, opracowywanie scenariuszy planów ZK i opracowywanie przyszłych działań ZK są w stanie ograniczyć lub nawet zniwelować zagrożenia.

Tabela 5.69 pokazuje zależności pomiędzy słabymi stronami a szansami. Suma interakcji wyniosła 20, co stanowi 66% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Suma iloczynów wag oraz interakcji wynosi 163. Na podstawie analizy tabeli można zauważyć, że na możliwość wykorzystania potencja-

łu technologii wpływają pewne słabe strony, takie jak wysokie koszty wdrożenia, nieznajomość technologii i ograniczenia czasowe. Jednakże ograniczenia te mogą być widoczne na wczesnych etapach wdrażania technologii.

Tabela 5.70 pokazuje zależności pomiędzy oddziałującymi na siebie słabymi stronami i zagrożeniami. Suma interakcji wynosi 6, co stanowi 30% maksymalnej możliwej liczby interakcji. Łączna suma iloczynów wag oraz interakcji wynosi 40. Z analizy tabeli można wyciągnąć wniosek, że pewne słabe strony takie, jak np. wysokie koszty wdrożenia, brak wiedzy technologicznej, ograniczenia czasowe i potrzeba szkolenia pracowników, wpływają na możliwość wystąpienia zagrożeń.

Następnie za pomocą pytań pomocniczych (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.71 pokazuje relacje pomiędzy szansami i mocnymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wynosi 48, co stanowi 100% maksymalnej liczby interakcji, które mogą wystąpić w przebadanym układzie. Łączna suma iloczynów wag oraz interakcji wynosi 528. Z analizy tabeli można wywnioskować, że mocne strony technologii GIS dają szansę usprawnienia całego procesu związanego z zarzadzaniem kryzysowym poprzez silny wpływ na poziom świadomości sytuacyjnej (szybszego i lepszego rozumienia dzięki zobrazowaniu i wizualizacji).

W tabeli 5.72 przedstawiono zależności pomiędzy zagrożeniami oraz mocnymi stronami, między którymi występuje bardzo silna interakcja. Suma interakcji wynosi 21, co stanowi 65% maksymalnej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 202. Z analizy tabeli wynika, że takie jak m.in. awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych, awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych technologii GIS są w stanie ograniczyć mocne strony technologii.

Tabela 5.73 pokazuje relacje pomiędzy szansami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 20, co stanowi 80% maksymalnej liczby interakcji, jaka może wystąpić. Łączna suma wag i interakcji wynosi 196. Z analizy tabeli można wywnioskować że słabe strony technologii GIS, takie jak wysokie koszty wdrożenia, brak wiedzy o technologii, konieczność szkoleń pracowników, ograniczenia czasowe. i brak gromadzenia informacji, wpływają na możliwość usprawnienia całego procesu związanego z zarządzaniem kryzysowym.

Tabela 5.74 pokazuje zależności pomiędzy zagrożeniami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 12, co stanowi 60% maksymalnej liczby interakcji. Natomiast suma wag i interakcji wynosi 82. Z analizy tabeli wynika, że zagrożenia mogą oddziaływać na takie słabe strony jak m.in. brak dostępu do informacji, brak wiedzy technologicznej i brak dostępu do informacji.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.13). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów i ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab. 5.13)

Tabela 5.13. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów wag
Mocne strony/Szanse	96	792
Mocne strony/Zagrożenia	41	374
Słabe strony/Szanse	44	359
Słabe strony/Zagrożenia	18	122

Źródło: opracowanie własne

Z analizy tabeli 5.13 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabe strony mogą ograniczać wspomniane szanse, ale także stwarzać zagrożenia. Ograniczenia te związane są ze słabszą powszechnością tej technologii w wersji zaawansowanej i ograniczona znajomością jej funkcji, a także z błędami ludzkimi takimi jak np. nieprawidłowa wizualizacja. Można zatem stwierdzić, że wskazane słabe strony i zagrożenia są możliwe do wyeliminowania dzięki czemu technologia GIS, może stać się skutecznym narzędziem możliwym do kreowania świadomości sytuacyjnej i sprawniejszego zarządzania sytuacjami kryzysowymi.

5.3.7. Funkcjonalność systemów klasy OLAP

Systemy klasy OLAP umożliwiają wieloaspektową analizę i ocenę sytuacji kryzysowych. Zastosowanie tej klasy systemów umożliwia oszacowanie ryzyka wystąpienia sytuacji kryzysowych na podstawie kolekcji danych historycznych. Przetwarzanie dużej liczby danych jest w stanie zapobiec niektórym zagrożeniem oraz umożliwia prognozowanie w czasie rzeczywistym. Pomimo, iż istnieje wiele usług monitorujących i rejestrujących wyniki tego procesu w bieżących bazach danych, nie istnieje zintegrowany system monitorowania i rejestracji wyników w dłuższym horyzoncie czasowym, umożliwiającym poszukiwanie analogii i trendów zachowań. Monitorowanie i gromadzenie danych w czasie rzeczywistym i uzupełnianie nimi kolekcji danych

historycznych jest niezbędne do poprawy efektywności zarządzania kryzysowego[334]. Funkcjonalność systemów klasy OLAP może zatem zostać zastosowana do wieloaspektowej analizy zagrożeń, oszacowania ryzyka wystąpienia sytuacji kryzysowych oraz do prognozowania jej skutków. Znaczenie systemów klasy OLAP wynika głównie ze wspomagania procesów analityczno-decyzyjnych. Eksploracja danych na zaawansowanym poziomie stanowi cenne źródło do wiarygodnego planowania strategicznego i podejmowania decyzji[335].

Przetwarzanie analityczne *online* (OLAP) organizuje duże bazy danych oraz obsługuje złożone analizy danych. Może zatem zostać wykorzystane do poszukiwania odpowiedzi na złożone zapytania analityczne bez ujemnego wpływu na działania bieżące (systemy transakcyjne). Bazy danych używane do przechowywania danych bieżących służą do przetwarzania transakcji *online* (OLTP)[336]. Bazy te odwzorowują wprowadzane pojedynczo rekordy danych dla ZZK[337] i stanowią źródło zasileń informacyjnych dla systemów OLAP (hurtownie danych). W tabeli 5.14 przedstawiono analizę SWOT systemów OLAP.

Tabela 5.14. Analiza SWOT systemów OLAP w aspekcie zarządzania kryzysowego

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Eksploracja danych	5	W1	Duże koszty wdrożenia	3
S2	Wspomaganie decyzji i raportowanie	5	W2	Brak znajomości technologii	1
S3	Szybka analiza wielowymiarowych informacji	5	W3	Potrzeba przeszkolenia pracowników	4
S4	Elastyczność	5	W4	Ograniczenia czasowe	5
S5	Łatwość dostępu do danych	5	W5	Zależność od sprawności infrastruktury technicznej (sieci energetycznej i Internetu)	5
S6	Konsolidacja	5			
S7	Łatwa analiza i obliczenia na danych	5			
S8	Szybkie poszukiwanie odpowiedzi na złożone zapytania analityczne	5			
	Suma wag:	**40**		**Suma wag:**	**18**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Ułatwiony przekaz informacji	5	T1	Podatność na ataki	5
O2	Zwiększenie świadomości sytuacyjnej na temat zagrożeń	5	T2	Awaria infrastruktury teleinformatycznej może unieruchomić technologię	3
O3	Możliwość klasyfikacji zagrożeń	4	T3	Błąd ludzki	1
O4	Cyfryzacja	5	T4	Awaria infrastruktury energetycznej może unieruchomić technologię	5
O5	Możliwość gromadzenia dużej ilości danych	5			
O6	Szybki dostęp do danych z dowolnego miejsca	4			
	Suma wag:	**18**		**Suma wag:**	**14**

Źródło: opracowanie własne

[334] A. Cuzzocrea, V. Russo, D. Saccà, *A Robust Sampling-Based Framework for Privacy Preserving OLAP*. DaWaK, 2008, s. 97-114.
[335] P. Zaskórski, Asymetria informacyjna w zarządzaniu procesami, Wojskowa Akademia Techniczna, Warszawa 2012, s. 263.
[336] https://learn.microsoft.com/en-us/azure/architecture/data-guide/relational-data/online-transaction-processing (data dostępu 7.11.2022).
[337] Tamże.

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu sformułowano następujące pytania:

1) Z perspektywy SWOT:

- Czy mocne strony OLAP mogą wykorzystać szanse? (tab. 5.75 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP),
- Czy mocne strony OLAP przeważają nad zagrożeniami? (tab. 5.76 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP,
- Czy słaba strona OLAP ogranicza wykorzystanie szansy? (tab. 5.77 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP),
- Czy słaba strona OLAP może mieć wpływ na zagrożenia? (tab. 5.78 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP).

2) Z perspektywy TOWS:

- Czy szanse OLAP wpływają na mocne strony? (tab. 5.79 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP),
- Czy zagrożenia OLAP wpływają na mocne strony ? (tab. 5.80 – Załącznik nr. 5 Analiza SWOT/TOWS *OLAP*),
- Czy szanse OLAP wpływają na słabe strony? (tab. 5.81 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP),
- Czy zagrożenia OLAP wpływają na słabe strony? (tab. 5.82 – Załącznik nr. 5 Analiza SWOT/TOWS OLAP).

Tabela 5.75 pokazuje związki pomiędzy mocnymi stronami i szansami, które wzajemnie na siebie oddziałują. Łącznie uzyskano 48 interakcji, co stanowi 100% maksymalnej możliwej liczby, które mogą wystąpić. Łączna suma iloczynów wag oraz interakcji wynosi 464. Na podstawie analizy tabeli można zauważyć, że potencjał technologii OLAP może znacząco usprawnić procesy analityczne i decyzyjne w procesie zarządzania kryzysowego, kreując świadomość sytuacyjną osób funkcyjnych i decydentów na odpowiednim poziomie.

Tabela 5.76 pokazuje relacje pomiędzy mocnymi stronami i zagrożeniami. Suma interakcji wyniosła 16, co stanowi 66% maksymalnej liczby interakcji, jaka może wystąpić w zaproponowanym układzie. Suma iloczynów wag oraz interakcji wynosi 132. Analiza tabeli pokazuje jednoznacznie, że pomimo mocnych stron technologii, zagrożenia takie jak narażenie na ataki, awaria infrastruktury teleinformatycznej, awaria

infrastruktury energetycznej czy błąd ludzki mogą . spowodować zatrzymanie lub nieprawidłowe działanie technologii.

Tabela 5.77 pokazuje relacje pomiędzy słabymi stronami a szansami. Na tej podstawie uzyskano 21 interakcji, co stanowi 70% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 166. Analiza tabeli pokazuje, że słabe strony, takie jak wysokie koszty wdrożenia, niewystarczająca znajomość technologii, konieczność szkolenia pracowników, ograniczenia czasowe oraz uzależnienie od wydajności infrastruktury technicznej (sieć elektroenergetyczna i Internet) mogą ograniczać . możliwości technologii.

Tabela 5.78 pokazuje zależności pomiędzy słabymi stronami oraz zagrożeniami. Suma interakcji wyniosła 6, co stanowi 20% maksymalnej liczby interakcji, jakie mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 40. Z analizy tabeli można wyciągnąć wniosek, że niektóre słabe strony takie, jak np Ograniczenia czasowe lub brak przeszkolonego personelu mogą mieć wpływ na możliwość wystąpienia zagrożenia.

Następnie za pomocą pytań pomocniczych (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.79 pokazuje relacje pomiędzy szansami i mocnymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 48, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. Łączna iloczynów wag oraz interakcji wynosi 464. Na podstawie analizy tabeli można zauważyć, że mocne strony technologii OLAP dają ogromne możliwości usprawnienia procesu zarządzania kryzysowego.

Tabela 5.80 przedstawia zależności pomiędzy interaktywnymi zagrożeniami, a mocnymi stronami. Suma interakcji wyniosła 7, co stanowi 21% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Suma iloczynów wag oraz interakcji wynosi 42. Z analizy tabeli można wyciągnąć wniosek, że zagrożenia takie jak awaria infrastruktury informatycznej czy energetycznej mogą ograniczać mocne strony technologii.

Tabela 5.81 pokazuje relacje pomiędzy szansami a słabymi stronami. Suma interakcji wyniosła 18, co stanowi 60% maksymalnej liczby interakcji, jaka może wystąpić. Całkowita suma iloczynów wag oraz interakcji wynosi 163. Na tej podstawie można stwierdzić, że możliwości takie jak. łatwiejsza transmisja danych, zwiększona świadomość sytuacyjna na temat zagrożeń, możliwość klasyfikacji zagrożeń, możli-

wość gromadzenia dużej ilości danych i szybki dostęp do danych z dowolnego miejsca są w stanie ograniczyć słabości wynikające z deklarowanego potencjału technologii.

Tabela 5.82 pokazuje zależności pomiędzy zagrożeniami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 10, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Suma iloczynów wag oraz interakcji wynosi 72. Z analizy tabeli wynika, że zagrożenia takie jak m.in. awarie technologii infrastruktury informacyjno-komunikacyjnej, błędy ludzkie i awarie infrastruktury energetycznej wpływają na słabe strony technologiczne.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.15). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab.5. 15)

Tabela 5.15. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów
Mocne strony/Szanse	96	928
Mocne strony/Zagrożenia	23	174
Słabe strony/Szanse	39	329
Słabe strony/Zagrożenia	16	112

Źródło: opracowanie własne

Z analizy tabeli 5.15 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabe strony mogą ograniczać wspomniane szanse, ale także stwarzać zagrożenia. Ograniczenia te związane są z nieznajomością przede wszystkim funkcjonalności technologii oraz dość wysokim kosztem wysokowydajnościowych komputerów do gromadzenia i przetwarzania danych. Można zatem stwierdzić, że wskazane słabe strony i zagrożenia są możliwe do wyeliminowania dzięki czemu technologia OLAP, może stać się skutecznym narzędziem doskonalącym poziom świadomości sytuacyjnej osób funkcyjnych w ZZK i decydentów w SZK.

5.3.8. Funkcjonalność systemów klasy OLTP

Perspektywa przetwarzania danych transakcyjnych, odwzorowujących bieżące działania jest realizowana za pomocą systemów klasy *online* (OLTP). Zadaniem tych systemów jest rejestrowanie bieżących zdarzeń na podstawie monitoringu realizowanych procesów. Systemy klasy OLTP swój pierwowzór mają w obszarze biznesowym, ale zyskały miano standardów komercyjnych wykorzystywanych powszechnie także w strukturach administracji publicznej. Wykorzystywane są do wydajnego prze-

twarzania i przechowywania danych[338]. Wdrożenie i korzystanie z systemów klasy OLTP może stanowić wyzwanie, ponieważ systemy OLTP nie są przeznaczone do obsługi dużej ilości danych. Ważne natomiast jest, że bazy danych transakcyjnych, utrzymywanych w tych systemach stanowią zasilenia informacyjne dla systemów OLAP, które funkcjonują na dużych objętościach danych (hurtownie danych jako kolekcje danych statystycznych, niezmienialnych), takie jak rozwiązanie oparte na *SQL* Server[339]. Stąd systemy OLTP mają istotne znaczenie, ponieważ bez transakcyjnych baz danych nie dałoby się zbudować hurtowni danych i wykorzystać funkcji agregacji danych, jak w systemach OLAP.

W tabeli 5.16 przedstawiono wyniki analizy SWOT dla systemów klasy OLTP.

Tabela 5.16. Analiza SWOT OLTP

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	współbieżność	5	W1	kopie zapasowe	3
S2	integralność danych	5	W2	podatność na awarię	1
S3	proste transakcje i zapytania	5	W3	zapytania *SQL*	4
S4	zindeksowane zestawy danych	5	W4	zależność od personelu	5
S5	czas reakcji	5	W5	koszt wdrożenia	5
S6	dostępność	5			
S7	rozmiar danych	5			
S8	atomowość	5			
	Suma wag:	**40**		**Suma wag:**	**18**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	ułatwiony przekaz informacji	5	T1	utrata danych	5
O2	zwiększenie świadomości sytuacyjnej na temat zagrożeń	5	T2	podatność na ataki	3
O3	możliwość klasyfikacji zagrożeń	3	T3	błąd ludzki	4
O4	cyfryzacja	4	T4	awaria infrastruktury technicznej (np. energetycznej) może unieruchomić technologię	5
O5	możliwość gromadzenia dużej ilości danych	4			
O6	szybki dostęp do danych z dowolnego miejsca	4			
	Suma wag:	**15**		**Suma wag:**	**17**

Źródło: opracowanie własne

Określenie mocnych i słabych stron, szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu zastosowano pomocniczo następujące pytania:

1) Z perspektywy SWOT:

- Czy mocne strony OLTP mogą wykorzystać szanse? (tab. 5.83 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP),
- Czy mocne strony OLTP przeważają nad zagrożeniami? (tab. 5.84 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP,

[338] S. A. Buckler, *The Spiritual Nature of Innovation*. Research Technology Management, 1997, Vol 40/2, s. 43-47.

[339] https://learn.microsoft.com/en-us/sql/relational-databases/in-memory-oltp/survey-of-initial-areas-in-in-memory-oltp?view=sql-server-ver16 (data dostępu 20.01.2023).

- Czy słaba strona OLTP ogranicza wykorzystanie szansy? (tab. 5.85 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP),
- Czy słaba strona OLTP może mieć wpływ na zagrożenia? (tab. 5.86 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP).

2) W perspektywie TOWS:

- Czy szanse OLTP wpływają na mocne strony? (tab. 5.87 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP),
- Czy zagrożenia OLTP wpływają na mocne strony ? (tab. 5.88 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP),
- Czy szanse OLTP wpływają na słabe strony? (tab. 5.89 – Załącznik nr. 5 Analiza SWOT/TOWS OLTP),
- Czy zagrożenia *OLTP* wpływają na słabe strony? (tab. 5.90 – Załącznik nr. 5 Analiza SWOT/TOWS *OLTP*).

Tabela 5.83 pokazuje relacje pomiędzy mocnymi stronami i szansami, które wchodzą w bardzo silną interakcję. Łącznie uzyskano 48 interakcji, co stanowi 100% maksymalnej możliwej liczby interakcji, która może wystąpić. Suma iloczynów wag oraz interakcji wynosi 440. Z analizy tabeli można wywnioskować, że możliwości technologii OLTP pozwalają na usprawnienie procesu zarządzania kryzysowego poprzez rejestrację ciągłego monitorowania realizowanych procesów oraz utrzymanie spójnej bazy danych.

W tabeli 5.84 przedstawiono związki pomiędzy mocnymi stronami i zagrożeniami między, którymi zachodzi interakcja. Suma interakcji wyniosła 9, co stanowi 37,5% maksymalnej liczby interakcji, jaka może wystąpić w danym systemie. Całkowita suma iloczynów wag oraz interakcji wynosi 76. Z analizy tabeli widać, że mocne strony takie jak m.in. integralność danych, proste transakcje, dane indeksowane, czas reakcji i dostępność mogą wyeliminować zagrożenia takie jak błąd ludzki czy podatność na atak.

Tabela 5.85 pokazuje relacje pomiędzy słabymi stronami i szansami, które wzajemnie na siebie oddziałują. Łącznie uzyskano 21 interakcji, co stanowi 70% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 154. Z analizy tabeli można wyciągnąć wniosek, że słabe strony mogą ograniczać możliwości technologii takie jak np. zwiększenie świadomości sytu-

acyjnej zagrożeń, umiejętność klasyfikacji zagrożeń, możliwość gromadzenia dużych ilości danych i szybki dostęp do danych z dowolnego miejsca.

Tabela 5.86 pokazuje zależności pomiędzy słabymi stronami a wysoce interaktywnymi zagrożeniami. Suma interakcji wyniosła 17, co stanowi 85% maksymalnej liczby interakcji, jaka może wystąpić w testowanym systemie. Całkowita iloczynów wag oraz interakcji wynosi 134. Z analizy tabeli można wywnioskować, że słabe strony wpływają na możliwość wystąpienia zagrożeń, takich jak utrata danych, narażenie na ataki, błąd ludzki i awaria infrastruktury energetycznej.

Następnie za pomocą pytań przewodnich (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.87 pokazuje relacje pomiędzy szansami i mocnymi stronami, które są wysoce interaktywne. Suma interakcji wyniosła 48, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. iloczynów wag oraz interakcji wynosi 452. Na podstawie analizy tabeli można stwierdzić, że mocne strony technologii OLTP dają szansę na usprawnienie całego zarządzania kryzysowego.

W tabeli 5.88 przedstawiono zależności pomiędzy zagrożeniami oraz mocnymi stronami, między którymi występuje interakcja. W przebadanym układzie uzyskano sumę interakcji równą 7, co stanowi 25% maksymalnej liczby interakcji, które mogą wystąpić. Łączna suma iloczynów wag oraz interakcji wynosi 63. Z analizy tabeli można wywnioskować, że błąd ludzki może ograniczyć możliwości mocnych stron.

W tabeli 5.89 przedstawiono zależności pomiędzy szansami oraz słabymi stronami, między którymi występuje bardzo silna interakcja. Na tej podstawie uzyskano sumę interakcji wynoszącą 18, co stanowi 60% maksymalnej liczby interakcji, jaka może wystąpić. Całkowita suma iloczynów wag oraz interakcji wynosi 124. Z analizy tabeli można wywnioskować, że szanse wpływają na słabe strony technologii, takie jak kopie zapasowe, zapytania SQL, zależność personelu i koszty wdrożenia.

Tabela 5.90 pokazuje zależności pomiędzy zagrożeniami i słabymi stronami, które wzajemnie na siebie oddziałują. Suma interakcji wyniosła 10, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić. Łączna iloczynów wag oraz interakcji wynosi 84. Na tej podstawie można stwierdzić, że zagrożenia wpływają na słabe strony, takie jak podatność na awarie zapytań SQL, zależność od personelu i koszty wdrożenia.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.17). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab. 5.17)

Tabela 5.17. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów
Mocne strony/Szanse	96	892
Mocne strony/Zagrożenia	16	139
Słabe strony/Szanse	39	278
Słabe strony/Zagrożenia	27	218

Źródło: opracowanie własne

Z analizy tabeli 5.17 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabe strony mogą ograniczać wspomniane szanse, ale także stwarzać zagrożenia. Istnieje jednak możliwość wyeliminowania zidentyfikowanych słabych stron i zagrożeń, dzięki czemu technologia OLTP może stać się potężnym narzędziem, które można wykorzystać w zarządzaniu kryzysowym.

5.3.9. Funkcjonalność Business Inteligence (BI)

Systemy Business Intelligence (BI) są rozwinięciem systemów OLAP poprzez wykorzystanie bardzo ważnych mechanizmów odkrywania wiedzy (*DM/Data Mining*) na bazie zagregowanych danych w funkcji czasu. Odnosi się do technologii i infrastruktury danych analitycznych i obejmuje kilka powiązanych technologii i procesów, w tym[340]:

- eksplorację danych,
- analizę procesów,
- analizę porównawczą wydajności,
- analitykę opisową.

W większości przypadków odnosi się to do skrócenia ram czasowych tak, aby dane były przydatne dla decydenta, gdy przychodzi czas na podjęcie decyzji[341]. We wszystkich przypadkach stosowanie *BI* jest uważane za proaktywne. Niezbędnymi elementami proaktywnego zachowania *BI* są[342]:

- duże objętościowo hurtownie danych dostępne w czasie rzeczywistym,
- eksploracja hurtowni danych (analiza dużej ilości danych może statystycznie bardziej obiektywizować ocenę niż szczegółowość małej kolekcji danych),

[340] https://www.investopedia.com/ask/answers/041415/what-are-some-common-functions-business-intelligence-technologies.asp (data dostępu 08.11.2022).
[341] Tamże.
[342] J. Langseth, N. Vivatrat, *Why Proactive Business Intelligence is a Hallmark of the Real-Time Enterprise: Outward Bound*," Intelligent Enterprise, (5)18, 2003 s. 34-41.

- automatyczne wykrywanie skupień szeregów czasowych, anomalii i wyjątków,
- proaktywne alarmowanie z automatycznym określaniem odbiorców,
- płynny przepływ między równymi poziomami agregacji danych,
- automatyczne uczenie się i udoskonalanie,
- wizualizacja danych z wykorzystaniem atrybutów geoprzestrzennych.

Business Intelligence reprezentuje zbiór narzędzi informatycznych wykorzystywanych do gromadzenia i analizowania danych zorientowanych na możliwość usprawniania procesów planistyczno-prognostycznych, co może potwierdzać ich szczególną rolę w SZK we wspomaganiu procesów podejmowania decyzji[343].

W tabeli 5.18 dokonano Analizy SWOT dla technologii *Business Inteligence.*

Tabela 5.18. Analiza SWOT dla technologii *Business Inteligence*

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	Ułatwienie podejmowania decyzji	5	W1	Koszt wdrożenia	5
S2	Wgląd w kluczowe informacje	5	W2	Wysokie wymagania sprzętowe	5
S3	Dodatkowa baza danych	5	W3	Wymaga stałego nadzoru	4
S4	Raporty	5	W4	Zależność od sieci energetycznej lub Internetu	5
S5	Łatwa lokalizacja punktów newralgicznych	5	W5	Koszt szkoleń pracowników	5
S6	Aktualność danych	5			
S7	Prosty interfejs oprogramowania	5			
S8	Relatywnie krótki czas odpowiedzi na zapytania	5			
	Suma wag:	**40**		**Suma wag:**	**24**
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	Zwiększenie świadomości sytuacyjnej na temat zagrożeń	5	T1	Podatność na ataki	5
O2	Opracowanie raportów na temat stanów przyszłych	5	T2	Błąd ludzki	3
O3	Dostęp do danych	3	T3	Utrata danych	3
O4	Wizualizacja danych	5	T4	Podatność na awarie systemu	5
O5	Cyfryzacja	5			
O6	Usprawniony proces zarządzania kryzysowego	5			
	Suma wag:	**18**		**Suma wag:**	**16**

Źródło: opracowanie własne

Określenie mocnych i słabych stron oraz szans i zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu sformułowano następujące pytania:

1) W perspektywie SWOT:

- Czy mocne strony *Business Inteligence* mogą wykorzystać szanse? (tab. 5.91 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*),
- Czy mocna strona *Business Inteligence* przeważają nad zagrożeniami? (tab. 5.92 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence),*

[343] S. Bartosiewicz *IT and telematic systems in Polish logistics centres,* Przedsiębiorczość i Zarządzanie Wydawnictwo SAN, Tom XIV, Zeszyt 7, 2013, s. 85-86.

- Czy słaba strona *Business Inteligence* ogranicza wykorzystanie szansy? (tab. 5.93 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*),
- Czy słaba strona *Business Inteligence* może mieć wpływ na zagrożenia? (tab. 5.94 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*).

2) W perspektywie TOWS:

- Czy szanse *Business Inteligence* wpływają na mocne strony? (tab. 5.95 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*),
- Czy zagrożenia *Business Inteligence* wpływają na mocne strony ? (tab. 5.96 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*),
- Czy szanse *Business Inteligence* wpływa na słabe strony? (tab. 5.97 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*),
- Czy zagrożenia *Business Inteligence* wpływają na słabe strony? (tab. 5.98 – Załącznik nr 5: Analiza SWOT/TOWS *Business Inteligence*).

Tabela 5.91 przedstawia zależności pomiędzy mocnymi stronami i szansami, miedzy którymi występuje bardzo silna interakcja, co pokazuje przydatność Business Intelligence w budowaniu świadomości na temat zagrożeń i w skutecznym zarządzaniu kryzysowym. Suma interakcji wyniosła 48, co stanowi 100% maksymalnej liczby interakcji, jaka może. Suma iloczynów wag oraz interakcji wynosi 464, co oznacza, że wskazane mocne strony pozwalają wykorzystać potencjał Business Intelligence.

Tabela 5.92 przedstawia interakcje pomiędzy mocnymi stronami i zagrożeniami. Suma interakcji wyniosła 7, co stanowi 16% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 66, co oznacza, że mocne strony mogą eliminować zagrożenia, takie jak podatność na atak, błąd ludzki i utrata danych.

Tabela 5.93 przedstawia zależności pomiędzy słabymi stronami i szansami. Suma interakcji wyniosła 19, co stanowi 63% maksymalnej liczby interakcji, jaka może wystąpić w testowanym układzie. Suma iloczynów wag oraz interakcji wynosi 178. Słabe strony mogą chwilowo ograniczyć możliwości i potencjał Business Intelligence, ponieważ wraz z wprowadzeniem technologii wzrasta wiedza na jej temat, co ostatecznie prowadzi do eliminacji zidentyfikowanych słabości, takie jak koszty wdrożenia, wysokie wymagania sprzętowe, ciągły monitoring, zależność od sieci energetycznej lub Internetu oraz koszty szkoleń pracowników.

Tabela 5.94 pokazuje zależności pomiędzy słabymi stronami i zagrożeniami. Suma interakcji wyniosła 17, co stanowi 85% maksymalnej liczby interakcji, jaka może

wystąpić. Suma iloczynów wag oraz interakcji wynosi149. Z analizy tabeli można wyciągnąć wniosek, że słabe strony mogą stwarzać zagrożenia takie jak podatność na ataki, błędy ludzkie, utratę danych oraz podatność na awarie systemów.

Następnie za pomocą pytań przewodnich (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.95 przedstawia związki pomiędzy szansami, a mocnymi stronami. Suma interakcji wyniosła 48, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 528.Na podstawie analizy tabeli można stwierdzić, że szanse wpływają na mocne strony, co wskazuje na ogromny potencjał technologii.

Tabela 5.96 przedstawia zależności pomiędzy zagrożeniami i mocnymi stronami. Łącznie uzyskano 5 interakcji, co stanowi 16% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Całkowita suma iloczynów wag oraz interakcji wynosi 62. Z analizy tabeli można wywnioskować, że zagrożenia takie jak takie jak wgląd w kluczowe informacje oraz łatwa lokalizacja punktów newralgicznych mogą mieć wpływ na mocne strony technologii.

Tabela 5.97 pokazuje zależności pomiędzy szansami i słabymi stronami, które są ze sobą powiązane. Suma interakcji wyniosła 30, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 254. Na tej podstawie można stwierdzić, że szanse wpływają na słabych stron technologii

Tabela 5.98 przedstawia zależności pomiędzy zagrożeniami i słabymi stronami. Suma interakcji wyniosła 8, co stanowi 40% maksymalnej możliwej liczby interakcji, które mogą wystąpić. Suma iloczynów wag oraz interakcji wynosi 61. Z analizy tabeli można stwierdzić, że zagrożenia wpływają na słabe strony technologii.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.19). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab. 5.19)

Tabela 5.19. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów
Mocne strony/Szanse	96	992
Mocne strony/Zagrożenia	12	128
Słabe strony/Szanse	49	432
Słabe strony/Zagrożenia	25	210

Źródło: opracowanie własne

Z analizy tabeli 5.19 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabe strony mogą ograniczać wspomniane szanse, ale także stwarzać zagrożenia. Niemniej jednak wskazane słabe strony i zagrożenia można usunąć, dzięki czemu technologia BI może stać się skutecznym narzędziem, które można wykorzystać w planowaniu i prognozowaniu procesów, a tym samym kreowaniu trzeciego poziomu świadomości sytuacyjnej, zwłaszcza dla decydentów i osób funkcyjnych w ZZK a tym samym w procesie zarządzania kryzysowego.

5.3.10. Funkcjonalność technologii Big Data

Big Data to operowanie dużymi zbiorami wielopostaciowych danych wykorzystywane do analizy przeszłości i teraźniejszości w celu przewidywania przyszłości. *Big Data* bardzo dobrze charakteryzuje symbol 5V, gdzie kolejne litery V oznaczają odpowiednie atrybuty: [344]:

- *volume* – objętość,
- *velocity* – duża szybkość narastania,
- *variety* – różnorodność struktury i treści,
- *veracity* – wiarygodność i dokładność,
- *value* – wartość , dzięki czemu wszelkie dane są łatwo przetwarzane.

Przetwarzane są zarówno dane, które są ustrukturyzowane, jak i te nieustrukturyzowane, co nie odbywa się przy użyciu tradycyjnych metod przetwarzania danych. Technologie *Big Data* to narzędzia programowe służące do zarządzania wszystkimi typami zbiorów danych i przekształcania ich w informacje. W tej technologii można wyodrębnić cztery główne typy funkcji[345]:

- przechowywanie danych – pobieranie, przechowywanie oraz zarządzanie dużą ilością danych,
- eksploracja danych – przekształcanie nieustrukturyzowanych, ustrukturyzowanych lub częściowo ustrukturyzowanych danych w użyteczne informacje,
- analiza danych – czyszczenie i przekształcanie danych w informacje, które można wykorzystać do podejmowania decyzji biznesowych
- wizualizacja danych – przedstawianie danych za pomocą schematów, wykresów itp.

---

[344] M. Jurek, M. Staruch, *Potencjał wykorzystania technologii 5G i big data w kreowaniu świadomości sytuacyjnej w aspekcie ochrony danych osobowych,* Ochrona danych osobowych. Perspektywa krajowa i międzynarodowa, red. K. Śmiałek, A. Kominek, Wydawnictwo Naukowe FNCE, Poznań 2021.
[345] https://doit.software/blog/big-data-technologies (data dostępu 7.11.2022).

W tabeli 5.20 przedstawiono syntetyczne wyniki Analizy SWOT dla technologii *Big Data*.

Tabela 5.20. Analiza SWOT *Big Data*

MOCNE STRONY (STRENGHTS)		WAGA	SŁABE STRONY (WEAKNESSES)		WAGA
S1	duża dostępność danych	5	W1	wymaga szkolenia personelu	5
S2	różnorodność danych	5	W2	niska jakość danych	5
S3	Szybkość przetwarzania bardzo dużych baz danych	5	W3	koszty urządzeń wspomagających	4
S4	szczegółowość danych	5	W4	zależność od technologii	5
S5	zbieranie danych	5	W5	niekompletne wyniki	5
S6	gromadzenie danych	5			
	Suma wag:	30		Suma wag:	24
SZANSE (OPPORTUNITIES)		**WAGA**	**ZAGROŻENIA (THREATS)**		**WAGA**
O1	przetwarzanie danych	5	T1	niewłaściwe wykorzystanie danych	5
O2	zwiększenie poziomu świadomości sytuacyjnej	5	T2	podatność na ataki	3
O3	dostępność	5	T3	zależność od dostępu do Internetu lub sieci energetycznej	3
			T4	nieznajomość technologii	5

Źródło: opracowanie własne

Określenie mocnych stron, słabych stron, szans oraz zagrożeń pozwoliło na utworzenie interakcji dla poszczególnych par czynników. Identyfikacja interakcji SWOT-TOWS przeprowadzona została z wykorzystaniem ośmiu tabel, będących wynikiem zestawienia dwóch czynników. W tym celu zastosowano pomocniczo następujące pytania:

1) W perspektywie SWOT:

- Czy mocne strony *Big Data* mogą wykorzystać szanse? (tab. 5.99 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*),
- Czy mocne strony *Big Data* przeważają nad zagrożeniami? (tab. 5.100 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data),*
- Czy słaba strona *Big Data* ogranicza wykorzystanie szansy? (tab. 5.101 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*),
- Czy słaba strona *Big Data* może mieć wpływ na zagrożenia? (tab. 5.102 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*).

2) W perspektywie TOWS:

- Czy szanse *Big Data* wpływają na mocne strony? (tab. 5.103 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*),
- Czy zagrożenia *Big Data* wpływają na mocne strony ? (tab. 5.104 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*),
- Czy szanse *Big Data* wpływa na słabe strony? (tab. 5.105 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*),
- Czy zagrożenia *Big Data* wpływają na słabe strony? (tab.5.106 – Załącznik nr 5: Analiza SWOT/TOWS *Big Data*).

Tabela 5.99 przedstawia wyniki interakcji pomiędzy mocnymi stronami i szansami. Suma interakcji wyniosła 18, co stanowi 100% maksymalnej liczby interakcji, jaka może wystąpić. Całkowita suma iloczynów wag oraz interakcji wynosi180. Maksymalna liczba interakcji między mocnymi stronami i szansami jest ważnym argumentem za przyjęciem tej technologii, której zastosowanie może przyczynić się do wzrostu świadomości sytuacyjnej na temat zagrożeń i poprawy . całego procesu zarządzania kryzysowego – usprawnić pracę służb ratowniczych i proces identyfikacji zagrożeń.

Tabela 5.100 przedstawia zależności pomiędzy mocnymi stronami i zagrożeniami. Suma interakcji wyniosła 13, co stanowi 54% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi114. Na podstawie uzyskanych wyników widać, że mocne strony są w stanie wyeliminować zagrożenia takie jak niewłaściwe wykorzystanie danych, podatność na ataki oraz uzależnienie od dostępności internetu czy sieci energetycznej.

Tabela 5.101 przedstawia zależności pomiędzy szansami i słabymi stronami. Suma interakcji wyniosła 8, co stanowi 53% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 78. Można zatem wyciągnąć wniosek, że słabe strony mogą ograniczać wykorzystanie szans, jak przetwarzanie danych oraz zwiększenie poziomu świadomości sytuacyjnej.

Tabela 5.102 przedstawia związek pomiędzy słabymi stronami i zagrożeniami mała liczba interakcji wskazuje na przydatność technologii big data w budowaniu świadomości zagrożeń i skutecznym zarządzaniu kryzysowym. Suma interakcji wyniosła 9, co stanowi 25% maksymalnej liczby interakcji, jaka może wystąpić w testowanym systemie. Suma iloczynów wag oraz interakcji wynosi 85. Na tej podstawie można stwierdzić, że słabe strony technologii mogą przyczyniać się do wystąpienia zagrożeń takich jak niewłaściwe wykorzystanie danych, podatność na ataki, uzależnienie od Internetu czy sieci elektrycznej. i nieznajomość technologii.

Następnie za pomocą pytań przewodnich (analiza TOWS) przeanalizowano interakcje pomiędzy zagrożeniami, szansami, słabymi i mocnymi stronami.

Tabela 5.103 przedstawia zależności między szansami i mocnymi stronami. Suma interakcji wyniosła 18, co stanowi 100% maksymalnej liczby interakcji, jaka może. Suma iloczynów wag oraz interakcji wynosi 220. Z analizy tabeli można wywnioskować, że mocne strony wpływają na szanse, co wskazuje na ogromny potencjał technologii.

Tabela 5.104 przedstawia zależności pomiędzy zagrożeniami i mocnymi stronami, które na siebie oddziałują. Suma interakcji wyniosła 12, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 128. Z analizy tabeli można wyciągnąć wniosek, że niewłaściwe wykorzystanie danych i narażenie na ataki mogą mieć wpływ na mocne strony technologii.

Tabela 5.105 pokazuje związek pomiędzy szansami i słabymi stronami. Suma interakcji wyniosła 6, co stanowi 33% maksymalnej liczby interakcji, jaka może wystąpić w badanym systemie. Łączna suma iloczynów wag oraz interakcji wynosi 59. Z analizy tabeli można stwierdzić, że na szanse wpływają słabe strony, takie jak zapotrzebowanie na personel, niska jakość danych, koszty urządzeń wspomagających oraz zależność od technologii.

Tabela 5.106 przedstawia zależności pomiędzy zagrożeniami i słabymi stronami. Suma interakcji wyniosła 10, co stanowi 50% maksymalnej liczby interakcji, jaka może wystąpić. Suma iloczynów wag oraz interakcji wynosi 90. Z analizy tabeli można wyciągnąć wniosek, że zagrożenia wynikają ze słabych stron, takich jak niska jakość danych, błędne wyniki ze względu na niewłaściwe przeszkolenie personelu.

Następnie zestawiono sumę interakcji pomiędzy przebadanymi układami (tab. 5.21). Określono zatem ile interakcji zachodzi i jaka jest suma iloczynów ich wag. W tym celu zsumowane zostały wyniki kombinacji czynników wewnętrznych i zewnętrznych z analizy SWOT/TOWS (tab. 5.21).

Tabela 5.21. Zestawienie interakcji

Interakcje	Suma interakcji	Suma iloczynów
Mocne strony/Szanse	36	400
Mocne strony/Zagrożenia	25	242
Słabe strony/Szanse	14	137
Słabe strony/Zagrożenia	19	175

Źródło: opracowanie własne

Z analizy tabeli 5.21 wynika, że przeważają mocne strony i szanse, warto jednak zwrócić uwagę na fakt, że słabe strony mogą ograniczać wspomniane szanse, ale także stwarzać zagrożenia. Przedstawione słabe strony i zagrożenia można jednak wyeliminować, dzięki czemu technologia Big Data może stać się potężnym narzędziem, które można wykorzystać w zarządzaniu kryzysowym.

5.4. Potrzeby i stan wyposażenia technologicznego służb RP w zakresie informowania ludności w sytuacjach kryzysowych

Zespoły zarządzania kryzysowego muszą koordynować, ujednolicać działania ratownicze i podejmować odpowiednie decyzje w celu zminimalizowania skutków zagrożenia. Technologie sztucznej inteligencji, *IoT* i *Blockchain* mogą stanowić pod-

stawę doskonalenia istniejących rozwiązań i sprzyjać podnoszeniu świadomości sytuacyjnej ludności poprzez agregację i analizę danych z heterogenicznych źródeł takie, jak[346]:

- zdjęcia dronów i satelitów,
- monitoring infrastruktury *IoT*,
- *chatboty* oparte na sztucznej inteligencji,
- zasoby z Numer 112,
- media społecznościowe.

Wszystkie te informacje mogą pomóc zespołom zidentyfikować pilne potrzeby, ustalić priorytety odpowiedzi i uniknąć niepotrzebnej pracy, ale tylko wtedy, gdy można je zidentyfikować. Dzięki zastosowaniu współczesnych technologii IT/ICT można przewidzieć rozwój sytuacji i w ten sposób zniwelować lub zmniejszyć jej skutki znacznie szybciej. W przypadku wystąpienia nieprzewidywalnych zagrożeń, np. klęsk żywiołowych osoby zaangażowane w taki proces mogą uzyskać dostęp do danych w czasie rzeczywistym, których analiza może wesprzeć szybkie procesy decyzyjne. Dlatego też istotne jest wdrożenie ogólnokrajowego systemu informatycznego, który będzie wykorzystywał funkcjonalność istniejących rozwiązań, a stopniowo będzie rozszerzany o nowe funkcje.

Klęski żywiołowe mogą wywołać przerwy w funkcjonowaniu danego systemu, np. poprzez utratę zasilania lub ataki cybernetyczne, dlatego też istotne jest posiadanie alternatywnych rozwiązań na wypadek zawodności systemu opartego na współczesnych technologiach. Między współczesnymi technologiami IT/ICT, a tradycyjnymi rozwiązaniami istnieje silne powiązanie. Obie te technologie mogą przyczynić się do poprawy świadomości sytuacyjnej ludności. Do weryfikacji tych konkluzji sformułowano hipotezę H.4: **Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów** oraz hipotezę H.5.: **Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świa-**

[346] G. Pokorski, P. Zaskórski, *Systemy informacji geoprzestrzennej w zarządzaniu procesami biznesowym,* Nowoczesne Systemy Zarządzania, Zeszyt 13, nr 2, Wojskowa Akademia Techniczna, 2018, s. 107-128.

domości sytuacyjnej ludności występuje silna dodatnia korelacja. Do weryfikacji ww. hipotez posłużyły pytania skierowano do zespołów SZK oraz obywateli.

Podstawą weryfikacji hipotezy H.4 są odpowiedzi na pytania, w których oceniono, które współczesne technologie teleinformatyczne IT/ICT są ważne w procesie kształtowania pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów (wyk. 5.1) oraz oceniono funkcje tradycyjnych form komunikowania się i poziomu ich przydatności w kształtowaniu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów (wyk. 5.2). Badanie przeprowadzone zostało na próbie 112 respondentów.

Wykres 5.1. Ocena przydatności współczesnych technologii IT/ICT w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów (N=112)
Źródło opracowanie własne

W celu oceny przydatności współczesnych technologii IT/ICT poproszono ankietowanych o wskazanie przydatnych technologii w procesie kształtowania pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów. W tym celu sformułowano następujące pytania:

1. *Wykorzystanie portali społecznościowych w celu zwiększenia poziomu świadomości o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 16 osób (14%) oceniło portale społecznościowe jako przydatne w procesie zwiększenia poziomu świadomości o zagrożeniach, a 96 osób (84%) uważa tego typu rozwiązanie za nieprzydatne.

2. *Przesyłanie podglądu na żywo z miejsca wystąpienia zagrożenia za pomocą urządzeń naziemnych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 15 osób (14%) oceniło podgląd na żywo z miejsc wystąpienia zagrożenia jako przydatny, a 97 osób (86%) uważa tego typu rozwiązanie za nieprzydatne.

3. *Dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 9 osób (8%) oceniło dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych jako przydatne, a 103 osoby (92%) uważają tego typu rozwiązanie za nieprzydatne.

4. *Analiza obecnej sytuacji*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 37 osób (30%) oceniło narzędzia do analizy aktualnej sytuacji jako przydatne, a 75 osób (70%) uważa tego typu rozwiązanie za nieprzydatne.

5. *Prognozowanie przyszłych zagrożeń*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 37 osób (30%) oceniło narzędzia do prognozowania przyszłych zagrożeń jako przydatne, a 75 osób (70%) uważa tego typu rozwiązanie za nieprzydatne.

6. *Porównywanie zagrożeń*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 20 osób (18%) oceniło narzędzia do porównywania jako przydatne, a, 92 osoby (82%) uważają tego typu rozwiązanie za nieprzydatne.

7. *Tworzenie statystycznych modeli przyszłych zagrożeń na podstawie danych historycznych*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 7 osób (6%) oceniło tworzenie modeli statystycznych przyszłych za-

grożeń jako przydatne, a 105 osób (94%) uważa tego typu rozwiązanie za nieprzydatne.

8. Symulowanie zagrożeń

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 37 osób (30%) oceniło symulowanie zagrożeń jako przydatne, a 75 osób (70%) uważa tego typu rozwiązanie za nieprzydatne.

9. Zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 18 osób (17%) oceniło zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania jako przydatne, a 94 osoby (83%) uważa tego typu rozwiązanie za nieprzydatne.

10. Dokumentowanie zagrożeń w formie elektronicznej

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 19 osób (15%) oceniło dokumentowanie zagrożeń w formie elektronicznej jako przydatne, a 93 osoby (85%) uważają tego typu rozwiązanie za nieprzydatne.

11. Odbieranie wiadomości o zagrożeniach

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 39 osób (35%) oceniło odbieranie wiadomości o zagrożeniach jako przydatne, a 73 osoby (65%) uważają tego typu rozwiązanie za nieprzydatne.

12. Przesyłanie wiadomości o zagrożeniach

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 60 osób (54%) oceniło przesyłanie wiadomości o zagrożeniach jako przydatne, a 52 osoby (46%) uważają tego typu rozwiązanie za nieprzydatne.

13. informowanie o zagrożeniach

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 59 osób (53%) oceniło przesyłanie wiadomości o zagrożeniach jako przydatne, a 53 osoby (47%) uważają tego typu rozwiązanie za nieprzydatne.

14. Monitorowanie

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 53 osoby (47%) oceniło monitorowanie jako przydatne, a 59 osób (53%) uważa tego typu rozwiązanie za nieprzydatne.

15. Lokalizacja

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112

ankietowanych 52 osoby (46%) oceniło lokalizowanie jako przydatne, a 60 osób (54%) uważa tego typu rozwiązanie za nieprzydatne. Analiza odpowiedzi pozwoliła ocenić przydatność zaproponowanych w badaniu współczesnych technologii IT/ICT. Spośród wskazanych odpowiedzi trudno jednoznacznie wskazać najbardziej użyteczną technologię, niemniej jednak na uwagę zasługuje skuteczny proces przekazywania, odbierania i informowania o zagrożeniu.

Otrzymane wyniki pokazują, że potencjał współczesnych technologii nie został w pełni wykorzystany, a możliwości jego wykorzystania nie są znane respondentom.

Następnie została wyliczona średnia ocenia ze wszystkich odpowiedzi, która wynosi 3,71 (tab. 5.22), co w 5 – stopniowej skali jest względnie wysoką oceną (to już nie wiem, co ta ocena ma oznaczać).

Tabela 5.22. Średnie oceny respondentów dla czynników z oceną przydatności współczesnych technologii IT/ICT w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów

Lp.	Odpowiedź	Średnia arytmetyczna (ocena)
1.	Wykorzystanie portali społecznościowych w celu zwiększenia poziomu świadomości o zagrożeniach	4,21
2.	Przesyłanie podglądu na żywo z miejsca wystąpienia zagrożenia za pomocą urządzeń naziemnych	3,68
3.	Dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych	3,87
4.	Analizowanie obecnej sytuacji	4,00
5.	Prognozowanie przyszłych zagrożeń	3,48
6.	Porównywanie zagrożeń	3,47
7.	Tworzenie modeli statycznych modeli przyszłych zagrożeń na podstawie danych historycznych	3,57
8.	Symulowanie zagrożeń	3,55
9.	Zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania	3,63
10.	Dokumentowanie zagrożeń w formie elektronicznej	3,57
11.	Odbieranie wiadomości o zagrożeniach	3,78
12.	Przesyłanie wiadomości o zagrożeniach	3,75
13.	Informowanie o zagrożeniach	4,00
14.	Monitorowanie	3,61
15.	Lokalizacja	3,56

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

Następnie analizie poddano tradycyjne formy komunikowania się w procesie kształtowania pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów (wyk. 5.2):

1. *Telefonia komórkowa*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 101 osób (90%) oceniło wykorzystanie telefonii komórkowej w zarządzaniu kryzysowym jako przydatne, a 11 osób (10%) uważa tego typu rozwiązanie za nieprzydatne.

2. *Telewizja*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 73 osoby (65%) oceniły wykorzystanie telewizji w zarządzaniu kryzy-

sowym jako przydatne, a 39 osób (35%) uważa tego typu rozwiązanie za nieprzydatne.

3. *Internet*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 90 osób (80%) oceniło wykorzystanie Internetu w zarządzaniu kryzysowym jako przydatne, a 22 osoby (20%) uważają tego typu rozwiązanie za nieprzydatne.

4. *Telefon stacjonarny*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że 112 (100%) ankietowanych uważa telefony stacjonarne jako nieprzydatne w zarządzaniu kryzysowym.

5. *Smartwatch*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 9 osób (7%) oceniło smartwatch jako przydatny w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 103 osoby (93%) uważa tego typu rozwiązanie za nieprzydatne.

6. *Media społecznościowe*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 73 osoby (65%) oceniają media społecznościowe jako przydatne w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 39 osób (35%) uważa tego typu rozwiązanie za nieprzydatne.

7. *Komunikatory*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 17 osób (15%) ocenia komunikatory jako przydatne w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 95 osób (85%) uważa tego typu rozwiązanie za nieprzydatne.

8. *Radio*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 59 osób (53%) ocenia radio jako przydatne w zarządzaniu kryzysowymi w procesie informowania ludności o zagrożeniach, a 53 osoby (47%) uważa tego typu rozwiązanie za nieprzydatne.

9. *Dron*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 6 osób (5%) ocenia drony jako przydatne w zarządzaniu kryzysowymi

w procesie informowania ludności o zagrożeniach, a 106 osób (95%) uważa tego typu rozwiązanie za nieprzydatne.

10. *Tablet*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 6 osób (5%) ocenia tablet jako przydatne urządzenie w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 106 osób (95%) uważa tego typu rozwiązanie za nieprzydatne.

11. *Megafon*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 22 osoby (20%) oceniają megafony jako przydatne w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 90 osób (80%) uważa tego typu rozwiązanie za nieprzydatne.

12. *Systemy alarmowe*

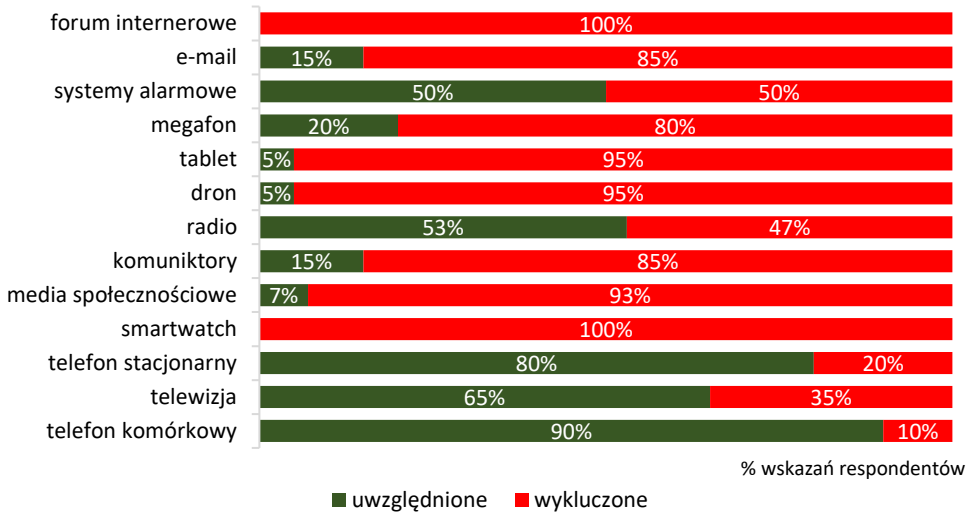
Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 56 osób (50%) ocenia systemy alarmowe jako przydatne w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 56 osób (50%) uważa tego typu rozwiązanie za nieprzydatne.

13. *E-mail*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 17 osób (15%) ocenia portale społecznościowe jako przydatne w zarządzaniu kryzysowym i w procesie informowania ludności o zagrożeniach, a 95 osób (85%) uważa tego typu rozwiązanie za nieprzydatne.

14. *Forum internetowe*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że 112 ankietowanych uważa forum internetowe jako nieprzydatne w zarządzaniu kryzysowymi w procesie informowania ludności o zagrożeniach.



Wykres 5.2. Ocena przydatności tradycyjnych form komunikowania się w procesie kształtowania pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów
Źródło opracowanie własne

Powyższe wyniki pokazują, że wśród respondentów są osoby preferujące tradycyjne rozwiązania co wynikać może z braku wiedzy na temat współczesnych technologii.

Analiza odpowiedzi pozwoliła ocenić przydatność zaproponowanych w badaniu tradycyjnych technologii. Wśród wskazanych odpowiedzi można zauważyć, że technologie takie, jak telefonia komórkowa, telewizja, Internet, media społecznościowe radio i syreny alarmowe, pomimo rozwoju współczesnych technologii, są nadal ważne i wciąż odgrywają użyteczną rolę w zarządzaniu kryzysowym oraz w procesie informowania ludności o zagrożeniach.

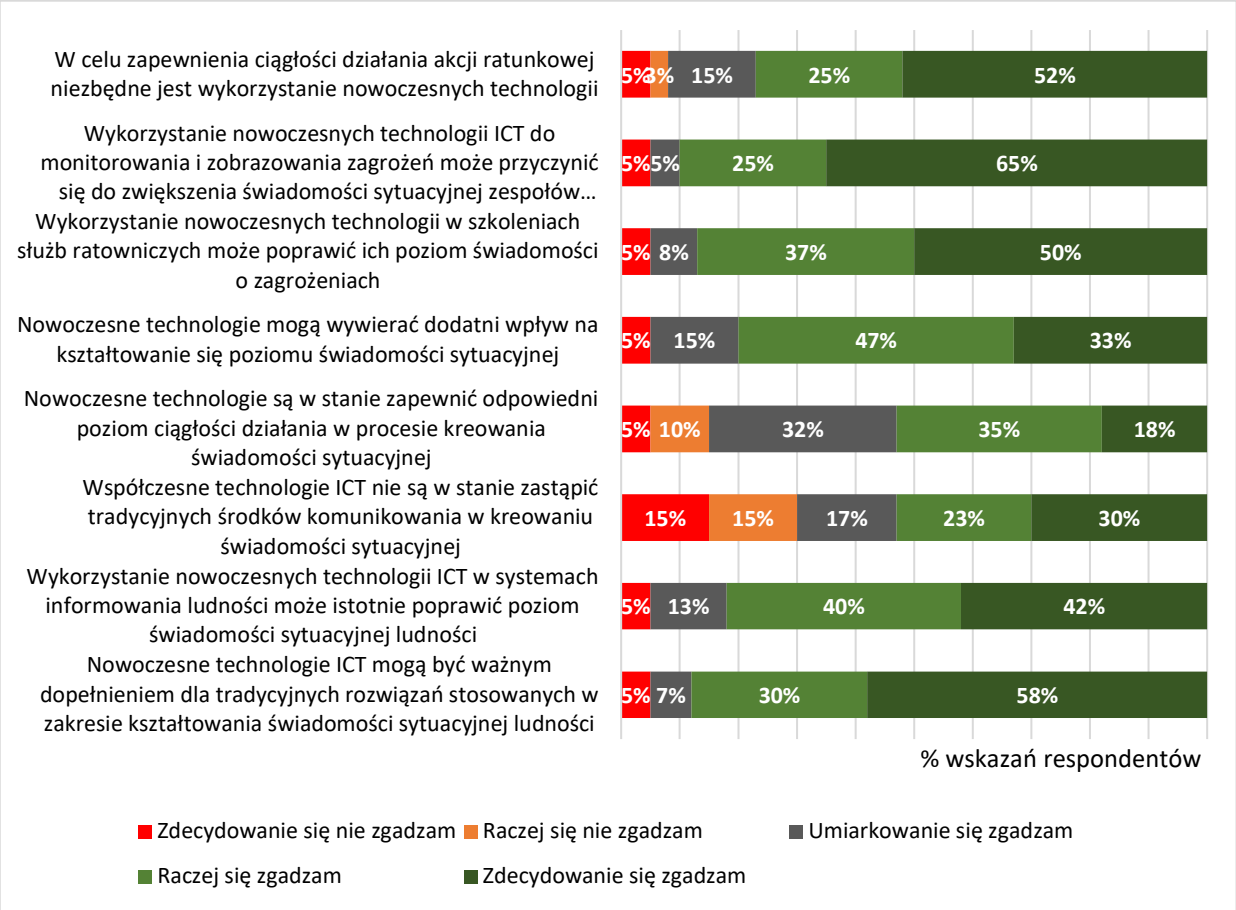
Współczesne technologie IT/ICT to przede wszystkim narzędzia sprzyjające obiektywizacji wiedzy nt. zagrożeń, ich prognozowanych skutków w różnych horyzontach czasowych wg wielowariantowych scenariuszy, czego nie zapewnią tradycyjne formy samego procesu przekazywania/obiegu informacji. Wartość informacji wyrażonej w komunikacie jest zaledwie uproszczoną treścią. Dochodzenie do tej treści i ocena jej wartości są determinowane zaawansowanymi technologiami. Stąd wydaje się, ze świadomość badanych respondentów nt. roli i zakresu oraz celu wykorzystania współczesnych technologii IT/ICT jest dość płytka. W autorskiej samoocenie oraz na podstawie studiów literaturowych uważa się, że te technologie mogą odgrywać kluczową rolę w procesie informowania ludności o zagrożeniach, a w szczególności w kreowaniu świadomości sytuacyjnej ludności w fazie ich postrzegania i rozumienia

i są coraz częściej wykorzystywana przez osoby młodszej generacji (poziom kultury informatycznej), co pokazują przeprowadzone badania. Ważny przy tym jest 3-ci poziom kształtowania świadomości sytuacyjnej związany z projekcją przyszłości, co jest szczególnie przydatne dla decydentów w SZK oraz osób funkcyjnych w ZZK. W zaprezentowanych wynikach można zauważyć, że wśród społeczeństwa zarówno wśród obywateli jak i członków ZZK są osoby, które preferują tradycyjne środki komunikacji lub częściowe wykorzystanie współczesnych technologii, co pokazuje, że te technologie powinny się nakładać i łączyć synergicznie swoje potencjały.

Weryfikacja hipotezy H.4. w brzmieniu: **Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów** przebiegła zatem pozytywnie, aczkolwiek wymagać to będzie dalszych bardziej precyzyjnych badań po cyklu szkoleniowym, podnoszącym kompetencje cyfrowe potencjalnej populacji respondentów (obywateli) w tym zakresie. Poniżej prezentowane badania na pracownikach ZZK (kompetentnych i odpowiedzialnych za monitorowanie sytuacji, przygotowanie odpowiednich analiz i prognoz do informowania ludności w SZK) są także potwierdzeniem prawdziwości hipotezy H4.

Podstawą weryfikacji hipotezy H.5 w brzmieniu: **Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja -** są odpowiedzi na pytania ankietowe skierowane do zespołów ZZK,w których ocenie został poddany stopień zgody ze stwierdzeniami zawartymi w badaniu ankietowym (wyk. 5.3). Badanie przeprowadzone zostało na próbie N=112.

Do oceny stopnia zgody ze stwierdzeniami zawartymi w pytaniu ankietowym przyjęto 5-cio stopniową skalę określającą stopień zgody z poszczególnym stwierdzeniami (1 – zdecydowanie się nie zgadzam, 2 – raczej się nie zgadzam, 3 – umiarkowanie się zgadzam, 4 – raczej się zgadzam, 5 – zdecydowanie się zgadzam). Ankietowani dokonali oceny poszczególnych stwierdzeń określając, w jakim stopniu się z nimi zgadzają:



Wykres 5.3. Ocena przydatności nowoczesnych technologii (N=112)

Źródło: opracowanie własne

1. *W celu zapewnienia ciągłości działania akcji ratunkowej niezbędne jest wykorzystanie nowoczesnych technologii*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 58 osób (52%) zdecydowanie się zgadza ze stwierdzeniem, że w celu zapewnienia ciągłości działania akcji ratunkowej niezbędne jest wykorzystanie nowoczesnych technologii, 28 osób (25%) raczej się zgadza, co pokazuje, że 77% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 23% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (17 osób), raczej się nie zgadzam (3 osoby) zdecydowanie się nie zgadzam (6 osób). Na tej podstawie można stwierdzić że niezbędne jest wykorzystanie nowoczesnych technologii w akcjach ratunkowych.

2. *Wykorzystanie nowoczesnych technologii ICT do monitorowania i zobrazowania zagrożeń może przyczynić się do zwiększenia świadomości sytuacyjnej zespołów zarządzania kryzysowego*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 73 osoby (65%) zdecydowanie się zgadzają ze stwierdzeniem, że wykorzystanie nowoczesnych technologii ICT do monitorowania i zobrazowania zagrożeń może przyczynić się do zwiększenia świadomości sytuacyjnej zespołów zarządzania kryzysowego, 29 osób (25%) raczej się zgadza, co pokazuje, że 90% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 10% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (5 osób), zdecydowanie się nie zgadzam (5 osób). Na tej podstawie można stwierdzić że niezbędne jest wykorzystanie nowoczesnych technologii ICT do monitorowania i zobrazowania zagrożeń może przyczynić się do zwiększenia świadomości sytuacyjnej zespołów zarządzania kryzysowego.

3. *Wykorzystanie nowoczesnych technologii w szkoleniach służb ratowniczych może poprawić ich poziom świadomości o zagrożeniach*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 56 osób (50%) zdecydowanie się zgadza ze stwierdzeniem, że wykorzystanie nowoczesnych technologii w szkoleniach służb ratowniczych może poprawić ich poziom świadomości o zagrożeniach, 41 osób (37%) raczej się zgadza, co pokazuje, że 87% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 13% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (9 osób), zdecydowanie się nie zgadzam (6 osób). Na tej podstawie można stwierdzić że niezbędne jest wykorzystanie nowoczesnych technologii w szkoleniach służb ratowniczych może poprawić ich poziom świadomości o zagrożeniach.

4. *Nowoczesne technologie mogą wywierać dodatni wpływ na kształtowanie się poziomu świadomości sytuacyjnej*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 37 osób (33%) zdecydowanie się zgadza ze stwierdzeniem, że nowoczesne technologie mogą wywierać dodatni wpływ na kształtowanie się poziomu świadomości sytuacyjnej, 54 osoby (47%) raczej się zgadza, co pokazuje, że 80% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 20% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (17 osób), zdecydowanie się nie zgadzam (4 osoby). Na tej podstawie można stwierdzić

że nowoczesne technologie mogą wywierać dodatni wpływ na kształtowanie się poziomu świadomości sytuacyjnej.

5. *Nowoczesne technologie są w stanie zapewnić odpowiedni poziom ciągłości działania w procesie kreowania świadomości sytuacyjnej*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 20 osób (18%) zdecydowanie się zgadza ze stwierdzeniem, że nowoczesne technologie są w stanie zapewnić odpowiedni poziom ciągłości działania w procesie kreowania świadomości sytuacyjnej, 39 osób (35%) raczej się zgadza, co pokazuje, że 53% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 47% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (36 osób), raczej się nie zgadza (11 osób), zdecydowanie się nie zgadzam (6 osób). Na tej podstawie nie można jednoznacznie ocenić przydatności wspomnianego rozwiązania, ponieważ zdania na ten temat są podzielone co pokazuje prócz nowoczesnych technologii niezbędne jest zastosowanie również innych rozwiązań.

6. *Współczesne technologie ICT nie są w stanie zastąpić tradycyjnych środków komunikowania w kreowaniu świadomości sytuacyjnej*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 34 osoby (30%) zdecydowanie się zgadza ze stwierdzeniem, że współczesne technologie ICT nie są w stanie zastąpić tradycyjnych środków komunikowania w kreowaniu świadomości sytuacyjnej, 26 osób (23%) raczej się zgadza, co pokazuje, że 53% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 47% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (18 osób), raczej się nie zgadza (17 osób), zdecydowanie się nie zgadzam (17 osób). Na tej podstawie nie można jednoznacznie ocenić przydatności wspomnianego rozwiązania, ponieważ zdania na ten temat są podzielone co pokazuje, że wśród ankietowanych są osoby które preferują zarówno współczesne jak i tradycyjne rozwiązania co oznacza, że współczesne technologie nie są w stanie zastąpić ich tradycyjnych odpowiedników.

7. *Wykorzystanie nowoczesnych technologii ICT w systemach informowania ludności może istotnie poprawić poziom świadomości sytuacyjnej ludności*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 47 osób (42%) zdecydowanie się zgadza ze stwierdzeniem, że wykorzy-

stanie nowoczesnych technologii ICT w systemach informowania ludności może istotnie poprawić poziom świadomości sytuacyjnej ludności, 45 osób (40%) raczej się zgadza, co pokazuje, że 82% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 18% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (14 osób), zdecydowanie się nie zgadzam (6 osób). Na tej podstawie można bardzo wysoko ocenić użyteczność nowoczesnych technologii ICT w procesie kreowania świadomości sytuacyjnej.

8. *Nowoczesne technologie ICT mogą być ważnym dopełnieniem tradycyjnych rozwiązań stosowanych w zakresie kształtowania świadomości sytuacyjnej ludności*

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że spośród 112 ankietowanych 65 osób (58%) zdecydowanie się zgadza ze stwierdzeniem, że wykorzystanie nowoczesnych technologii ICT w systemach informowania ludności może istotnie poprawić poziom świadomości sytuacyjnej ludności, 34 osoby (30%) raczej się zgadza, co pokazuje, że 88% uważa za przydatne wykorzystanie tego typu rozwiązania. Osoby, które oceniły przydatność tego typu rozwiązania na niskim poziomie zgody stanowią 12% ankietowanych, a ich odpowiedzi rozkładają się na stopień umiarkowanie się zgadzam (7 osób), zdecydowanie się nie zgadzam (6 osób). Na tej podstawie można bardzo wysoko ocenić użyteczność nowoczesnych technologii ICT, które stanowią doskonałe dopełnienie dla tradycyjnych rozwiązań w zakresie kreowania świadomości sytuacyjnej.

Analiza powyższych wyników pozwala stwierdzić, że współczesne technologie IT/ICT odgrywają dużą rolę w procesie kształtowania świadomości sytuacyjnej, niemniej jednak ich tradycyjne odpowiedniki są nadal wykorzystywane i dla wielu osób stanowią główne źródło informacji o zagrożeniach, co oznacza, że aktualnie obie technologie powinny funkcjonować w trybie dopełnieniowym.

W celu weryfikacji hipotezy H.5. obliczona została całkowita wyjaśniona wariancja, która posiada 3 składowe (tab. 5.23) co oznacza, że przyjmie postać średniej ważonej.

Tabela 5.23. Całkowita wyjaśniona wariancja

Składowa	Początkowe wartości własne			Sumy kwadratów ładunków po wyodrębnieniu			Sumy kwadratów ładunków po rotacji			
	Ogółem	% wariancji	% skumulowany	Ogółem	% wariancji	% skumulowany	Ogółem	% wariancji	% skumulowany	Waga
1	4,973	35,520	35,520	4,973	35,520	35,520	3,540	25,286	25,286	0,43 – W1
2	2,233	15,953	51,473	2,233	15,953	51,473	2,902	20,731	46,017	0,35 – W2
3	1,014	7,246	58,719	1,014	7,246	58,719	1,778	12,701	58,719	0,22 – W3
Metoda wyodrębniania czynników – głównych składowych.										

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

Następnie czynniki zostały przydzielone do składowych i zapisane w tabeli 5.24.

Tabela 5.24. Przydział czynników do składowych

Składowa	WAGI	Czynniki
1	0,43 (W1)	C4; C5; C9; C10; C11; C13; C14
2	0,35 (W2)	C2; C3; C6; C7; C8;
3	0,22 (W3)	C1; C12

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

Następnie obliczona została średnia ważona w tym celu zastosowano wzór (2.4).

Po przekształceniu wzoru (2.4) zgodnie z danymi zapisanymi w tabeli 5.24. przyjmuje on formułę:

$$ZICT^{347} = \frac{W1(C4+C5+C9+C10+C11+C13+C14)}{7} + \frac{(W1(C4+C5+C9+C10+C11+C13+C14)\ )}{5} + \frac{(W3(C1+C12)}{2} \quad (2.4)$$

Następnie wyliczona została Korelacja pomiędzy PŚSL[348], a ZICT (tab. 5.25)

Tabela 5.25. Korelacja pomiędzy PŚSL i ZICT

Korelacje		
		PŚSL
~~PŚSL~~	~~Korelacja Pearsona~~	~~1~~
	~~N~~	~~112~~
ZICT	Korelacja Pearsona	0,434**
	Istotność (dwustronna)	0,000
	N	112

Źródło: opracowanie własne przy wykorzystaniu PS IMAGO PRO

Z przeprowadzonych badań wynika, że pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja co pokazuje jednoznacznie, że współcześnie technologie oraz świadomość sytuacyjna stanowią nierozłączny element determinujący zarówno bezpieczeństwa państwa, jak i obywateli. W związku z tym faktem obie hipotezy zostały zweryfikowane pozytywnie.

5.5. Podsumowanie rozdziału piątego

Analiza aktualnego stanu Systemu Zarządzania Kryzysowego RP jednoznacznie pokazuje, że niezbędne jest wprowadzenie stosownych zmian w aktualnie funkcjonujących rozwiązaniach. Głównym krokiem w tym kierunku powinno być stwo-

[347] ZICT – złożoność procesu wykorzystania ICT w informowaniu ludności.
[348] PŚSL – poziom świadomości sytuacyjnej ludności.

rzenie ogólnopolskiego Systemu Zarządzania Kryzysowego, który łączyłby w sobie funkcjonalność poszczególnych podsystemów działających w ramach służb, które je wykorzystują. System ten powinien być wspierany przez współczesne technologie takie, jak *IoT*, *AI*, *VR*, AR, *Cloud Computing* oraz *Blockchain,* a w szczególności przez komercyjne aplikacje dla potrzeb zintegrowanego zarządzania procesami bieżącego monitorowania i oceny sytuacji oraz prognozowania działań podwyższających świadomość decydentów i obywateli o zagrożeniach. System taki powinien być wyposażony w funkcje usprawniające proces przekazywania informacji pomiędzy różnymi interesariuszami stosownie do realizowanego scenariusza przebiegu kryzysu. Jak wspomniano, kluczową rolę w tym procesie mogą odegrać współczesne technologie coraz częściej wykorzystywane również przez obywateli w życiu codziennym.

Wykorzystanie ICT zwiększa efektywność działań poprzez skuteczne i rzeczywiste połączenie w jedną sieć wszystkich rozproszonych ośrodków decyzyjnych, sił możliwych do użycia, sensorów i efektorów w celu stworzenia możliwości pozyskiwania kompletnej i komunikatywnej informacji o zagrożeniach, co determinuje pożądany stan wspólnej świadomości sytuacyjnej oraz zwiększenie szybkości podejmowania decyzji na wszystkich szczeblach zarządzania oraz tempa realizowanych akcji i operacji. Wykorzystanie ICT opiera się na założeniach: silnie powiązane elementy sieci zwiększają możliwość wymiany informacji, co z kolei wpływa na zwiększenie jej jakości i współdzielenie świadomości sytuacyjnej. Następstwem tego jest możliwość współpracy i wzajemnej koordynacji działań[349].

Współczesne technologie IT/ICT stanowią ważne wsparcie dla procesów kreowania świadomości sytuacyjnej. Technologie takie, jak Internet rzeczy, sztuczna inteligencja, *Blockchain*, systemy analityczno-decyzyjne, mogą przyczynić się do poprawy działania zespołów zarządzania kryzysowego i służb ratowniczych. Technologie te mogą eliminować błędy ludzkie w działaniu i operowaniu niepełną i nieaktualna informacja oraz wiedza. Bieżąca, wiarygodna (zweryfikowana przez wiele źródeł) informacja ma kluczowe znaczenie dla skutecznego przeciwdziałania sytuacji kryzysowej. Współczesne technologie IT/ICT stanowić mogą dopełnienie tradycyjnych środków komunikowania w procesach informowania ludności o zagrożeniach przy zapewnieniu powyższych atrybutów dla tak pozyskiwanych i weryfikowanych infor-

[349] https://www.coolfiresolutions.com/blog/5-situational-awareness-technologies/ (data dostępu 30.10.2021).

macji. Zarówno współczesne technologie, jak i tradycyjne środki informowania ludności o zagrożeniach służą poprawie poziomu świadomości sytuacyjnej w zakresie, o którym była mowa przy specyfikowaniu ich funkcjonalności i ocenie użyteczności. Oceny te zostaną wykorzystane przy formułowaniu założeń i ograniczeń do autorskiej koncepcji doskonalenia istniejącego sytemu z wykorzystaniem współczesnych platform IT/ICT .

ROZDZIAŁ VI
KONCEPCJA DOSKONALENIA SYSTEMU KREOWANIA ŚWIADOMOŚCI SYTUACYJNEJ LUDNOŚCI

6.1. Założenia i ograniczenia koncepcji

W rozdziale przedstawiono koncepcję doskonalenia systemu kreowania świadomości sytuacyjnej ludności umożliwiającą zwiększenie poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego oraz obywateli. Celem koncepcji doskonalenia systemu kreowania świadomości sytuacyjnej jest poprawa zdolności reagowania i rozumienia przez członków ZZK oraz obywateli różnorodnych sytuacji kryzysowych, wydarzeń i zagrożeń występujących w otoczeniu.

Świadomość sytuacyjną oraz przetwarzanie informacji należy traktować jako jedne z głównych czynników uskuteczniających działania w momencie wystąpienia zagrożeń i kryzysów. Zagrożenia te i ryzyko z nim związane powinno być odpowiednio rozpoznane i zidentyfikowane w taki sposób, aby możliwe było zwalczanie lub redukowanie skutków. Zagrożenie powstałe w następstwie katastrof naturalnych, awarii technicznych oraz działalności człowieka należy traktować jako zaburzenie funkcjonowania w normalnych warunkach, w których świadomość sytuacyjna może być znacznie obniżona, a przetwarzanie informacji ograniczone lub uproszczone.

Jak wspomniano w poprzednich rozdziałach świadomość sytuacyjną należy rozumieć jako umiejętność rozumienia i interpretowania rzeczywistości oraz środowiska w odniesieniu do różnych czynników, zdarzeń i sytuacji czy zjawisk. Umiejętność ta obejmuje zdolność postrzegania, analizowania i przetwarzania informacji z różnych źródeł, co stanowi istotny czynnik w skutecznym podejmowaniu decyzji w zarządzaniu kryzysowym.

Przetwarzanie informacji można zinterpretować jako proces, w którym otrzymywane są bodźce sensoryczne, które następnie przekształcane są w zrozumiałe i użyteczne informacje. Świadomość sytuacyjna i przetwarzanie informacji są zatem ściśle ze sobą powiązane:[350]

- postrzeganie – odbieranie informacji sensorycznych pochodzących z otoczenia,
- zrozumienie – analiza oraz uporządkowanie otrzymanych informacji oraz dostrzeganie zależności między różnymi elementami,

[350] J. Oleński, *Ekonomika informacji: Metody*, Wydawnictwo PWE, Warszawa 2003, s. 92.

- prognozowanie – podejmowanie decyzji na podstawie odebranych informacji oraz dostosowywanie reakcji do nowo otrzymywanych informacji.

Zapewnienie odpowiedniego poziomu świadomości sytuacyjnej oraz skuteczne przetwarzanie informacji to istotny element zarządzania kryzysowego. Zastosowanie odpowiednich strategii, narzędzi oraz technologii może ułatwić podejmowanie ważnych decyzji co pozwala na lepsze przygotowanie się na zagrożenia. Bazując na aktualnych rozwiązaniach oraz przeprowadzonych badaniach ankietowych sformułowano następujące założenia dotyczące Systemu Zarządzania Kryzysowego oraz podsystemów wchodzących w jego strukturę:

- System Zarządzania Kryzysowego powinien być wyposażony w rozwiązania dostosowane do potrzeb obywateli i wykorzystywać alternatywnie lub łącznie (synergicznie) zarówno współczesne jak i tradycyjne technologie w procesie informowania ludności o zagrożeniach oraz w procesie kształtowania ich świadomości sytuacyjnej.
- Skuteczne reagowanie na sytuacje kryzysowe wymaga systematycznej inwentaryzacji stanów magazynowych sprzętu niezbędnego do wykorzystania w fazie przygotowania i reagowania na zagrożenia. Inwentaryzacja ta może zostać przeprowadzona za pośrednictwem takich technologii jak m.in. RFID lub kody kreskowe, a dane na temat ich ilości zgromadzone w bazach danych.
- Odpowiednia reakcja na zagrożenia wymaga systematycznych szkoleń, ćwiczeń oraz stosowania modeli i systemów symulacyjnych, a także narzędzi sztucznej inteligencji do rozpoznawania zagrożeń, monitorowania i prognozowania ich skutków oraz opracowywania wielowariantowych scenariuszy przebiegu sytuacji kryzysowej z wykorzystaniem współczesnych technologii IT/ICT (ZSIZ/BI/*OLTP*/OLAP/DM, *IoT*, *Big Data*/DM/AI, *VR/AR*, CC, *Blockchain*) wspierających tradycyjne rozwiązania.
- Odpowiednie reagowanie na zagrożenia wymaga skutecznego przetwarzania informacji za pośrednictwem dostępnych technologii dostosowanych do potrzeb obywateli (chatboty, sztuczna inteligencja, telefon stacjonarny, klasyczny telefon komórkowy, urządzenia mobilne np. smartfon tablet, itp., a także technologie takie jak *IoT*, media społecznościowe oraz rozwiązania takie jak np. radio, telewizja, megafony, syreny alarmowe oraz reklamy rozumiane jako

formy przetwarzania informacji za pośrednictwem: plakatów, spotów telewizyjnych, audycji radiowych, telebimów, bilbordów itp.).

- Kształtowanie świadomości sytuacyjnej dla członków ZZK oraz obywateli wymaga dostępu do informacji na temat zagrożeń, dzięki czemu możliwe jest skuteczniejsze przygotowanie się na nie.
- Podsystemy wykorzystywane na każdym szczeblu zarządzania kryzysowego wchodzące w skład SZK powinny być ujednolicone tak, aby możliwe było wykorzystanie scenariuszy zagrożeń, informacji o zagrożeniach, technologii oraz danych w dowolnym regionie kraju.
- System Zarządzania Kryzysowego powinien wykorzystywać technologie w taki sposób, aby możliwe było dopasowanie ich do potrzeb osób, które będą je wykorzystywać.

Co istotne należy zwrócić uwagę na fakt, że skuteczne przetwarzanie informacji oraz zapewnienie świadomości sytuacyjnej powinno być uwzględnione we wszystkich fazach zarzadzania kryzysowego tj.:

- przygotowania i zapobiegania – identyfikacja i ocena zagrożeń, przygotowanie planów zarządzania kryzysowego, dobór technologii możliwych do wykorzystania,
- reagowanie – wykorzystanie wcześniej wypracowanych rozwiązań oraz wdrożonych technologii, ujednolicenie sposobu reagowania na zagrożenia,
- odbudowa – powrót do funkcjonowania sprzed wystąpienia zagrożenia oraz przywrócenie użyteczności terenów dotkniętych kryzysem wykorzystując technologie takie jak m.in. zdjęcia satelitarne, mapy historyczne itp.

Warto jednak zwrócić uwagę na fakt, że dynamiczny rozwój sytuacji kryzysowych powoduje, że nie zawsze możliwa jest szybka reakcja na zagrożenia oraz odpowiednie przetwarzanie informacji. Skuteczne przeciwdziałanie zagrożeniom możliwe jest pod warunkiem:

- wcześniejszego przygotowania się na nie poprzez analizę danych historycznych i poszukiwanie analogii,
- monitorowanie aktualnego stanu oraz symulowanie przyszłych zagrożeń zarówno w środowisku wirtualnym, jak i rzeczywistym,

- przygotowania poradników, dla Zespołów Zarządzania Kryzysowego (na temat wykorzystywanych technologii) i obywateli (na temat zagrożeń oraz jak należy zachować się w sytuacjach kryzysowych),
- opracowanie jednolitych planów zarządzania kryzysowego na każdym szczeblu (województwo, powiat, gmina, państwo),
- określenia, które omówione w rozprawie technologie są możliwe do wykorzystania,
- określenia odpowiednich procedur działania w poszczególnych fazach zarządzania kryzysowego (zapobiegania, przygotowania, reagowania i odbudowy),
- ujednolicenia procedur działania (plany zarządzania kryzysowego) na każdym szczeblu (województwo, powiat, gmina, państwo),
- dobór odpowiedniej technologii IT/ICT oraz określenie, na którym poziomie świadomości sytuacyjnej może zostać użyta i w jakim konkretnie celu.

Spełnienie tych warunków może przyczynić się do szybszego reagowania na zagrożenia poprzez jednoznaczny przydział obowiązków dla interesariuszy zaangażowanych w „walkę" z zagrożeniem oraz zapewnienie ciągłości działania na terenach dotkniętych kryzysem. Analiza danych historycznych, stałe monitorowanie zagrożeń oraz odpowiednie przygotowanie się na nie poprzez prowadzenie ćwiczeń w środowisku wirtualnym i rzeczywistym może znacznie przyspieszyć prowadzone akcje ratownicze. Tego typu działania możliwe będą do wykonania pod warunkiem ukształtowania odpowiedniego poziomu świadomości sytuacyjnej warunkowanej dostępnością odpowiedniej informacji. Stosowne zatem jest przygotowanie odpowiednich materiałów i szkoleń zarówno dla Zespołów Zarządzania Kryzysowego, jak i obywateli. Rozwiązania tego typu powinny być wsparte współczesnymi technologiami w trosce o rzetelność przekazu, mimo że przeprowadzone badania ankietowe wskazują także na potrzebę wykorzystania tradycyjnych rozwiązań. Dodatkowo należy uwzględnić fakt, że w przypadku zagrożeń mogą pojawić się problemy z funkcjonowaniem współczesnych technologii na skutek uszkodzenia np. infrastruktury teleinformatycznej. Istnieje również ryzyko, że brak wiedzy na temat wykorzystania proponowanych rozwiązań bądź niewłaściwe ich wykorzystanie może uczynić je nieprzydatne lub podatne ataki.

Usprawnienie funkcjonowania Systemu Zarządzania Kryzysowego będzie zatem wymagało przygotowania odpowiedniej infrastruktury pod funkcjonowanie pro-

ponowanych technologii, a także szkoleń, tak aby wdrożona technologia była właściwie wykorzystywana. Należy zatem przyjąć, że nie spełnienie tych warunków może uczynić technologię bezużyteczną. Ponadto warto zwrócić uwagę na fakt, że ze względu na zróżnicowane wiekowo grupy społeczne niewskazane jest bazowanie na jednej technologii. Dlatego też niezbędne jest wykorzystanie potencjału wszystkich dostępnych rozwiązań. Ograniczeniem przyjętym w koncepcji jest grupa odbiorców, dla której są dedykowane poszczególne rozwiązania. Pomimo licznych grup zaangażowanych w zarządzanie kryzysowe przyjęto, że najważniejsze grupy docelowe stanowią Zespoły Zarządzania Kryzysowego oraz obywatele jako aktywni interesariusze SZK.

Niezbędna jest zatem etapowa weryfikacja dostępnych procedur w zakresie informowania ludności o zagrożeniach i modeli świadomości sytuacyjnej w celu opracowania odpowiedniej strategii działania w poszczególnych fazach zarządzania kryzysowego. Dynamiczny rozwój sytuacji kryzysowych powoduje, że nie zawsze możliwa jest szybka reakcja na zagrożenia oraz odpowiednie przekazywanie informacji na ich temat. Dlatego też wykorzystanie potencjału technologii ma na celu zarówno zapewnienie skutecznego przepływu informacji, jej weryfikacji jak i ochrony. Ważne zatem jest kreowanie pożądanego poziomu świadomości sytuacyjnej na temat zagrożeń przed ich wystąpieniem poprzez zapewnianie postrzegania, rozumienia i projekcji działania na bazie rzetelnego procesu informowania. Dotyczy to przede wszystkim możliwości odpowiedniego przygotowania Zespołów Zarządzania Kryzysowego, służb ratowniczych i obywateli.

Badania ankietowe oraz raport NIK[351] wskazały na potrzebę doskonalenia aktualnie wykorzystywanych rozwiązań.

Zaproponowana koncepcja eksponuje nowoczesne rozwiązania, które w znacznym stopniu mogą poprawić poziom świadomości sytuacyjnej ZZK oraz obywateli na poszczególnych poziomach jej kształtowania. Przyjmuje się że, aby możliwe było osiągnięcie pożądanego stanu, niezbędne jest wdrożenie technologii do gromadzenia danych bez ograniczeń objętościowych połączone z procesami wielowariantowego monitorowania zagrożeń i ich przetwarzania (OLAP/*OLTP*/DM, *IoT*, *Big Data*, *Blockchain*, *BI, CC*) oraz bezpiecznego przekazywania (szyfrowania). Ważne stają się tu narzędzia do symulowania zagrożeń, przewidywania skutków ich

[351] https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html (data dostępu 03.08.2021).

materializacji oraz kreowania świadomości sytuacyjnej ludności i obywateli (sztuczna inteligencja, systemy GIS, AR/*VR*). Współczesne technologie to szereg rozwiązań możliwych do wykorzystania w sytuacjach kryzysowych. Nie sposób wdrożyć wszystkie obecnie istniejące technologie, dlatego też ograniczono ich wybór do najbardziej reprezentatywnych z punktu widzenia potrzeb potencjalnych użytkowników/interesariuszy, które w ocenie autora rozprawy mogą mieć znaczący wpływ na usprawnienie procesów zarządzania kryzysowego w odniesieniu do wskazanych wcześniej grup docelowych.

Co istotne wykorzystanie współczesnych technologii w zarządzaniu kryzysowym pomimo korzyści z nimi związanymi niesie ze sobą pewne ograniczenia i wyzwania. Spośród głównych ograniczeń związanych z wdrożeniem wspomnianych technologii można wyróżnić takie jak:

- Koszt wdrożenia technologii – technologie takie jak sztuczna inteligencja, IoT/IoE, czy VR/AR mogą być kosztowne zarówno w zakresie zakupu specjalistycznego sprzętu np. czujników, kamer, okularów do wirtualnej rzeczywistości jak i w zakresie rozbudowy infrastruktury o urządzenia takie jak np. mikrokontrolery *Arduino czy Raspberry Pi* możliwe do wykorzystania w celu budowy prostych urządzeń IoT, które można programować i łączyć z siecią, a także o wysokowydajnościowe komputery wspierające technologię wirtualnej rzeczywistości, a także oprogramowanie do tworzenia zaawansowanych scenariuszy zagrożeń w wirtualnym środowisku,
- Dostęp do infrastruktury – w niektórych regionach kraju wdrożenie współczesnych technologii może być utrudnione ze względu na brak odpowiedniej infrastruktury teleinformatycznej, a w szczególności na obszarach wiejskich oraz słabo rozwiniętych,
- Wsparcie i szkolenia – osoby odpowiedzialne za wykorzystanie współczesnych technologii mogą potrzebować odpowiedniego szkolenia, aby było możliwe ich wykorzystanie,
- Bezpieczeństwo danych – wykorzystywanie oraz wdrażanie współczesnych technologii wymaga zapewnienia wysokiego poziomu bezpieczeństwa danych ze względu na wrażliwe dane,
- Zrozumienie i akceptacja obywateli – wdrożenie współczesnych technologii w zarządzaniu kryzysowym wymaga przeprowadzenie szkoleń oraz edukowa-

nia nie tylko członków zespołów zarządzania kryzysowego i służb ratowniczych ale również obywateli, aby wdrożone rozwiązania były dla nich zrozumiałe,

- Wydajność i niezawodność – w niektórych sytuacjach na przykład na skutek klęsk żywiołowych współczesne technologie mogą okazać się niewystarczająco stabilne lub wydajne co może spowodować opóźnienia lub awarie w czasie rzeczywistym,
- Regulacje prawne – wdrożenie współczesnych technologii może wymagać spełnienia warunków w bezpieczeństwa z zakresie ochrony danych osobowych,

Skuteczne wdrożenie współczesnych technologii teleinformatycznych wymaga uwzględnienia wskazanych ograniczeń. Niemniej jednak pomimo wspomnianych utrudnień warto wziąć pod uwagę korzyści z zastosowania współczesnych technologii, które w znaczący sposób mogą poprawić efektywność i skuteczność działań w sytuacjach kryzysowych. Zasadne zatem wydaje się dokładne przeanalizowanie dostępnych technologii oraz dostosowanie ich do potrzeb członków zespołów zarządzania kryzysowego, służb ratowniczych oraz obywateli.

6.2. Zakres procesu doskonalenia istniejących rozwiązań

Doskonalenie aktualnie wykorzystywanych rozwiązań w zarządzaniu kryzysowym odgrywa istotną rolę, ponieważ umożliwia skuteczniejsze przygotowanie się do sytuacji kryzysowych oraz może usprawnić reakcję na nie w momencie ich wystąpienia, a także poprawić zdolność reagowania na sytuacje kryzysowe oraz zminimalizować skutki przez nie wywołane. Proces doskonalenia powinien obejmować takie obszary jak:

- analiza i ocena ryzyka – identyfikacja potencjalnych zagrożeń oraz oszacowanie prawdopodobieństwa ich wystąpienia oraz skutków, które mogą wywołać, co w dalszej perspektywie pozwala na lepsze dostosowanie strategii i planów działania,
- planowanie kryzysowe – udoskonalenie aktualnie wykorzystywanych planów zarządzania kryzysowego lub ich utworzenie w przypadku ich braku, tworzenie scenariuszy zagrożeń oraz kroki jakie należy wykonać na wypadek wystąpienia,

- wdrażanie procedur i ćwiczenia – systematyczne przeprowadzanie szkoleń, symulowanie zagrożeń, regularne wdrażanie procedur co pozwala na poprawę działania służb ratowniczych oraz zidentyfikowanie słabych punktów w SZK oraz lepsze zrozumienie procesów zarządzania kryzysowego,
- szkolenia i konferencje – szkolenia personelu z funkcjonowania technologii oraz edukowanie obywateli na temat zachowań w sytuacjach kryzysowych, co może znacznie zwiększyć poziom świadomości sytuacyjnej oraz przygotować na zagrożenia, a także poprawić zdolność do efektywnej reakcji na różne scenariusze kryzysowe.
- współpraca międzysektorowa – doskonalenie procesu zarządzania kryzysowego poprzez współpracę między różnymi sektorami, takimi jak administracja publiczna, służby ratownicze, organizacje pozarządowe, przedsiębiorstwa oraz obywatele. Współpraca ta i wymiana informacji może znacznie zwiększyć efektywność działań,
- wykorzystanie technologii – doskonalenia SZK poprzez użycie technologii, takich jak m.in. systemy wczesnego ostrzegania, analiza danych w czasie rzeczywistym czy aplikacje mobilne ułatwiające komunikację w czasie kryzysu, a także tradycyjnych rozwiązań takich jak: radio, telewizja, syreny alarmowe itp.
- Ulepszenie infrastruktury i technologii – wdrożenie współczesnych technologii teleinformacyjnych takich jak systemy *IoT*, sztuczna inteligencja, czy analiza danych w czasie rzeczywistym, w celu poprawy monitorowania, wczesnego ostrzegania i zarządzania sytuacją kryzysową.
- Testowanie i ciągłe doskonalenie – regularne sprawdzanie i testowanie planów oraz procedur zarządzania kryzysowego, w celu sprawdzenia ich skuteczności, a także stosowanie odpowiednich korekt i procedur ulepszeń tych planów i procedur.
- Ulepszenie komunikacji – udoskonalenia systemu komunikacji wewnętrznej i zewnętrznej w czasie sytuacji kryzysowych poprzez wykorzystanie współczesnych technologii takich jak np. media społecznościowe, w celu zapewnienia skutecznego przepływu informacji.
- Stworzenie alternatywnych źródeł komunikacji zewnętrznej i wewnętrznej w czasie kryzysu na wypadek awarii infrastruktury teleinformatycznej.

- Świadomość sytuacyjna – edukowanie społeczeństwa w zakresie zachowań w sytuacjach kryzysowych, dostarczanie jasnych i precyzyjnych informacji oraz zwiększenie zaufania do organów rządzących.

Doskonalenie istniejących rozwiązań w zarządzaniu kryzysowym jest procesem ciągłym i wymaga zaangażowania wielu podmiotów oraz dostosowywania działań do zachodzących zmian. Skuteczne zarządzanie kryzysowe może znacząco wpłynąć na minimalizację strat, ochronę zdrowia i życia ludzi oraz zapewnienie szybkiego powrotu do normalności po wystąpieniu sytuacji kryzysowych, co stanowi istotny atrybut systemowy w zarządzaniu kryzysowym oraz w procesie zapewnienia bezpieczeństwa publicznego. Do osiągnięcia tych celów niezbędna jest sprawna komunikacja oraz dostęp do krytycznych informacji przed, w trakcie i po zakończeniu zagrożenia. Wzajemne powiązania i współpraca między różnymi służbami ratowniczymi ma zasadnicze znaczenie dla skutecznego ratowania życia i ochrony mienia. Pomimo znacznej wiedzy osób zarządzających państwem oraz członków Zespołów Zarządzania Kryzysowego w zakresie zmniejszania ryzyka związanego z klęskami żywiołowymi, ryzyko to może stale rosnąć[352]. Efektywne procesy komunikowania się w sytuacjach kryzysowych zmniejszają niepewność, która może wywołać lęk, strach oraz brak skutecznych działań[353]. Dlatego też istotne jest dopasowanie dostępnych rozwiązań do potrzeb obywateli, aby zagwarantować im poczucie bezpieczeństwa i zwiększyć ich poziom świadomości sytuacyjnej na temat zagrożeń. Oprócz komunikacji istotną rolę w zarządzaniu kryzysowym odgrywa umiejętność szybkiego podejmowania decyzji na bazie wiarygodnych zasobów informacyjnych (rola współczesnych technologii IT/ICT), co w przypadku zagrożenia może także sprzyjać lepszemu poziomowi bieżącej kontroli i oceny rozwoju sytuacji kryzysowej. Niemniej jednak podjęcie odpowiedniej decyzji wymaga zarówno od obywateli, jak i Zespołów Zarządzania Kryzysowego, skutecznej analizy zagrożeń poprzez uczenie się oraz obserwowanie otoczenia w celu kształtowania wysokiego poziomu świadomości sytuacyjnej, którego trzy etapy zaprezentowała w swoim modelu M. R. Endsley[354] (postrzeganie, zrozumienie, prognozowanie). Etapy te mogą ułatwić stopniowe przygotowywanie się na zagrożenie. Do osiągnięcia oczekiwanego poziomu świadomości sytua-

[352] A. Boin, P. Hart, E. Stern, B. Sundelius, *The Politics of Crisis Management: Public Leadership Under Pressure*. Cambridge, UK: Cambridge University Press; 2016.
[353] Tamże.
[354] C.A. Bolstad, M.R. Endsley, *Tools for supporting team collaboration, Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA: HFES. s. 374-378.

cyjnej oprócz zastosowania tradycyjnych oraz współczesnych technologii IT/ICT niezbędne jest również ćwiczenie zachowań warunkowanych na obserwację otoczenia i analizę zdarzeń zachodzących w nim, co może okazać się determinantą skutecznego działania zarówno pojedynczych obywateli, jak i osób funkcyjnych w strukturach SZK.

Analiza funkcjonalności istniejących technologii IT/ICT w Systemie Zarządzania Kryzysowego RP oraz przeprowadzone badania ankietowe wskazują na potrzebę uskutecznienia procesu przetwarzania informacji i podnoszenia poziomu świadomości sytuacyjne, ponieważ niektórzy obywatel nie są w stanie przygotować się na zagrożenia na podstawie otrzymanych informacji ze względu na niezrozumiałość otrzymanych treści. Doskonalenie aktualnych rozwiązań funkcjonujących w ramach Systemu Zarządzania Kryzysowego posiada pewne ograniczenia co do ich zastosowania. Podstawowym ograniczeniem jest nieznajomość nowo wdrażanych rozwiązań (utrudniony proces ich wykorzystania bez odpowiedniego szkolenia). Bez wiedzy na temat funkcjonowania wdrażanych technologii niemożliwy jest odczyt danych z nich pochodzących np. z czujników *IoT* oraz zaplanowanie dalszych działań niezbędnych do wykonania (podjęcie działań zapobiegawczych, przydzielenie zadań służbom ratowniczym, informowanie ludności, itp.).

Warto zwrócić uwag na fakt, że pomimo iż istnieje potrzeba wprowadzenia nowych rozwiązań, to te nie mogą zostać zaimplementowane w pośpiechu. Proces wdrażania wymaga odpowiednich zasobów i musi być rozłożony w czasie, jest to bowiem często okres intensywnego szkolenia. Ponadto nowe rozwiązania mogą nakładać się na siebie, ponieważ mają stanowić alternatywę dla aktualnie wykorzystywanych. Doskonalenie istniejących rozwiązań jest uwarunkowane także przygotowaniem adekwatnego do potrzeb budżetu. Przed wdrożeniem wybranej technologii należy mieć pewność oceny jej przydatności i sprawdzenia jej działania w warunkach rzeczywistych. W przypadku nowoczesnych technologii warto zwrócić uwagę na fakt, że ich rozwój wykreował również nowe zagrożenia, a część z nich dotyczy również cyberprzestrzeni. Dlatego też wdrożone technologie powinny opierać się nie tylko na rozwiązaniach ułatwiających funkcjonowanie wskazanych grup docelowych, ale również na poufności i integralności zasobów informacyjnych, a w tym na potrzebie stosowania mechanizmów zapewniania bezpieczeństwa przesyłanych informacji w procesie przygotowywania oceny sytuacji jak i na etapie planowania działań związanych z zagrożeniem.

6.2.1. Syntetyczna ocena kierunków doskonalenia istniejących rozwiązań

Zarządzanie kryzysowe może bezpośrednio dotyczyć zmian zachodzących w społeczeństwie i w środowisku. Aby sprostać tym zmianom i zagrożeniom, które wywołały niezbędne jest wprowadzanie rozwiązań akceptujących te zmiany. Syntetyczna ocena kierunków doskonalenia istniejących rozwiązań w zarządzaniu kryzysowym wskazuje na potrzebę poprawy działań oraz reakcji na zaistniałe sytuacje kryzysowe w celu minimalizacji skutków, które mogą one wywołać, co jest możliwe do osiągnięcia poprzez:

- integrację systemów takich jak systemy monitorowania, wczesnego ostrzegania, powiadomień oraz analizy danych co umożliwia skuteczniejszą wymianę informacji oraz koordynację działań,
- wykorzystanie sztucznej inteligencji do prognozowania i modelowania zagrożeń oraz analizy danych poprzez zastosowanie algorytmów pozwalających na analizę dużej ilości danych w celu uskutecznienia podejmowania decyzji w czasie rzeczywistym,
- automatyzację i inteligentne systemy takie jak systemy wczesnego ostrzegania, sterowania ruchem itp.,
- technologie mobilne takie jak np. aplikacje, powiadomienia, SMS-y oraz media społecznościowe do szybkiego i efektywnego informowania o zagrożeniach oraz do przekazywania informacji na temat sposobu zachowania się,
- współpracę międzyinstytucjonalną niezbędną do koordynowania działań i wymiany informacji między różnymi organami państwowymi oraz prywatnymi podmiotami,
- edukowanie społeczności poprzez podnoszenie świadomości sytuacyjnej obywateli na temat zagrożeń oraz kształtowanie umiejętności reagowania na nie.

Przeprowadzona w ten sposób ocena zastosowania technologii sprzyja określeniu jej użyteczność w warunkach zagrożeń i kryzysów.

W rozprawie przeanalizowane zostały aktualne rozwiązania w zakresie:

- monitorowania zagrożeń, zbierania oraz gromadzenia danych,
- przetwarzania różnorodnych kolekcji zebranych/dostępnych danych dla uzyskania kompletnych, kompleksowych i spójnych informacji o zagrożeniu,

- informowania o zagrożeniach w formie zrozumiałej dla danej grupy odbiorców,
- bezpiecznego i pewnego przepływu informacji,
- kreowania świadomości sytuacyjnej poprzez odpowiednią formę przesyłanej treści w zależności od grupy docelowej,
- wsparcia działań przeciw-zagrożeniowych zarówno w fazie reagowania, jak i w fazie odtworzeniowej w tym prowadzenia akcji ratowniczych.

Analiza ta umożliwiła dokonanie oceny aktualnych rozwiązań i kierunków rozwoju. Upatruje się zatem we współczesnych technologiach IT/ICT skuteczne rozwiązanie, które może:

- usprawnić proces podejmowania decyzji,
- usprawnić koordynację działań,
- usprawnić proces komunikowanie się,
- poprawić świadomość sytuacyjną na temat zagrożeń (w zakresie indywidualnym, lokalnym, globalnym, a także funkcjonowania organizacji i instytucji oraz władzy publicznej na wszystkich poziomach świadomości sytuacyjnej dla wszystkich znanych społeczeństwu zagrożeniom),
- usprawnić proces wymiany i przetwarzania informacji,
- przyspieszyć działania służb zaangażowanych w sytuację kryzysową.

Koncepcja doskonalenia systemu kreowania świadomości sytuacyjnej ludności wymaga wykorzystania nowoczesnych technologii, integracji różnych systemów, wykorzystania sztucznej inteligencji i analizy danych oraz skupienia się na współpracy międzyinstytutowej. Ważne jest również dążenie do ciągłego doskonalenia działań edukacyjnych i szkoleniowych, które podnoszą świadomość społeczeństwa i przygotowują je do efektywnego reagowania na różnego rodzaju zagrożenia, co może się przyczynić do uodpornienia społeczeństwa na zagrożenia oraz skutecznego zarządzania kryzysowego.

6.2.2. Aspekty poprawy postrzegania zagrożeń

Poprawa postrzegania zagrożeń odgrywa istotną role w procesie zapewnienia świadomości sytuacyjnej oraz zwiększa zdolność reagowania na potencjalne niebezpieczeństwa. Odpowiednie przygotowanie się na zagrożenia oraz kreowanie świadomości sytuacyjnej ludności na ich temat wymaga stałego ich monitorowania, po-

równywania z danymi historycznymi oraz analizowania potencjalnych skutków, które mogą wywołać. Do osiągnięcia pożądanego stanu poziomu świadomości sytuacyjnej zmierzającej do przeciwdziałania zagrożeniom niezbędne jest:

- uaktualnianie odpowiedniej klasyfikacji zagrożeń (katastrofy naturalne, awarie techniczne, zagrożenia wynikające z działalności człowieka) z określeniem sposobu postępowania w momencie ich wystąpienia (wymaga ewakuacji, wymaga informowania, wymagające izolacji – tabela 6.1),
- przydzielanie (określone) niezbędnych zasobów do wykorzystania w momencie wystąpienia zagrożeń (tabela 6.2),
- określenie zadań dla Zespołów Zarządzania Kryzysowego na bazie informacji o grupach docelowych.

Tabela 6.1. Klasyfikacja zagrożeń

ZAGROŻENIA																			
Rodzaj zagrożeń	**Katastrofy naturalne**					**Awarie techniczne**						**Zagrożenia wynikające z działalności człowieka**							
	Powodzie	Pożary	Susze	Wyładowania atmosferyczne	Silne wiatry	Awarie sieci energetycznych	Awarie sieci wodociągowych	Awarie instalacji gazowej	Awarie telekomunikacyjne	Katastrofy budowlane	Zakłócenia bezpieczeństwa i porządku publicznego	Katastrofy techniczne i naturalne powstałe na skutek działalności człowieka: Awarie urządzeń infrastruktury technicznej	Katastrofy budowlane	Katastrofy komunikacyjne	Awarie chemiczne	Katastrofy ekologiczne	Epidemie	Akty terroru
	W – Wymaga ewakuacji, N – Wymaga informowania, I – Wymaga izolacji																	
Wymaga ewakuacji	**W**	**W**						**W**		**W**			**W**	**W**				
Wymaga informowania			**N**	**N**	**N**	**N**	**N**		**N**		**N**	**N**				**N**		
Wymaga izolacji	**I**	**I**	**I**		**I**			**I**			**I**				**I**		**I**	**I**

Źródło opracowanie własne

Dla celów pracy dokonano klasyfikacji zagrożeń z uwzględnieniem podstawowych procesów podejmowanych przez ZZK, które dotyczą obywateli czyli: ewakuacja, informowanie oraz izolacja (tab. 6.1).

Zaproponowana klasyfikacja zagrożeń może w znacznym stopniu ułatwić proces zarządzania kryzysowego oraz zwiększyć świadomość sytuacyjną ZZK i obywa-

teli na poziomie postrzegania zagrożenia i jego interpretacji. Dzięki zaproponowanej klasyfikacji możliwe jest uproszczenie procesu informowania ludności o zagrożeniach oraz ujednoznacznienie charakterystyki zagrożeń i sposobu radzenia sobie z nimi.

W procesie kreowania świadomości sytuacyjnej obywateli zasadna wydaje się również identyfikacja niezbędnych zasobów związanych z poszczególnymi zagrożeniami. Tabela istotności zasobów może zwiększyć świadomość sytuacyjną ludności o zagrożeniach oraz ułatwić proces przygotowania się na nie (tab. 6.2). Pomimo, iż zaprezentowane rozwiązania mogą wydawać się oczywiste, to należy zwrócić uwagę na fakt, że wśród społeczeństwa są osoby odznaczające się niskim poziomie świadomości sytuacyjnej lub takie, w których zachowaniu podczas zagrożeń może pojawić chaos, dezorientacja, lęk, strach, co w rezultacie może spowodować brak racjonalnych działań lub „paraliż". Sytuacje kryzysowe same w sobie mogą wywołać dezorientację oraz brak logicznego myślenia. Brak wiedzy na temat niezbędnych zasobów, które mogą ułatwić przeżycie lub przetrwanie w sytuacji kryzysowej powoduje, że społeczeństwo w momencie wystąpienia zagrożenia nie jest odpowiednio na nie przygotowane w efekcie czego często nie posiada przy sobie niezbędnych zasobów. Wprowadzenie zaproponowanych rozwiązań może nie tylko usprawnić funkcjonowanie SZK, ale także podnieść poziom postrzegania sytuacji wywołanej konkretnym zagrożeniem oraz zmniejszyć liczbę ofiar/poszkodowanych oraz ograniczyć straty w mieniu.

Zaprezentowane dane w tabeli 6.2 dotyczą głównie obywateli, ale mogą także usprawnić pracę Zespołom Zarządzania Kryzysowego w zakresie gromadzenia niezbędnych zasobów do zwalczania skutków zaistniałej sytuacji kryzysowej.

Tabela 6.2. Identyfikacja zasobów istotnych z punku widzenia obywatela w sytuacjach kryzysowych

ZAGROŻENIA																			
RODZAJ ZAGROŻENIA	Katastrofy naturalne					Awarie techniczne						Zagrożenia wynikające z działalności człowieka						
												Katastrofy techniczne i naturalne powstałe na skutek działalności człowieka						
	Powodzie	Pożary	Susze	Wyładowania atmosferyczne	Silne wiatry	Awarie sieci energetycznych	Awarie sieci wodociągowych	Awarie instalacji gazowej	Awarie telekomunikacyjne	Katastrofy budowlane	Zakłócenia bezpieczeństwa i porządku publicznego	Awarie urządzeń infrastruktury technicznej	Katastrofy budowlane	Katastrofy komunikacyjne	Awarie chemiczne	Katastrofy ekologiczne	Epidemie	Akty terroru
Rodzaj zasobu niezbędny w czasie sytuacji kryzysowej	Istotne zasoby dla ludności w momencie wystąpienia zagrożenia: **X** – istotne																	
Woda	X	X	X		X		X	X		X	X		X		X	X	X	X
Pożywienie	X	X	X		X			X		X	X		X		X	X	X	X
Odzież	X	X									X							X
Apteczka	X	X								X	X		X	X	X	X	X	X
Latarka	X	X		X	X	X				X		X	X					X
Gaśnica		X												X				
Dokumenty	X	X									X		X	X				X
Środki higieniczne	X	X								X	X		X		X	X	X	X
Zapasowe źródła energii: - baterie -powerbank	X	X		X	X	X			X	X	X	X	X	X	X	X		X
Dostęp do informacji: - telefon komórkowy - radio przenośne - krótkofalówki	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X
Suma istotnych zasobów:	9	10	3	3	5	3	1	3	2	7	8	3	8	5	6	6	5	9

Źródło: opracowanie własne

Aby udoskonalić proces informowania ludności o zagrożeniach oraz odpowiednie przygotowanie się na zagrożenia niezbędne jest stałe monitorowanie pracy i nadzorowanie osób wchodzących w skład ZZK poprzez prowadzenie szkoleń w zakresie postępowania na wypadek wystąpienia sytuacji kryzysowej, prowadzenie ćwiczeń zmierzających do opracowania właściwych procedur działania w momencie wystąpienia zagrożenia oraz określenie ról dla członków zespołów i służb ratowniczych. Aspekt ten może ułatwić postrzeganie zagrożeń, stałe ich monitorowanie oraz zrozumienie, co w rezultacie może ułatwić odpowiednie przygotowanie się na nie. Tradycyjne technologie mają jednak ograniczoną funkcjonalność w zakresie wariantowania skutków zagrożeń oraz indywidualizowania metod ich postrzegania i interpretacji.

6.2.3. Aspekty wzrostu komunikatywności i rozumienia treści

Wzrost komunikatywności i treści stanowią istotny aspekt w zakresie budowania efektywnych relacji interpersonalnych zarówno w sferze zawodowej jak i osobistej. Poprawa komunikatywności to zdolność do rozumienia treści, która wymaga praktyki i zaangażowania. Istotne zatem jest poświecenie czasu na rozwijanie tych umiejętności, ponieważ efektywna komunikacja jest kluczowym elementem w budowaniu trwałych relacji i osiąganiu sukcesu w zarządzaniu kryzysowym.

W sytuacjach kryzysowych ludzie często nie potrafią skutecznie komunikować się z powodu braku jasnych przekazów komunikacyjnych. Ustalenie konkretnych celów przekazu to problem, który należy rozwiązać przed wydaniem jakiegokolwiek komunikatu i komentarza publicznego szczególnie w sytuacjach kryzysowych. Informowanie opinii publicznej o problemach i konkretnych zagrożeniach oraz dostarczenie wskazówek dotyczących odpowiedniej reakcji to główne cele jakie należy osiągnąć w procesie komunikowania się. Przesyłane informacje muszą być zatem skuteczne i przemawiać do odbiorców. Po ustaleniu celu i komunikatów wyzwaniem staje się dostarczenie ich do odbiorców oraz zapewnienie, że przesłane komunikaty zostaną przez nich wysłuchane, a określone w nich cele i zadania zrealizowane[355] .

W sytuacjach kryzysowych istnieje presja związana z dostarczaniem szybkich i dokładnych informacji, które przed udostępnieniem ich dla opinii publicznej muszą być zweryfikowane. Przekazanie niezweryfikowanych informacji może wiązać się

[355] Communicating in a Crisis: Risk Communication Guidelines for Public Officials. Rockville, MD, Substance Abuse and Mental Health Services Administration, 2019 (https://store.samhsa.gov/sites/default/files/d7/priv/pep19-01-01-005.pdf).

z ryzykiem wprowadzania w błąd opinii publicznej oraz podważyć wiarygodność osób, które je udostępniły. Dlatego komunikaty i informacje powinny być proste oraz przekazywane zwięźle, przejrzyście i skutecznie[356].

Skutecznym sposobem na sprostanie temu wyzwaniu jest regularne organizowanie spotkań z mediami podczas, których wszystkie informacje mogą być wyjaśniane i aktualizowane. Tego typu podejście w połączeniu z faktem, że informacje będą aktualizowane pozwala, na zwiększenie zaufania do organów, które je przekazują. W przypadku komunikatów przesyłanych za pośrednictwem mediów społecznościowych poczty, e-mail, czy smsów kluczowe, jest poinformowanie opinii publicznej o fakcie, że dalsze informacje o rozwoju zagrożenia będą wysyłane regularnie. Zastosowanie tego typu rozwiązania może nie tylko uwiarygodnić organy wysyłające informacje, ale także zmniejszyć ryzyko dostępu do informacji niezweryfikowanych[357].

Sukces skutecznego komunikowania się i informowania o zagrożeniach zależy od pracy zrealizowanej w fazie przygotowania na zagrożenie. W tej fazie powinno być określone, jakie informacje należy przekazywać, kto podejmuje decyzje, kto wydaje polecenia oraz kto je wykonuje. Istotne jest, aby powyższe warunki zostały określone w fazie przygotowania na zagrożenia, a nie w momencie jego wystąpienia, ponieważ zagrożenie lub kryzys to „najgorszy" czas na określanie tego typu zadań, ponieważ osoby podejmujące decyzje zamiast skupiać się na zagrożeniach określają metody komunikowania się.

Dlatego też niezbędne jest wcześniejsze przygotowanie informacji o zagrożeniach zawierające aktualne listy telefonów alarmowych oraz arkuszy informacyjnych i materiałów pomocniczych na temat tego, jak się zachować w momencie wystąpienia konkretnej sytuacji kryzysowej. Narzędzia oraz informacje potrzebne do pełnej i skutecznej komunikacji w przypadku wybuchu zagrożenia muszą być łatwo dostępne oraz musi istnieć uzgodniony plan działania[358].

Rozwój technologii IT/ICT doprowadził do wykorzystania potencjału mediów społecznościowych w procesie komunikowania się, co pomogło przekształcić informowanie o ryzyku z jednokierunkowego[359] podejścia liniowego w ciągłą wymianę oraz przepływ informacji między ekspertami a opinią publiczną. Dzięki temu osoby

---

[356] Tamże.
[357] G. Wachinger, O. Renn, C. Begg, C. Kuhlicke, *The risk perception paradox: Implictions for governance and communication of natural hazards*. Risk Analysis, 33(6), 2013 s.1049–1065.
[358] Tamże.
[359] P. Jedynak i S. Szydło, *Zarządzanie ryzykiem,* Zakład Narodowy im. Ossolińskich – Wydawnictwo Wrocław 1997, s. 58.

korzystające z nich mają możliwość dzielenia się opinią między sobą, a funkcjonariusze i organizacje udzielenia odpowiedzi w czasie rzeczywistym. Oprócz zamieszczania ogłoszeń i informacji na stronie internetowej lub w innym jednokierunkowym kanale komunikacji, członkowie Zespołów Zarządzania Kryzysowego i inne organizacje wspierające zarządzanie kryzysowe mogą angażować się w rozmowy, odpowiadać na pytania i wątpliwości oraz korygować nieprawdziwe informacje[360]. Niemniej jednak media społecznościowe mogą być trudne w kontrolowaniu przekazywanych treści. Funkcjonariusze/indywidualne osoby mogą kontrolować treść swoich wiadomości, ale po wejściu do środowiska *online* dynamika przesyłanych informacji powoduje, że te zmieniają się z kontrolowanych na niekontrolowane[361].

W aspekcie wzrostu komunikatywności i rozumienia treści istotne jest zatem, aby w fazie przygotowania na zagrożenie określić i wskazać opinii publicznej wiarygodne źródła informacji, a także określić osoby odpowiedzialne za formę i treść przekazywanej wiadomości i jej weryfikację/potwierdzenie. Sam proces weryfikacji informacji może być utrudniony ze względu na rozwój mediów społecznościowych, niemniej jednak regularne umieszczanie informacji przez osoby zaangażowane w daną sytuację kryzysową może zwiększyć poczucie bezpieczeństwa i zmniejszyć ryzyko dostępu do niezweryfikowanych źródeł[362]. Tradycyjne technologie mają jednak ograniczoną funkcjonalność w zakresie wariantowania formy prezentacji zagrożeń, ważnej dla łatwiejszego ich rozumienia oraz interpretacji przez wybrane grupy docelowe odbiorców.

6.2.4. Aspekt prognozowania zagrożeń i sposobów działania

Prognozowanie zagrożeń oraz opracowywanie odpowiednich sposobów ma istotny wpływ na podejmowanie działań zapobiegawczych. Może to mieć charakter krótkoterminowy i umożliwić określenie prawdopodobieństwa wystąpienia zagrożenia na określonym obszarze lub długoterminowy umożliwiający ocenę ryzyka jego wystą-

[360] A. Perrin, M. Anderson, Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. Fact Tank: News in the Numbers. Washington, DC: Pew Research Center (dostęp 22.07.2022 https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostlyunchanged-since-2018).
[361] A.B. Heldman, J. Schindelar, J. Weaver, *Social media engagement and public health communication: Implications for public health organizations being truly "social*." Public Health Reviews", 35(1), s. 1–18.
[362] Tamże, s. 1 – 18.

pienia z uwzględnieniem potencjalnych strat jakie mogą być wywołane. Uzyskane dane na skutek prognozowania można następnie wykorzystać do[363]:

- opracowania lub weryfikacji planów likwidacji skutków zagrożeń,
- przygotowania map zagrożeń,
- ukierunkowania działań w zakresie reagowania na zagrożenia.

Aktualnie najczęściej wykorzystywane metody w zakresie badania katastrof to metody statystyczne, które zakładają tworzenie zbioru danych statystycznych, ich systematyzację oraz przetwarzanie. Pomimo częstego ich stosowania wykorzystywane są głównie do matematycznej analizy zgromadzonych danych. Ich rola powinna się ograniczać zatem do oceny poprawności analizy istotności zjawiska bądź zagrożenia. Określenie skutków zagrożeń jest stosunkowo trudne, ale ma duże znaczenie dla skutecznego zarządzania kryzysowego. Wczesne oszacowanie skali zagrożenia pozwala na wdrożenie odpowiednich działań w zakresie reagowania na klęski żywiołowe, co umożliwia decydentom wgląd we wdrażane działania w zakresie reagowania na katastrofy. Tradycyjne technologie mają jednak ograniczoną funkcjonalność w zakresie wspomagania procesów prognozowania przebiegu sytuacji kryzysowej oraz propagacji wykrytych zagrożeń i ich skutków w czasie. Współczesne technologie stanowią innowacyjne rozwiązanie w tym zakresie. Dzięki analizie danych pochodzących z dużych zbiorów danych historycznych, prognozowaniu potencjalnych skutków, tworzeniu map zagrożeń, ich wizualizacji, przewidywaniu przyszłych wydarzeń wykorzystując takie technologie jak m.in. *VR/AR*, sztuczna inteligencja itp., możliwe jest lepsze przygotowanie się na zagrożenia np. poprzez możliwości symulacji przebiegu rzeczywistych zagrożeń w środowisku wirtualnym. Wykorzystanie w ten sposób potencjału technologii pozwala na prognozowanie prawdopodobnych skutków oraz umożliwia lepsze przygotowanie się na dane zagrożenie[364].

Skuteczne prognozowanie zagrożeń pozwala na wcześniejsze wykrycie potencjalnych zagrożeń oraz ich identyfikację, co umożliwia podjęcie odpowiednich działań zapobiegawczych w celu zminimalizowania ich skutków. Prognozowanie zagrożeń oraz opracowanie odpowiednich działań prewencyjnych to kompleksowy proces, który wymaga współpracy pomiędzy interesariuszami zaangażowanymi

[363] L. Lukáš, P. Hrůza, M. Kný, *Information Management in Security Components*, Prague: Ministry of Defence of the Czech Republic; 2008.
[364]R. Rahmi, H. Joho, T. Shirai, An Analysis of Natural Disaster-Related Information-Seeking Behavior Using Temporal Stages. Journal of the Association for Information Science and Technology 70(7), 2018., s. 715–728.

w sytuację kryzysową. Istotne zatem jest przewidywanie zagrożeń oraz skutków jakie mogą wywołać, w celu minimalizacji ryzyka oraz ochrony obywateli i ich mienia.

6.2.5. Specyfikacja treści informacyjnej w kontekście wybranych źródeł zagrożeń

Specyfikacja treści informacyjnej w kontekście wybranych źródeł zagrożeń odnosi się do określenia istotnych elementów informacji, które są kluczowe dla przekazywania komunikatów związanych z zagrożeniem. Treść informacji powinna być zatem odpowiednio sformułowana i dostosowana do rodzaju zagrożenia oraz grupy odbiorców. Skuteczne przekazanie informacji o zagrożeniach jest kluczowym elementem w zarządzaniu kryzysowym, ponieważ pozwala na odpowiednie przygotowanie się i reakcję społeczności na zmieniające się sytuacje kryzysowe, które mają wpływ nie tylko na środowisko, ale również na dobra materialne. Sytuacje kryzysowe negatywnie wpływają na funkcjonowania państwa, a także potrafią zaburzyć funkcjonowanie działań informacyjnych i są często trudne do kontrolowania. W początkowej fazie zagrożenia mogą wywołać reakcje zagrażające życiu, zdrowiu i mieniu, a także wzbudzić różne emocje itp.[365]. Odpowiednie przekazywanie treści i komunikacja w czasie kryzysu odgrywa bardzo ważną rolę i jest to warunkiem skutecznego reagowania w sytuacjach kryzysowych. Informacje powinny spełniać następujące wymagania, które są również określane mianem atrybutów informacji[366]:

- trafność/esencjonalizm – zakres i charakter informacji powinien odzwierciedlać istotę przekazu,
- poprawność/wiarygodność – informacje powinny być prawdziwe i wiarygodne,
- terminowość – informacje muszą być dostarczone we właściwym czasie, a ważne decyzje nie mogą być podejmowane bez niezbędnych informacji,
- aktualność – informacje powinny odzwierciedlać rzeczywistość,
- kompletność – wszystkie wymagane informacje, a nie tylko niektóre, powinny być dostępne. Niewystarczająca wiedza z powodu niekompletnych informacji jest bardzo niebezpieczna dla podejmowania decyzji,
- adekwatność – informacje powinny być w miarę szczegółowe.

---

[365] Tamże., s. 715–728.

[366] J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce,* Presscom Sp. z o.o.,Wrocław 2004, s. 21.

Za skuteczny przepływ informacji odpowiadają Centra Zarządzania Kryzysowego których, zadaniem jest zapewnienie sprawnego przepływu informacji pomiędzy organami i strukturami odpowiedzialnymi za zarządzanie kryzysowe. Podejmowanie właściwych decyzji, a w konsekwencji skuteczne działanie, zależy od jakości informacji, dlatego też te muszą być stale aktualizowane[367]. Uaktualnione informacje na temat zagrożeń powinny być przesyłane do wszystkich odbiorców, aby w ten sposób zwiększyć ich poziom świadomości sytuacyjnej na temat zagrożeń. Osoby znające tematykę zagrożeń są w stanie dzięki uzyskanym informacjom łatwiej przygotować się na nie i podejmować odpowiednie decyzje. Model świadomości sytuacyjnej J. Coopera zaprezentowany w rozdziale IV potwierdza słuszność tego stwierdzenia[368].

Treści informacyjne w kontekście zagrożeń umożliwiają uruchomienie procedur związanych z zarządzaniem kryzysowym. Istotne jest zatem, aby były zweryfikowane, skutecznie przekazywane i odpowiednio wykorzystane. Przeszkodą w przekazie informacji jest ich wiarygodność ze względu na różnorodność źródeł, z których pochodzą. Kolejny problem związany z przekazem informacji może dotyczyć aspektów technicznych. Awarie techniczne, działalność człowieka i zagrożenia naturalne mogą uniemożliwić sprawne komunikowanie się za pomocą współczesnych technologii IT/ICT, w efekcie czego niezbędne jest skorzystanie z alternatywnych źródeł takich, jak tradycyjne technologie np. radio, telewizja. W przypadku zagrożeń nie istnieje wspólny kanał komunikacyjny pomiędzy służbami ratowniczymi stąd też w momencie awarii, np. telekomunikacyjnej komunikacja pomiędzy służbami staje się niemożliwa. Niezbędne zatem jest zapewnienie alternatywnych sposobów komunikacji dla służb ratowniczych oraz dla obywateli. Wykorzystanie potencjału współczesnych i tradycyjnych technologii umożliwia stworzenie alternatywnych rozwiązań tego typu. Zasadne zatem wydaje się wybór dostępnych technologii w celu usprawnienia procesu informowania na temat zachodzących zjawisk, a także do podniesienia poziomu świadomości sytuacyjnej na temat zagrożeń.

Istotne zatem jest, aby przesyłane informacje dotarły do jak największej liczby odbiorców, a wykorzystywane technologie były dostosowane do potrzeb obywateli. W celu rozwiązania tego typu problemów należałoby wprowadzić np. specjalne re-

[367] Tamże, s. 21.
[368] J. Ahern, *Gun Digest Buyer's Guide to Concealed-Carry Handgun*, w: Gun Digest Books, Stany Zjednoczone, 2010, s. 60.

gionalne kanały telewizyjne, dostępne u wszystkich operatorów, których zadaniem byłoby informowanie w czasie rzeczywistym o zagrożeniach w danym województwie, wprowadzenie przerw reklamowych w audycjach telewizyjnych z alertami, umieszczanie pasków z informacjami o zagrożeniach oraz procedurami radzenia sobie z nimi, wprowadzenie audycji radiowych na temat zagrożeń, przekazywanie komunikatów radiowych o nadchodzących zagrożeniach w rejonach, w których wystąpiły, a także reklam w miejscach publicznych, których celem byłoby przygotowanie społeczeństwa na zagrożenia.

Ponadto w przypadku awarii aktualnie wykorzystywanych technologii zasadne wydaje się stworzenie rozwiązań w formie papierowej zawierających wskazówki, instrukcje postępowania w czasie zagrożeń, które powinny być ogólnodostępne. Pomimo iż tego typu technologia wydawać się może „przestarzała" w sytuacjach kryzysowych, podczas których może zostać zaburzone działanie infrastruktury krytycznej tego typu rozwiązanie może okazać się niezbędną i jedyną pomocą wszędzie tam, gdzie technologie zawiodą.

Ponadto wykorzystanie sztucznej inteligencji w celu utworzenia chatbotów może w znacznym stopniu przyczynić się do zwiększenia poziomu świadomości sytuacyjnej na temat zagrożeń w kontekście treści informacyjnej. Chatboty mogą udzielać odpowiedzi na pytania zadawane przez obywateli i mogą przyjąć formę:

- asystenta ulokowanego na stronie internetowej lub aplikacji na smartfon, dzięki której poprzez czat zadane pytanie jest przetwarzane, a informacje o zagrożeniach wyszukiwane w bazie danych, aby następnie udzielona została odpowiedź obywatelowi,
- asystenta głosowego, który na podstawie zadanego pytania udziela odpowiedzi. Tego typu rozwiązanie może być wykorzystane równolegle z numerem 112, który w momencie wystąpienia zagrożenia może być przeciążony przez co nie ma możliwości uzyskania informacji na temat zagrożenia. Wprowadzenie dodatkowego numeru, telefonu nie tylko usprawni funkcjonowanie numeru alarmowego, ale także ułatwi obywatelom pozyskiwanie informacji na temat zagrożeń. Rozwój sztucznej inteligencji spowodował, że wiedza na temat zagrożeń może być pobierana z wcześniej utworzonej bazy danych, a odpowiedzi mogą być udzielane w czasie rzeczywistym.

Treści informacyjne w kontekście wybranych źródeł zagrożeń odgrywają istotną rolę w zapewnieniu bezpieczeństwa i w skutecznym zarządzaniu kryzysowym. Celem

treści jest przekazywanie kluczowych informacji na temat zagrożeń, a także sposobów radzenia sobie z nimi, co jest niezwykle ważne, ponieważ umożliwia szybkie powiadomienie o zagrożeniu oraz personalizację treści.

6.2.6. Rozwój bazy techniczno-technologicznej w aspekcie możliwości wzrostu poziomu świadomości sytuacyjnej

Rozwój bazy techniczno-technologicznej jest istotnym elementem w aspekcie możliwości wzrostu poziomu świadomości sytuacyjnej na temat zagrożeń. Technologie mogą być wykorzystywane w celu skutecznego zbierania, analizy i przetwarzania informacji na temat zagrożeń co umożliwia szybsze reagowanie obywateli na sytuacje kryzysowe. Odpowiednie reagowanie na klęski żywiołowe lub katastrofy wywołane na skutek działalności człowieka może zmniejszyć skutki zaistniałych sytuacji[369]. Wykorzystanie nowoczesnych technologii oraz systemów umożliwiających przetwarzanie informacji pozwala na bardziej skuteczną reakcję na zagrożenia i minimalizację ich skutków. Istotne jednak jest, aby rozwój technologiczny szedł w parze z odpowiednią edukacją i szkoleniem obywateli oraz ZZK, aby zwiększyć efektywność wykorzystania tych narzędzi w procesie usprawniania zarządzania kryzysowego.

W związku z tym służby ratownicze oraz Zespoły Zarządzania Kryzysowego powinny dostosować plany działania i narzędzia, tak aby skutecznie przeciwdziałać zagrożeniom. Zarządzanie kryzysowe, które składa się z czterech faz (zapobieganie, przygotowanie, reagowanie, odbudowa) obejmuje ocenę ryzyka, reakcję na kryzys, opracowanie planu działania, mobilizację różnych podmiotów, łagodzenie skutków kryzysu oraz odbudowę[370]. Pomimo iż technologia może być ważnym atutem w zarządzaniu kryzysowym, istotne jest, aby uwzględnić różne osiągnięcia technologiczne (formy komunikacji, gromadzenia informacji, monitorowania, oceny sytuacji itp.).

Współczesne technologie IT/ICT obejmują szeroki zakres urządzeń i rozwiązań (ZSIZ/BI/*OLTP*/OLAP/DM, *IoT*, *Big Data*/DM/*AI*, *VR/AR*, CC, *Blockchain*), które ułatwiają przygotowanie się na zagrożenia oraz uproszczają przepływ informacji. W zarządzaniu kryzysowym urządzenia i aplikacje tego typu mogą być wykorzystywane do systemów wspomagania decyzji, wykrywania zagrożeń, zarządzania informacjami, komunikacji, oraz do działań poszukiwawczo – ratowniczych – począwszy, od telefonów komórkowych i mediów społecznościowych, po bezzałogowe statki po-

[369] P. Jenkins, *Distributed Situation Awareness Theory, Measurement and Application to Teamwork*, Wydawnictwo: Ashigate, Wielka Brytania 2009, s. 10.
[370] Tamże, s. 10.

wietrzne i stacje pogodowe, służące do gromadzenia, rozpowszechniania i monitorowania różnego rodzaju informacji i danych w celu zapewnienia wspólnego obrazu operacyjnego i zapewnienia ciągłości działania.

Wykorzystanie zaawansowanych technologii w rozwijaniu bazy techniczno-technologicznej odgrywa istotną rolę w zakresie wzrostu poziomu świadomości sytuacyjnej na temat zagrożeń co pozwala na ich szybsze wykrywanie i powiadamianie o ich wystąpieniu.

6.3. Syntetyczna ocena kierunków wykorzystania współczesnych technologii IT/ICT

Syntetyczna ocena kierunków doskonalenia istniejących rozwiązań w skutecznym zarządzaniu kryzysowym wskazuje na możliwości poprawy efektywności reakcji na sytuacje kryzysowe oraz minimalizacji ich skutków.

Pomimo iż możliwe jest zidentyfikowanie zagrożeń, nierzadko nie można ich całkowicie wyeliminować. Ludziom znajdującym się w pobliżu zagrożenia trudno jest zrozumieć ostrzeżenie o nich, pomimo iż w niektórych przypadkach skutki zagrożenia mogą być określone zawczasu na podstawie zaistniałych wcześniej sytuacji. Dlatego też niezbędne jest posiłkowanie się współczesnymi technologiami IT/ICT, umożliwiającymi łagodzenie skutków zagrożeń oraz poprawę poziomu świadomości na ich temat[371].

Współczesne technologie IT/ICT mają duży potencjał w zakresie rozwoju i doskonalenia zarządzania kryzysowego. Z ich pomocą można znacznie poprawić skuteczność i efektywność działań w sytuacjach kryzysowych.

Twierdzi się również, że rosnące znaczenie technologii informacyjno-komunikacyjnych w koordynacji między osobami, organizacjami i organami rządowymi jest w stanie zapewnić przepływ informacji w sposób terminowy i przejrzysty[372]. Modernizacja infrastruktury teleinformatycznej oraz popularność inteligentnych urządzeń o rozbudowanych funkcjach poszerza kanały wymiany informacji między nadawcą a odbiorcą. Bogactwo i różnorodność danych odgrywają kluczową rolę w określaniu zróżnicowanych źródeł danych. Źródła te zazwyczaj obejmują blogi, interaktywne mapy i są stosowane na prawie wszystkich etapach działań związanych z zarządzaniem kryzysowym, np., w bibliotekach cyfrowych, portalach społecznościowych oraz radiofonii i telewizji.

---

[371] E. Gruntfest, M. Weber, *Internet and emergency management:* Prospects for the future 1998.
[372] E. Tamże.

W celu określenia oceny możliwości wykorzystania tradycyjnych oraz współczesnych technologii w procesie skutecznego informowania ludności o zagrożeniach dokonano analizy za pomocą metody QFD (rys 6.1).

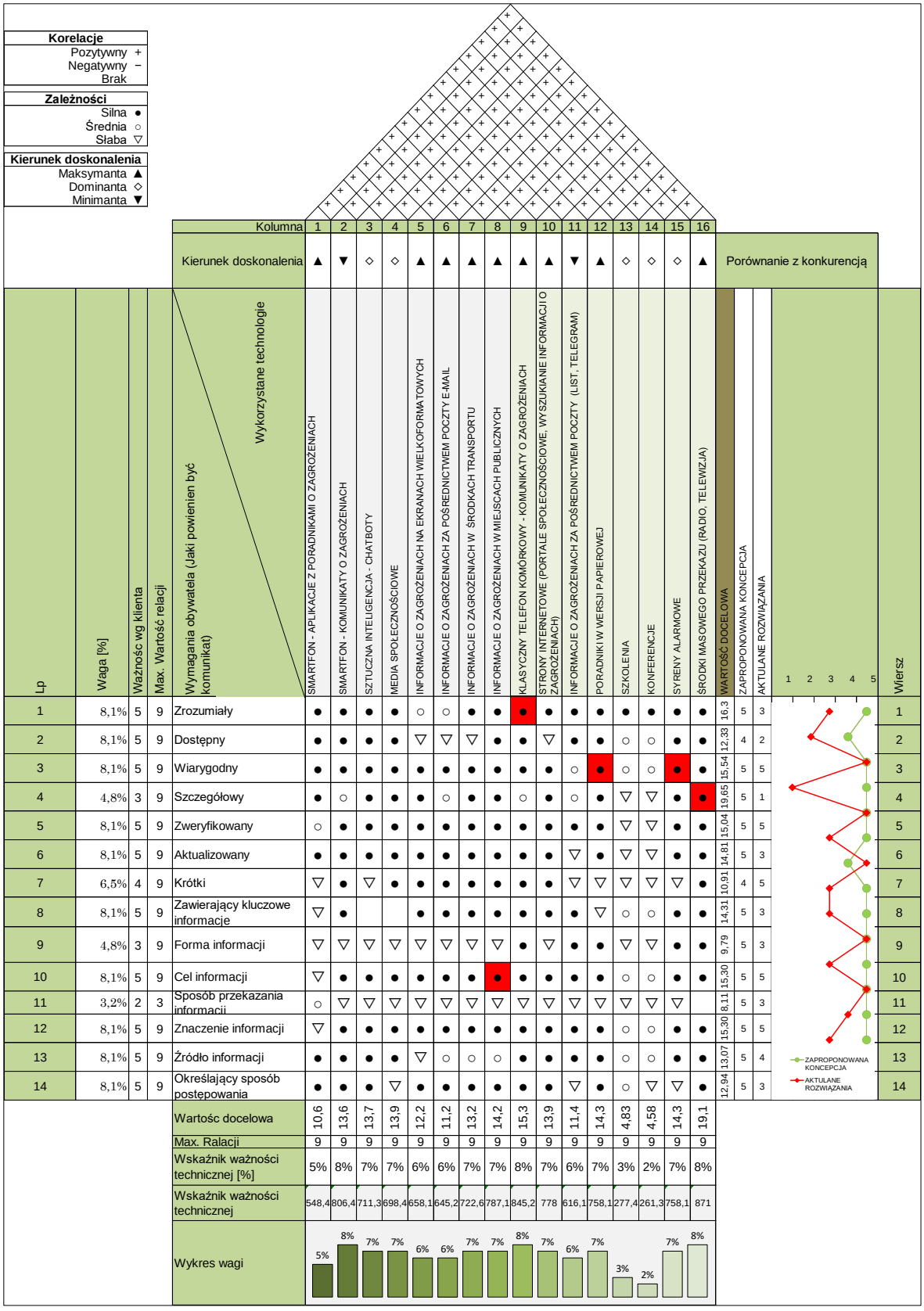
W zaprezentowanym rozwiązaniu przedstawiono koncepcję udoskonalenia procesu informowania ludności o zagrożeniach. W tym celu przeanalizowano aktualne rozwiązania przypisując im odpowiednio wagi od 1 do 5 określające poziom ważności cech komunikatu (1- bardzo niski, 2 – niski, 3 – średni, 4 – wysoki, 5 – bardzo wysoki). Następnie zestawiono je z koncepcją udoskonalenia procesu informowania ludności o zagrożeniach w oparciu o możliwe do wykorzystania współczesne i tradycyjne technologie. Na podstawie przypisanych zależności - kierunek doskonalenia (● – 9, ○ – 3 oraz ▽ – 1) możliwe było określenie najskuteczniejszych technologii w procesie kreowania świadomości sytuacyjnej ludności na temat zagrożeń oraz jakie cechy powinien posiadać przekazywany komunikat.

Za pomocą metody QFD wyodrębniono takie technologie i rozwiązania jak (zaznaczone na rysunku kolorem czerwonym):

- informacje o zagrożeniach w miejscach publicznych,
- klasyczny telefon komórkowy - komunikaty o zagrożeniach,
- poradniki w wersji papierowej,
- syreny alarmowe,
- środki masowego przekazu (radio, telewizja).

Następnie wyodrębniono istotne cechy informacji przekazywanej obywatelowi, która powinna zawierać cel, być zrozumiała, wiarygodna, szczegółowa. Wśród wyodrębnionych technologii oraz rozwiązań można zauważyć że technologie takie jak klasyczny telefon, komórkowy oraz syreny alarmowe są technologiami aktualnie wykorzystywanymi, a rozwiązania takie jak informacje o zagrożeniach w miejscach publicznych, poradniki w wersji papierowej oraz środki masowego przekazu (radio, telewizja) pomimo iż nie są tak rozpowszechnione, mogą uzupełniać wykorzystywane rozwiązania i przyczynić się do podniesienie poziomu świadomości sytuacyjnej na temat zagrożeń. Rozszerzenie procesu informowania ludności o zagrożeniach o zdefiniowane cechy informacji powinno przyczynić się do poprawy tego poziomu.

Zasadne zatem wydaje się wprowadzenie do zarządzania kryzysowego informacji o zagrożeniach w miejscach publicznych, poradników w wersji papierowej, a także audycji na temat zagrożeń, które będą wiarygodne, zrozumiałe oraz na tyle szczegółowe, aby możliwe było jak lepsze przygotowanie się na przyszłe zagrożenia.



Rysunek 6.1. Analiza możliwości wykorzystania współczesnych i tradycyjnych technologii w procesie informowania ludności o zagrożeniach wg modelu QFD w SZK

Źródło: opracowanie własne

Przedstawiona analiza QFD jednoznacznie pokazuje, że pomimo potencjału współczesnych technologii nie są one w stanie zastąpić ich tradycyjnych odpowiedników, a obie te technologie nawzajem uzupełniają się. Zaprezentowane w koncepcji wyodrębnione technologie na podstawie analizy QFD w ocenie autora rozprawy stanowią istotną rolę w procesie informowania ludności o zagrożeniach, co nie oznacza, że pozostałe technologie są zbędne. Każda z zaproponowanych technologii możliwa jest do wykorzystania w procesie informowania ludności o zagrożeniach oraz w procesie kształtowania świadomości sytuacyjnej, dlatego też w dalszym etapie analizy zaproponowano schemat przypisania współczesnych (tab. 6.3) oraz tradycyjnych (tab. 6.4) technologii do jednego z trzech poziomów świadomości sytuacyjnej określonych przez M.R. Endsley (postrzeganie, zrozumienie, postrzeganie), aby określić, w którym momencie są one możliwe do wykorzystania.

Tabela 6.3. Możliwości wykorzystania współczesnych technologii w poszczególnych fazach świadomości sytuacyjnej

Poziom świadomości sytuacyjnej / Technologia	*IoT/IoE*	Smartfon - komunikaty o zagrożeniach	Sztuczna inteligencja - chatboty	Media społecznościowe	Informacje o zagrożeniach na ekranach wielkoformatowych	Informacje o zagrożeniach za pośrednictwem poczty e-mail	Informacje o zagrożeniach w środkach transportu	Informacje o zagrożeniach w miejscach publicznych
Postrzeganie	+	+		+	+	+	+	+
Zrozumienie	+	+	+	+	+	+	+	+
Prognozowanie	+	+	+	+	+	+	+	+

Źródło: opracowanie własne

W tabeli 6.3 zaprezentowano możliwe do wykorzystania współczesne technologie na poszczególnych poziomach świadomości sytuacyjnej (postrzeganie, zrozumienie, prognozowanie). Technologie możliwe do wykorzystania oznaczono symbolem „+". Warto zwrócić uwagę na fakt, że symbolem „+" oznaczono większość technologii. Wynika to z możliwości wykorzystania poszczególnych funkcji technologii przez członków ZZK oraz obywateli.

Tabela 6.4. Możliwości wykorzystania tradycyjnych technologii w poszczególnych fazach świadomości sytuacyjnej

Poziom świadomości sytuacyjnej / Technologia	Klasyczny telefon komórkowy - komunikaty o zagrożeniach	Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach)	Informacje o zagrożeniach za pośrednictwem poczty(list, telegram)	Poradniki w wersji papierowej	Szkolenia	Konferencje	Syreny alarmowe	Środki masowego przekazu (radio, telewizja)
Postrzeganie	+	+		+	+	+	+	+
Zrozumienie	+	+	+	+	+	+	+	+
Prognozowanie	+	+	+	+	+	+	+	+

Źródło: opracowanie własne

Zaprezentowane w tabeli 6.4 tradycyjne technologie tak jak w przypadku tabeli 6.3 oznaczono symbolem :+", wskazując na możliwości wykorzystania poszczególnych funkcji technologii przez członków ZZK oraz obywateli. W celu wizualizacji możliwości poszczególnych technologii zidentyfikowano funkcjonalność technologii, które zostały przedstawione w tabelach 6.5 i 6.6.

Tabela 6.5. Poziomy świadomości sytuacyjnej dla współczesnych technologii w procesie przygotowania się na zagrożenia

Wpływ wybranych atrybutów na POZIOMY ŚWIADOMOŚCI SYTUACYJNEJ / TECHNOLOGIE/wybrane atrybuty	POSTRZEGANIE	ZROZUMIENIE	PROGNOZOWANIE
IoT/IoE			
Monitorowanie zagrożeń i aktualnego stanu	+	+	+
Udostępnianie informacji		+	+
Pobieranie danych	+	+	+
Wykrywanie zagrożeń i otrzymywanie alertów	+	+	+
Identyfikacja zagrożeń	+	+	+
Sprawdzanie statusu siec np. energetycznej	+	+	+
Smartfon - komunikaty o zagrożeniach			
Alerty o zagrożeniach, np. RCB	+	+	+
Alerty o zagrożeniach, np. wiadomości z komunikatorów		+	+
Alerty o zagrożeniach, np. wiadomości ze stron internetowych	+	+	+
Alerty o zagrożeniach, np. wiadomości ze stron internetowych np. połączenia telefoniczne	+	+	+
Alerty o zagrożeniach z urządzeń *IoT/IoE* np. czujniki poziomu wody	+	+	+
Sztuczna inteligencja - chatboty			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+

Tabela 6.5. cd.. Poziomy świadomości sytuacyjnej dla współczesnych technologii w procesie przygotowania się na zagrożenia

Media społecznościowe			
Informacje o zagrożeniach za pośrednictwem mediów społecznościowych – posty	+	+	+
Informacje o zagrożeniach za pośrednictwem mediów społecznościowych – prywatne wiadomości	+	+	+
Informacje o zagrożeniach za pośrednictwem audycji wideo (youtube.pl, wykop.pl itp.)	+	+	+
Informacje o zagrożeniach na ekranach wielkoformatowych			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo – graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+
Informacje o zagrożeniach za pośrednictwem poczty e-mail			
Wiadomości na temat zagrożeń	+	+	+
Komunikaty na temat zagrożeń	+	+	+
Informacje o zagrożeniach w środkach transportu			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo – graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+
Informacje o zagrożeniach w miejscach publicznych			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo – graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+

Źródło: opracowanie własne

Tabela 6.6. Poziomy świadomości sytuacyjnej dla tradycyjnych technologii w procesie przygotowania się na zagrożenia

Wpływ wybranych atrybutów na POZIOMY ŚWIADOMOŚCI SYTUACYJNEJ / TECHNOLOGIE/wybrane atrybuty	POSTRZEGANIE	ZROZUMIENIE	PROGNOZOWANIE
Klasyczny telefon komórkowy – komunikaty o zagrożeniach			
Alerty o zagrożeniach np. RCB	+	+	+
Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach)			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami	+	+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej	+	+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach	+	+	+
Informacje o zagrożeniach za pośrednictwem poczty (list, telegram)			
Wiadomości tekstowe na temat zagrożeń			+
Poradniki w wersji papierowej			
Informacje o zagrożeniach	+	+	+
Informacje na temat zachowania się w sytuacjach kryzysowych	+	+	+
Szkolenia			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+
Konferencje			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+
Syreny alarmowe			
Analiza zagrożenia	+	+	+
Środki masowego przekazu (radio, telewizja)			
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Informacje na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+

Źródło: opracowanie własne

W tabelach 6.5 i 6.6 przedstawiono możliwości wykorzystania współczesnych i tradycyjnych technologii oraz określono, na którym poziomie świadomości sytuacyjnej i w jakim celu mogą być one wykorzystane. Na podstawie danych zwartych w tabeli można stwierdzić, że większość technologii możliwa jest do wykorzystania na wszystkich poziomach świadomości sytuacyjnej i mogą się one wzajemnie uzupełniać, co pokazują powtarzające się funkcje poszczególnych technologii oraz ich uniwersalność.

W celu oszacowania użyteczności współczesnych technologii w procesie usprawnienia działania służb ratowniczych oraz Zespołów Zarządzania Kryzysowego wykorzystano metodę QFD (rys 6.2). W tym celu do każdej z technologii, przypisano poziomy świadomości sytuacyjnej oraz atrybuty je uzupełniające:

Poziom 1 – postrzeganie:

- kompletność – stosunek ilości dostępnych informacji do całkowitej informacji ze świata rzeczywistego,
- przydatność – stopień, postrzegania otrzymanych informacji, czy jest ona wartościowa, czy nie,
- spójność – powiązanie starych informacji z nowymi,
- szczegółowość – jak najwięcej informacji na temat konkretnego zdarzenia,
- terminowość – dostępność informacji w określonym czasie

Poziom 2 – zrozumienie:

- przejrzystość – informacje jednoznaczne i przekazywane w taki sposób, aby te same dane dotarły to różnych odbiorców,
- użyteczność – ocena istotności informacji,
- adekwatność – właściwa prezentacja oraz opis informacji,
- relatywność – informacja spełnia oczekiwania odbiorcy,
- wiarygodność – informacja jest zweryfikowana, pochodzi z rzetelnego źródła,

Poziom 3 – postrzeganie:

- sprawność – zdolność do przesyłania określonej liczby informacji,
- dokładność – informacja odpowiada poziomowi wiedzy odbiorcy oraz wyczerpuje zaprezentowany temat,
- efektywność – przekazana informacja jest skuteczna i potrafi zwiększyć poziom świadomości,

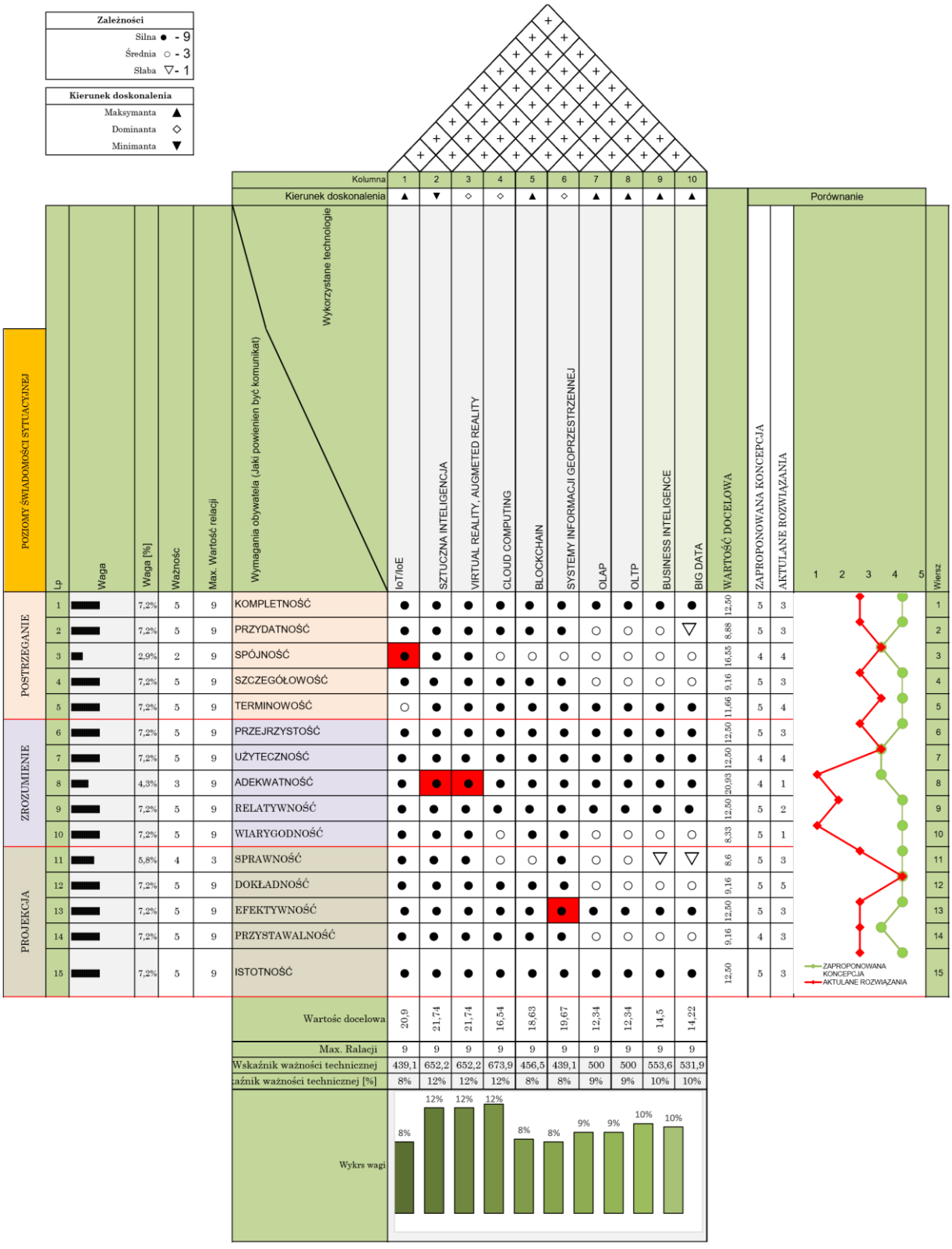
- przystawalność – przedstawienie informacji w sposób analogiczny do innej informacji,
- istotność – ocena, na ile przydatne są informacje.

W zaprezentowanym rozwiązaniu przedstawiono koncepcję udoskonalenia działania służb ratowniczych oraz Zespołów Zarządzania Kryzysowego. W tym celu poddano analizie aktualne rozwiązania przypisując im odpowiednio wagi od 1 do 5 określające poziom ważności cech komunikatu (1- bardzo niski, 2 – niski, 3 – średni, 4 – wysoki, 5 – bardzo wysoki). Na podstawie przypisanych zależności – kierunek doskonalenia (● – 9, ○ – 3 oraz ▽ – 1) możliwe było określenie najskuteczniejszych technologii w procesie doskonalenia działania służ ratowniczych oraz członków ZZK oraz jakie cechy powinny zawierać.

Na podstawie metody QFD wyodrębniono takie technologie jak:

- *IoT/IoE*
- sztuczna inteligencja
- *VR/AR*
- systemy informacji geoprzestrzennej

Następnie wyodrębniono istotne cechy dla tych technologii, które wg. kryterium analizy (najwyższe wartości) pozwoliły na określenie, która z technologii najlepiej sprawdzi się na jednym z trzech poziomów świadomości sytuacyjnej. Na tej podstawie ustalono, że technologia IoT/IoE ulokowana została w 1 poziomie świadomości sytuacyjnej – postrzegania i wyróżnia ją spójność. Technologie takie jak sztuczna inteligencja oraz *Virtual Reality, Augmented Reality* ulokowane zostały w 2 poziomie świadomości sytuacyjnej i charakteryzują się adekwatnością. Technologia taka jak Systemy informacji geoprzestrzennej ulokowane zostały na 3 poziomie świadomości sytuacyjnej i cechuje je efektywność. Zaprezentowana analiza QFD jednoznacznie pokazuje, jak duży potencjał mają współczesne technologie.



Rysunek 6.2. Możliwości wykorzystania współczesnych technologii w zarządzaniu kryzysowym w procesie doskonalenia działań służb ratowniczych oraz Zespołów Zarządzania Kryzysowego za pomocą analiz QFD

Źródło opracowanie własne

Proces wdrażania technologii to czynność złożona ze względu na dynamicznie rozwijające się sytuacje kryzysowe, w których istotną rolę odgrywa czas. Dlatego też technologie tego typu nie powinny zastępować obecnie używanych rozwiązań, ale stanowić dla nich alternatywę, tak aby możliwe było wykorzystanie tych aktualnie wykorzystywanych i sprawdzenie nowych w warunkach rzeczywistych po wcześniejszym sprawdzeniu ich w warunkach ćwiczeniowych.

Dla każdej technologii zawartej w analizie QFD (rys. 6.2) określone zostały możliwości jej wykorzystania oraz poziomy świadomości sytuacyjnej (tab. 6.7).

Tabela 6.7. Poziomy świadomości sytuacyjnej dla współczesnych technologii w procesie usprawnienia działania służb ratowniczych oraz Zespołów Zarządzania Kryzysowego

Wpływ poszczególnych atrybutów na POZIOM ŚWIADOMOŚCI SYTUACYJNEJ / TECHNOLOGIE/wybrane atrybuty	POSTRZEGANIE	ZROZUMIENIE	PROGNOZOWANIE
IoT/IoE			
Monitorowanie zagrożeń i aktualnego stanu	+		+
Udostępnianie informacji	+		+
Pobieranie danych	+		+
Wykrywanie zagrożeń i otrzymywanie alertów	+		+
Monitoring niezbędnych zasobów	+		+
Identyfikacja zagrożeń	+		+
Poszukiwanie poszkodowanych	+		
Sprawdzanie statusu siec np. energetycznej	+		
Sprawdzanie parametrów życiowych	+		
Wysyłanie alertów	+	+	+
Odbieranie alertów	+	+	+
Sztuczna inteligencja			
Robotyka(operacje ratowniczo-poszukiwawcze)	+		
Wymiana informacji	+	+	+
Pobieranie danych	+	+	+
Symulowanie zagrożeń	+	+	+
Tworzenie Chatbotów	+	+	+
Chatboty	+	+	+
VR/AR			
Symulowanie realistycznych zagrożeń	+	+	+
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	+	+	+
Tworzenie realistycznych szkoleń dla służb ratowniczych	+	+	+
Wyświetlanie nazw ulic, śledzenie służb ratowniczych	+		
Komunikacja głosowa	+	+	+
Lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar	+		
Nanoszenie obrazów 3D na rzeczywiste środowisko	+		+
Cloud Computing			
Hosting w chmurze	+		+
Dostęp do zasobów za pośrednictwem Internetu	+	+	+
Komunikacja z dowolnego miejsca	+	+	+
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	+	+	+
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	+	+	+
Blockchain			
Współpraca między interesariuszami zaangażowanymi w proces reagowania na katastrofy	+		+
Identyfikacja poszkodowanych i zmarłych	+	+	
Weryfikacja tożsamości	+	+	
Szyfrowanie danych	+		+
Rejestracja wolontariuszy	+		
Śledzenie dostaw	+		

Tabela 6.7. cd.. Poziomy świadomości sytuacyjnej dla współczesnych technologii w procesie usprawnienia działania służb ratowniczych oraz Zespołów Zarządzania Kryzysowego

Systemy informacji geoprzestrzennej			
Wizualizacja danych		+	+
Analiza danych	+	+	+
Pobieranie danych	+	+	+
Ocena ryzyka	+	+	+
Opracowanie strategii analizy ryzyka	+	+	+
Lokalizowanie ważnych punktów np. szpital, komisariat policji itp. Za pomocą zapytań *SQL*	+		
Szacowanie szkód	+	+	+
Ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli	+	+	+
Identyfikacja dróg ewakuacyjnych	+		
Tworzenie planów odbudowy	+		+
Odbieranie alertów	+	+	+
Analiza danych historycznych	+	+	+
Opracowanie scenariuszy sytuacji kryzysowych	+	+	+
Analiza skutków zagrożenia	+	+	+
Planowanie przyszłych działań	+		+
Zobrazowanie sytuacji kryzysowej	+	+	+
OLAP			
Analiza danych	+	+	+
Przechowywanie danych			+
Eksploracja danych			+
Tworzenie raportów			+
Zobrazowanie danych		+	+
OLTP			
Współbieżność	+	+	+
Indeksowanie zbiorów danych	+	+	+
Pobieranie danych	+		+
Wyszukiwania i zapytania w bazie danych	+		+
Tworzenie kopii zapasowych	+	+	+
Monitorowanie sytuacji kryzysowych	+	+	+
Zabezpieczenie danych	+		+
Monitorowanie danych	+	+	+
Raportowanie i wsparcie procesów decyzyjnych	+	+	+
Business Inteligence			
Analiza danych	+	+	+
Kontrola dostępu do danych	+		
Raportowanie i wizualizacja danych	+	+	+
Monitorowanie zagrożeń	+		+
Podejmowanie decyzji	+	+	+
Przetwarzanie danych	+	+	+
Wymiana informacji	+	+	+
Analiza danych historycznych	+	+	+
Filtrowanie, sortowanie i grupowanie danych	+	+	+
Big Data			
Identyfikacja i śledzenie populacji	+		+
Mapowanie sytuacji kryzysowych	+		
Gromadzenie danych i modelowanie scenariuszy zagrożeń	+		+
Lokalizacja zasobów	+		+
Wysyłanie informacji o zagrożeniach	+		
Analiza danych	+		+
Planowanie przyszłych działań	+		+

Źródło opracowanie własne.

W tabeli 6.7 zaprezentowano technologie takie jak BI/OLTP/OLAP/DM, IoT/IoE, *Big Data*, AI, *VR/AR*, CC, *Blockchain* oraz możliwości ich wykorzystania w procesie usprawnienia działań służb ratowniczych oraz Zespołów Zarządzania Kryzysowego. Każdej z technologii uwzględnionej w tabeli 6.7 przypisano możliwości ich wykorzystania na poszczególnych poziomach świadomości sytuacyjnej. Tabela 6.7 pokazuje jak, duży potencjał mają te technologie niemniej jednak zanim zostaną one wdrożone istotne jest to, aby dla osób, dla których są one przeznaczone, były zrozumiałe. Dlatego też niezbędne jest wyznaczenie osób odpowiedzialnych za ob-

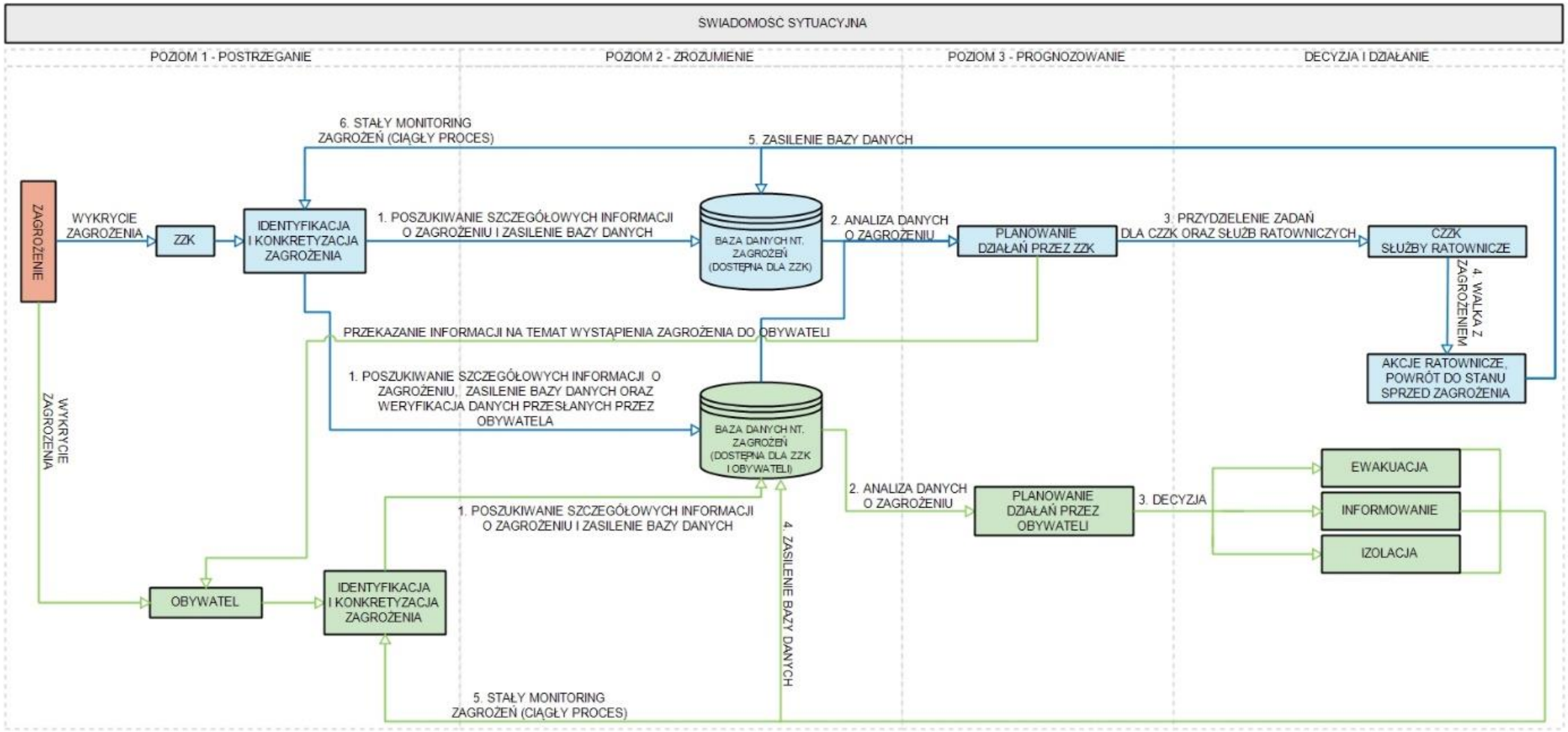
sługę wspomnianych technologii w aspekcie technicznym, tak, aby pracownicy Zespołów Zarządzania Kryzysowego otrzymali zrozumiały dla nich interfejs, za pośrednictwem, którego są w stanie posługiwać się zaproponowanymi technologiami oraz aby były one zrozumiałe dla obywateli. Należy zwrócić uwagę na fakt, że samo wdrożenie technologii może okazać się niewystarczające bez odpowiedniego przeszkolenia w zakresie ich wykorzystania, określania do kogo są skierowane poszczególne technologie oraz ich funkcje (obywatel, służby ratownicze, członkowie zespołów zarządzania kryzysowego) oraz wskazania urządzeń niezbędnych do ich wykorzystania.

6.4. Obszary i zalecenia doskonalenia systemu kształtowania świadomości sytuacyjnej

Zaproponowana koncepcja doskonalenia systemu kreowania świadomości sytuacyjnej ludności wskazuje na możliwości wzrostu poziomu świadomości sytuacyjnej zarówno osób funkcyjnych ZZK jak i obywateli Wdrożenie koncepcji pozwoli na znaczne usprawnienie procesu informowania ludności o zagrożeniach oraz lepsze przygotowanie członków ZZK oraz służb ratowniczych na zagrożenia.

Z przeprowadzonych analiz wynika, że najistotniejszy wpływ na zwiększenie świadomości sytuacyjnej mają takie technologie jak: IoT/IoE, sztuczna inteligencja, systemy informacji geoprzestrzennej oraz VR/AR. Omówione w rozprawie technologie i potencjalne możliwości ich wykorzystania w znaczonym stopniu mogą przyczynić się do wzrostu skuteczności działań zespołów zarządzania kryzysowego, służb ratowniczych oraz obywateli. Zaproponowana w koncepcji klasyfikacja zagrożeń oraz tabela niezbędnych zasobów może być wykorzystywana niezależnie od zastosowanych technologii i będzie miała istotny wpływ na poprawę świadomości sytuacyjnej obywateli.

Ponadto zaprezentowane w koncepcji analizy dla różnych perspektyw wskazują jednoznacznie, które dostępne technologie wpływają na poszczególne poziomy świadomości sytuacyjnej. Wśród zaprezentowanych technologii trudno jednoznacznie wskazać jedną konkretną stanowiącą rozwiązanie wszystkich problemów. Przeprowadzona analiza wskazuje jednak na potrzebę wdrażania każdej wykorzystywanej technologii stosownie do potrzeb i możliwości działania poszczególnych podmiotów. Z uwagi na szybki rozwój technologii zaproponowano również koncepcję doskonalenia istniejącego systemu kreowania świadomości sytuacyjnej ludności oraz ZZK (rys. 6.3).



Rysunek 6.3. Koncepcję doskonalenia systemu kreowania świadomości sytuacyjnej ludności oraz ZZK.

Źródło: opracowanie własne

Przedstawiona na rysunku 6.3 koncepcja doskonalenia systemu kreowania świadomości sytuacyjnej ludności podzielona została na 4 etapy stanowiące 3 poziomy świadomości sytuacyjnej (postrzeganie, zrozumienie oraz prognozowanie) oraz etap decyzji i działania.

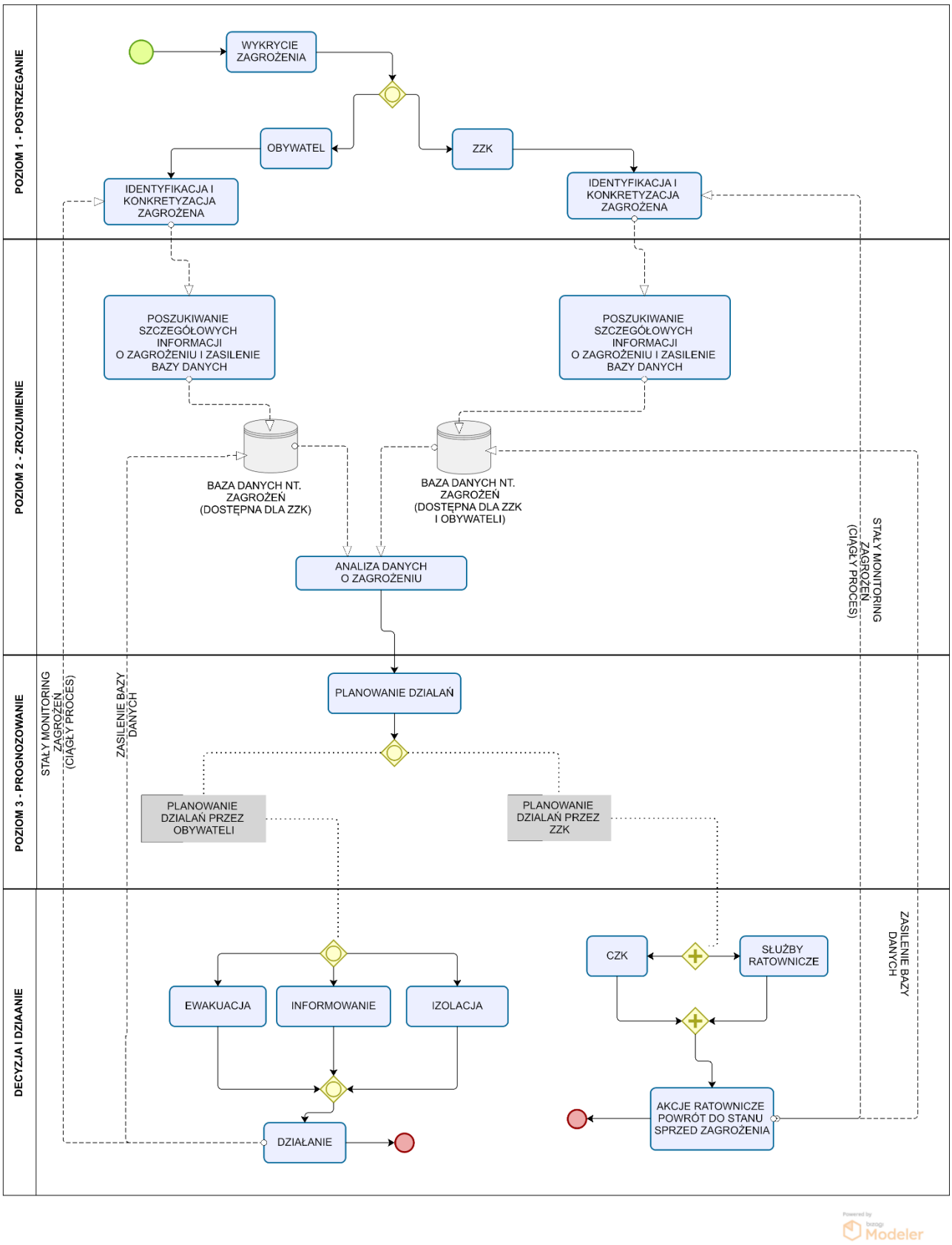
W pierwszej fazie (postrzeganie) w momencie wystąpienia zagrożenia następuje jego wykrycie przez obywateli lub ZZK, którzy dokonują jego identyfikacji i konkretyzacji.

Druga faza (zrozumienie) związana jest z poszukiwaniem przez obywateli oraz ZZK informacji na temat zagrożeń. Bazy danych dla Obywateli oraz ZZK różnią się od siebie ze względu na fakt, że baza z danymi przeznaczonymi dla obywateli nie zawiera danych dostępnych wyłącznie członków Zespołów Zarządzania Kryzysowego oraz służb ratowniczych.

W fazie trzeciej (prognozowanie) podejmowane są decyzje zarówno przez obywateli jak i przez ZZK. W przypadku Zespołów Zarządzania Kryzysowego decyzje te dotyczą zarówno przydzielenia zadań służbom ratowniczym jak i obywatelom jeśli nie wykryli oni dotychczas zagrożenia. Obywatele, którzy nie byli w stanie samodzielnie wykryć zagrożenia identyfikują je przechodząc przez wszystkie fazy uwzględnione na schemacie.

W fazie czwartej (decyzja i działanie) podejmowane są działania zapobiegawcze oraz przeprowadzana jest akcja ratownicza zmierzająca do zniwelowania skutków zagrożeń, a także następuje powrót do funkcjonowania sprzed jego wystąpienia. W przypadku obywatela faza ta związana jest z podjęciem decyzji o ewakuacji, informowaniu lub izolacji w zależności od tego jakiego działania wymaga zagrożenie (tab. 6.1). Faza ta stanowi również uaktualnienie bazy danych na temat zagrożeń. Warto zwrócić również uwagę na fakt, że zagrożenia muszą być stale monitorowane co stanowi istotę świadomości sytuacyjnej.

Opracowana koncepcja uwzględnia sposób postępowania zarówno osób funkcyjnych w ZZK jak i obywateli. W celu implementacji koncepcji w informatycznych systemach modelowania procesów biznesowych przedstawiono również koncepcję w postaci procesu identyfikowanego w środowisku BPMN, który zobrazowuje sposoby przygotowania się i działania ZZK i obywateli na wypadek wystąpienia zagrożenia (rys. 6.4).



Rysunek 6. 4. Proces doskonalenia systemu kreowania świadomości sytuacyjnej ludności.

Źródło: opracowanie własne

Zaprezentowany proces ten tak jak i koncepcja składa się z 4 etapów:

- poziom 1 – postrzeganie związany jest z wykryciem identyfikacją zagrożeń przez obywateli oraz ZZK.
- poziom 2 – zrozumienie dotyczy poszukiwania szczegółowych informacji na temat zagrożeń, co możliwe jest m.in. dzięki dostępowi do danych z czujników (technologia IoT), danych historycznych itp.
- poziom 3 – prognozowanie związany z planowaniem działań zapobiegawczych.
- decyzja i działanie – etap związany z przydzieleniem zadań i przeprowadzeniem akcji ratowniczych. Ponadto w przypadku obywateli decyzję o ewakuacji, informowaniu lub izolacji określa tabela 6.2, dzięki której możliwe szczegółowe określenie niezbędnych kroków. W fazie tej możliwa jest również aktualizacja danych na temat zagrożeń. Ponadto warto zwrócić uwagę na fakt, że do skutecznego zarządzania kryzysowego niezbędne jest stałe monitorowanie zagrożeń, co zawarte zostało w etapie działanie/decyzja.

Odpowiednie wsparcie obywateli w zakresie radzenia sobie z sytuacjami kryzysowymi wydaje się zatem niezbędne. Zasadne jest więc wprowadzenie klasyfikacji zagrożeń oraz dostosowanie technologii do potrzeb obywateli członków zespołów zarządzania kryzysowego i służb ratowniczych.

Rozdział VI pracy poświęcony został przedstawieniu założeń i ograniczeń koncepcji doskonalenia systemu kreowania świadomości sytuacyjnej ludności z uwzględnieniem potencjału współczesnych i tradycyjnych technologii w informowaniu o zagrożeniach i procesie kształtowania świadomości sytuacyjnej. wśród członków zespołów zarządzania kryzysowego, służb ratowniczych i obywateli. Rozdział ten zawiera zatem koncepcję wykorzystania współczesnych i tradycyjnych technologii zmierzających do zapewnienia ciągłości działania w sytuacjach kryzysowych poprzez wykorzystanie potencjału technologii, która możliwa jest do wykorzystania w procesie informowania o zagrożeniach, monitorowania zagrożeń, zabezpieczenia i przechowywania informacji, gromadzenia danych, usprawnienia działań służb o członków ZZK oraz zwiększania świadomości sytuacyjnej na temat potencjalnych niebezpiecznych zjawisk wśród osób zaangażowanych w zarządzanie kryzysowe, a także obywateli.

Przedstawione w koncepcji rozwiązania wyznaczają kierunek rozwoju Systemu Zarządzania Kryzysowego w celu usprawnienia jego funkcjonowania. Dlatego też efektywne wykorzystanie zarówno tradycyjnych jak i współczesnych technologii ułatwia przygotowanie się na zagrożenia oraz przyśpiesza czas reakcji na nie, co z kolei zwiększa bezpieczeństwo obywateli oraz usprawnia działanie służb ratowniczych oraz Zespołów Zarządzania Kryzysowego.

W koncepcji wskazano możliwe do wykorzystania technologie zarówno przez obywateli jak i członków zespołów zarządzania kryzysowego w tym służby ratownicze. Istotne zatem jest określenie możliwości wykorzystania poszczególnych technologii przez interesariuszy zaangażowanych w zarządzanie kryzysową oraz biorących w niej udział:

1. **Internet Rzeczy**
    a. **Obywatele**

Analiza technologii zaprezentowanych w koncepcji pozwala zauważyć, że wykorzystanie Internetu Rzeczy przez obywateli może przyczynić się do usprawnienia procesu podejmowania decyzji w czasie rzeczywistym poprzez odbieranie komunikatów z czujników IoT takich jak np. czujniki poziomu wody, czujniki dymu, zanieczyszczeń itp., a także poprzez obserwacje terenu przy wykorzystaniu takich rozwiązań jak np. drony czy monitoring. Warto również zwrócić uwagę na fakt, że informacje zbierane przez czujniki gromadzone są w formie danych historycznych, co umożliwia skuteczną analizę i lepsze przygotowanie na ewentualne przyszłe zagrożenia oraz ułatwia wykrywanie zagrożeń. Ponadto wykorzystanie technologii IoT daje możliwość obywatelom ciągłego monitorowania parametrów życiowych i kontrolę stanu sieci elektrycznej.

    b. **Zespoły Zarządzania Kryzysowego i służby ratownicze**

Zaproponowane w koncepcji rozwiązania dotyczące możliwości wykorzystania IoT wskazują na ogromny potencjał wymienionej technologii, dzięki której zarówno ZZK jak i służby ratownicze mogą w czasie rzeczywistym monitorować stan środowiska i sytuacji kryzysowej za pośrednictwem danych zebranych z czujników temperatury, wilgotności, czujniki dymu i czujniki zanieczyszczeń powietrza, wiatru i deszczu itp. Ponadto jak wspomniano w koncepcji zastosowanie technologii Internetu rzeczy umożliwia śledzenia lokalizacji pojazdów, sprzętu ratowniczego i personelu, co pozwala na bardziej efektywne zarządzanie zasobami i lepszą koordynację działań, zdalne monitorowanie i zarządzanie urządzeniami, organizowanie wideokonferencji

i komunikacji w czasie rzeczywistym między zespołami zarządzania kryzysowego, służbami ratowniczymi i innymi podmiotami zaangażowanymi w sytuację kryzysową, a także przesyłanie danych do chmur obliczeniowych, zarządzanie dostawami i dystrybucją pomocy humanitarnej, zdalną inspekcję obszarów dotkniętych kryzysem, co pozwala na ocenę szkód i potrzeb rekonstrukcji (drony), Ponadto wykorzystanie technologii IoT umożliwia zdalne sterowanie i dostarczanie informacji o sytuacji kryzysowej oraz pomoc poszkodowanym za pomocą specjalistycznych robotów, utrzymanie łączności awaryjnej.

2. Syreny alarmowe

a. Obywatele

Syreny alarmowe stanowią jedno z najważniejszych rozwiązań w procesie informowania o zagrożeniach, a za ich pośrednictwem przekazywane są alarmy na temat:

- klęsk żywiołowych i zagrożeniach środowiska (dźwięk ciągły trwający 3 minuty),
- zagrożeń powietrznych – alarm przeciwlotniczy (dźwięk modułowy trwający 3 minuty),
- skażeń (dźwięki trwające 10 sekund powtarzany przez 3 minuty; czas trwania przerwy między dźwiękami 25-30 sekund).

Pomimo iż syreny alarmowe stanowią nieodłączna część zarzadzania kryzysowego, przeprowadzone w rozprawie badania ankietowe wskazały na potrzebę zwiększenia form informowania o znaczeniu syren alarmowych wykorzystując takie technologie jak m.in. poradniki w wersji papierowej, poradniki w formie aplikacji na urządzenie typu smartfon lub tablet, strony internetowe z poradnikami na temat zagrożeń, informacje na temat syren alarmowych za pośrednictwem ekranów wielkoformatowych, szkolenia i konferencje z materiałami zawierającymi tego typu informacje oraz udostępnione informacje radiu, telewizji i mediach społecznościowych. Wynika to z faktu, że wśród obywateli są osoby, które są w stanie rozpoznać znaczeń tego typu dźwięków.

Odpowiedzialność przygotowania niezbędnych materiałów w zakresie informowania ludności o zagrożeniach spoczywa na ZZK, które powinno określić odpowiednie formy przekazu i opracować odpowiednie poradniki i szkolenia dla obywateli.

3. GIS

a. Obywatele

W przypadku rozwiązań dla obywateli takich jak GIS należy zwrócić uwagę na fakt, że zastosowanie tego typu rozwiązania może usprawnić proces podejmowania decyzji na podstawie map zagrożeń, pogodowych oraz otrzymanych danych w tym również otrzymanych za pośrednictwem nawigacji na smartfony, która pozwala nie tylko na unikanie zatłoczonych ulic ale również na odnalezienie istotnych punktów takich jak miejsca zbiórek szpitale itp.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Jak wspomniano w koncepcji wykorzystanie technologii Systemów Informacji Geoprzestrzeszennej przez ZZK i służby ratownicze umożliwia opracowanie szczegółowych planów ewakuacji, uwzględniających topografię, dostępność dróg i lokalizację schronień. Plany te mogą zostać wykorzystane do efektywnego kierowania ewakuacją ludności w czasie kryzysu; monitorowania zagrożeń naturalnych poprzez tworzenie map interaktywnych, które prezentują bieżącą sytuację i ostrzeżenia; oceny skutków kryzysu takich jak zniszczenia budynków, obszarów zalanych lub obszarów pożarów, co daje możliwość określenia priorytetów i kierowania działań ratowniczych tam, gdzie są najbardziej potrzebne; koordynacji działań między różnymi zespołami zarządzania kryzysowego oraz służbami ratowniczymi poprzez dostarczanie wspólnej platformy do wymiany informacji i danych przestrzennych; przeprowadzania symulacji i szkoleń, które pomagają służbom zarządzania kryzysowego oraz obywatelom przygotować się do różnych scenariuszy kryzysowych; uaktualniania danych w czasie rzeczywistym; analizy trendów i prognozowania rozwoju sytuacji kryzysowej, co pomaga w podejmowaniu długofalowych decyzji i planowaniu działań na przyszłość.

4. Sztuczna Inteligencja

a. Obywatele

Wykorzystanie potencjału sztucznej inteligencji może również przyczynić się do zwiększenia poziomu świadomości sytuacyjnej. Wykorzystanie takiej technologii jak sztuczna inteligencja nie tylko pozwala na wygenerowanie informacji o zagrożeniu oraz sposobie radzenia sobie z nim, ale również na udzielanie odpowiedzi w czasie rzeczywistym przez chatboty głosowo – tekstowe co omówiono w rozdziale koncepcyjnym.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Jak wspomniano w rozdziale koncepcyjnym sztuczna inteligencja ma potencjał do znacznego zwiększenia efektywności i skuteczności działań zespołów zarządzania kryzysowego oraz służb ratowniczych, a jej zastosowanie umożliwia analizowanie ogromnej ilości danych pochodzących z różnych źródeł, takich jak kamery, czujniki, media społecznościowe czy systemy monitorowania, wykorzystanie danych historycznych i bieżących do prognozowania rozwoju sytuacji kryzysowej, co pozwala na: wcześniejsze ostrzeganie i lepsze planowanie działań zmierzających do zażegnania sytuacji kryzysowej; automatyczne rozpoznawanie obrazów i analizę wideo np. identyfikacja obszarów zniszczonych w wyniku katastrofy naturalnej lub do śledzenia ruchu ludzi w obszarze ewakuacji; monitorowanie danych z czujników i kamer; automatyczne generowanie alertów i ostrzeżeń w przypadku wykrycia niebezpieczeństwa lub nieprawidłowości, co umożliwia natychmiastową reakcję służb ratowniczych; ocenę ryzyka i bezpieczeństwa w danym regionie dzięki czemu możliwe jest usprawnienie działań; automatyzowanie rutynowych procesów, co pozwala na skoncentrowanie się na zadaniach wymagających ludzkiego rozsądku i kreatywności np. stosowanie robotów do dostarczania pomocy humanitarnej w trudno dostępne miejsca; analizowanie treści generowanych przez obywateli w mediach społecznościowych, co pozwala na śledzenie reakcji na sytuację kryzysową oraz identyfikowanie miejsc, gdzie pomoc jest najbardziej potrzebna; generowanie scenariuszy zagrożeń, określenie prawdopodobieństwa wystąpienia zagrożenia; określenie możliwego kierunku rozwoju zagrożenia oraz ocenę wpływu kryzysów na zdrowie psychiczne ludzi, co pozwala na dostarczenie odpowiedniego wsparcia psychologicznego.

5. Telefon

a. Obywatele

Wśród zaprezentowanych rozwiązań należy wyróżnić takie rozwiązanie jak telefon stacjonarny, klasyczny telefon komórkowy orz smartfon. W przypadku telefonu stacjonarnego i klasycznego telefonu komórkowego (odbieranie alertów w tym RCB) pomimo iż, są one coraz częściej zastępowane przez Smartfon to rozwiązanie to mimo wszystko jest nadal używane przez niektórych obywateli. Możliwość dotarcia do jak największej liczby odbiorców oraz poinformowanie ich o zagrożeniu i zwiększenie ich poziomu świadomości sytuacyjnej na temat zagrożeń stanowi jedno z najważniejszych zadań w czasie sytuacji kryzowej, dlatego też nie należy rezygnować z funkcjonalności wspomnianych rozwiązań. Wykorzystanie telefonu niezależnie

od jego rodzaju umożliwia kontakt z wirtualnym asystentem, który odpowiednio przygotowany udzieli odpowiedzi na pytania z zakresu zarządzania kryzysowego.

Smartfon również posiada funkcjonalność taką jak jego poprzedniki, a rozwój technologiczny spowodował, że został on rozbudowany o dodatkowe funkcje, które dają możliwość: wyszukiwania informacji o zagrożeniach za pomocą stron internetowych; skorzystania z funkcji chatbotów w formie tekstowej; dostępu do poradników na temat zagrożeń które przyjmują formę aplikacji dedykowanej na urządzenia mobilne. Ponadto funkcjonalność Smartfonów pozwala na dostęp do danych otrzymywanych za pośrednictwem aplikacji wspomagających wykorzystanie czujników IoT w zależności od rodzaju czujnika. Dzięki wspomnianym aplikacjom możliwe jest otrzymywanie alertów na temat zagrożeń poprzez zebranie danych z dedykowanych czujników tj. czujniki wody, skażeń dymu monitorowanie zagrożeń dane z kamer itp. Co istotne smartfony umożliwiają również komunikację głosowo tekstową za pośrednictwem komunikatorów oraz umieszczenie wpisów na temat zagrożeń w mediach społecznościowych.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Telefony stanowią niezwykle ważne narzędzie dla zespołów zarządzania kryzysowego i służb ratowniczych. Dzięki nim możliwa jest komunikacja w czasie rzeczywistym między interesariuszami odpowiedzialnymi za zarządzanie kryzysowe, szybkie informowanie obywateli o zagrożeniach i instrukcjach dotyczących zachowania w przypadku kryzysu, monitorowanie sytuacji, zarządzanie danymi i koordynowanie działań, dostęp do dokumentów, map, planów ewakuacji i innych informacji kryzysowych w czasie rzeczywistym, co ułatwia podejmowanie decyzji opartych na aktualnych danych, diagnozowanie i udzielanie pierwszej pomocy. Ponadto możliwości wykorzystania telefonów w sytuacjach kryzysowych pozwalają na dokumentowanie sytuacji na miejscu zdarzenia, co jest przydatne w celach analizy, dokumentacji i raportowania. Telefony komórkowe, stacjonarne oraz Smartfony umożliwiają również kontakt z mediami oraz komunikację z lokalną społecznością w celu dostarczenia informacji, zarządzanie dostawami medycznymi, żywnością i innymi zasobami w sytuacjach kryzysowych. W rozprawie zwrócono również uwagę na fakt, że możliwości Smartfonów pozwalają na stworzenie przez ZZK dedykowanych aplikacji mających na celu przygotowanie społeczeństwa na zagrożenia poprzez opracowanie poradników dzięki, którym możliwe jest zwiększenie ich świadomości sytuacyjnej na temat zagrożeń. Co ważne wykorzystanie Smartfonów daje możliwość dostępu do danych

w czasie rzeczywistym z dowolnego miejsca oraz odbieranie i przesyłanie danych z czujników w czasie rzeczywistym i przekazywanie ich ZZK oraz służbom ratowniczym. Ponadto aparaty w telefonach komórkowych pozwalają na dokumentowanie sytuacji na miejscu zdarzenia, co jest przydatne w celach analizy, dokumentacji i raportowania, a także w fazie odbudowy.

6. Media społecznościowe

a. Obywatele

Media społecznościowe stanowią w ostatnim czasie jedno z najpopularniejszych źródeł przesyłania i odbierania informacji na różnorodne tematy. Niemniej jednak dane udostępnione za ich pośrednictwem nie zawsze są wiarygodne, a zespoły zarządzania kryzysowego nie mają wglądu do wszystkich danych udostępnianych za ich pośrednictwem w tym do danych, które obywatele przesyłają w formie prywatnych wiadomości. Niemniej jednak utworzenie oficjalnych kanałów informacyjnych w mediach społecznościowych takich jak np. Facebook, Twitter, Instagram itp. może uwiarygodnić przekazywane w cyberprzestrzeni informacje. Przyjęcie tego typu rozwiązania umożliwia obywatelom dostęp do danych w czasie rzeczywistym, a także możliwość uzyskania informacji o zagrożeniach poprzez materiały szkoleniowe, poradniki itp. utworzone i udostępnione na specjalnych kanałach informacyjnych.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Media społecznościowe stanowią ważne narzędzie komunikacji i zarządzania informacją dla służb ratowniczych i zespołów zarządzania kryzysowego i możliwiają szybkie publikowanie informacji o sytuacjach kryzysowych, zagrożeniach lub ostrzeżeniach, co pozwala na dotarcie do szerokiego grona odbiorców w krótkim czasie. Służby ratownicze i zespoły zarządzania kryzysowego mogą wykorzystywać media społecznościowe do komunikacji z mieszkańcami i społecznością lokalną. Wykorzystanie tego typu rozwiązania umożliwia dostarczenie informacji na temat ewakuacji, punktów schronień, dostępnych usług i pomocy. Ponadto wykorzystanie mediów społecznościowych przez służby ratownicze i ZZK umożliwia przekazywanie wiarygodnych informacji obywatelom, a także monitorowanie reakcji społeczności na sytuacje kryzysowe. Służby ratownicze mogą uzyskać informację na temat tego, gdzie potrzebne są dodatkowe środki i wsparcie oraz jakie są główne obawy mieszkańców. Media społecznościowe pozwalają również na dokumentowanie sytuacji na miejscu zdarzenia poprzez udostępnianie zdjęć i wideo oraz relacjonowanie wydarzeń na

żywo, co może znacząco ułatwić podejmowanie decyzji służbom ratowniczym oraz ZZK.

7. Poradniki w wersji papierowej

a. Obywatele

Poradniki w wersji papierowej to rozwiązanie coraz częściej wypierane przez ich elektroniczne odpowiedniki udostępniane za pomocą stron internetowych lub aplikacji mobilnych. Badania ankietowe przeprowadzone w rozprawie wykazały, że pomimo postępu technologicznego istnieje potrzeba skorzystania również z tej formy przekazu informacji ze względu na fakt, że wśród obywateli można wyróżnić osoby preferujące tego typu rozwiązania, osoby starsze, które nie przystosowały się do współczesnych technologii, a także jako rozwiązanie zapobiegawcze na wypadek braku dostępu do sieci internetowej i energetycznej. Wskazane rozwiązanie wymaga oczywiście przygotowania odpowiednich informacji na temat najczęściej występujących zagrożeń, sposobów radzenia sobie z nimi. Ponadto do tego typu rozwiązań mogą zostać wykorzystane zaproponowane w rozdziale koncepcyjnym klasyfikacja zagrożeń (tab. 6.1) oraz przykładowa tabela zasobów istotnych z punku widzenia obywatela w sytuacjach kryzysowych (tab. 6.2). Należy jednak pamiętać, że przekazywane informacje powinny być krótkie i zawierać najważniejsze informacje, ponieważ duża ilość treści może okazać się nie zrozumiała dla obywateli lub zniechęcić ich do czytania.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Poradniki w wersji papierowej umożliwiają Zespołom Zarządzania Kryzysowego orz służbom ratowniczym zapoznanie się z zasadami działania współczesnych i tradycyjnych technologii możliwych do wdrożenia do skutecznego zarządzania kryzysowego, co pozwala na lepsze przygotowanie się na zagrożenia oraz zwiększenie świadomości sytuacyjnej na ich temat. Poradniki te różnią się od poradników dla obywateli ze względu na fakt, że opisane w poradnikach zagrożenia powinny być znane służbom ratowniczym oraz członkom ZZK zważywszy na fakt, że osoby te odpowiadają za przygotowanie materiałów dla obywateli.

8. Szkolenia i konferencje

a. Obywatele

Rozwiązania takie jak szkolenia i konferencje dają możliwość zapoznania obywateli nie tylko z rodzajem zagrożeń i sposobami radzenia sobie z nimi w tym edukowanie najmłodszej grupy obywateli (dzieci w szkołach), ale również daje moż-

liwość zapoznania obywateli z technologiami możliwymi do wykorzystania w celu zwiększenia świadomości sytuacyjnej na temat zagrożeń, a podczas szkoleń i konferencji zaprezentowane mogą zostać wszystkie możliwe do wykorzystania technologie co umożliwia obywatelom wybranie najbardziej odpowiedniej technologii.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Tak jak w przypadku poradników w wersji papierowej szkolenia i konferencje ułatwiają przyswojenie nowo wdrażanych technologii. Ponadto udział w szkoleniach i konferencjach przez ZZK oraz służby ratownicze umożliwia lepsze przygotowanie się na zagrożenia oraz wymianę doświadczeń pomiędzy różnymi interesariuszami zaangażowanymi w zarządzanie kryzysowe.

9. Megafony

a. Obywatele

Wykorzystanie megafonów w sytuacjach kryzysowych to jedna z najprostszych i najskuteczniejszych form przekazywania krótkich informacji o zbliżających się zagrożeniu zarówno przed jego wystąpieniem jak i w trakcie trwania. Dane przekazywany za ich pośrednictwem są aktualne pochodzą z wiarygodnego źródła i mogą zawierać kluczowe informacje na temat zagrożenia tj. jak się na nie przygotować jak sobie z nim radzić oraz jakie środki ostrożności należy podjąć w konkretnej sytuacji.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Odpowiedzialność za przygotowanie treści komunikatów dla obywateli.

10. Środki masowego przekazu (radio i telewizja)

a. Obywatele

Tak jak w przypadku megafonów dane przekazywane za pośrednictwem radiofonii i telewizji mogą zawierać kluczowe informacje na temat zagrożeń. Ponadto wykorzystanie potencjału wspomnianych technologii umożliwia wprowadzenie specjalnych audycji i reklam na temat zagrożeń w celu skuteczniejszego przygotowania obywateli na nie w przyszłości.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Odpowiedzialność za przekazywanie informacji, aby były przekazywane w czasie rzeczywistym oraz zweryfikowane.

11. Ekrany wielkoformatowe

a. Obywatele

Odbieranie informacji na temat zagrożeń na ekranach wielkoformatowych w formie graficzno-tekstowej oraz alertów RCB.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Od 2022 na mocy umowy zawartej przez *Screen Network S.A* oraz Rządowe Centrum Bezpieczeństwa jako jedną z form przekazywania alertów RCB na temat zagrożeń przyjęto ekrany wielkoformatowe. Rozszerzenie funkcjonalności tej technologii o kluczowe informacje na temat zagrożeń tj. krótkie poradniki w formie graficzno-tekstowej jest w stanie zwiększyć świadomość sytuacyjną obywateli na ich temat. Obowiązek przygotowania tego typu informacji spoczywa na wyznaczonych przez ZZK interesariuszom zaangażowanym w zarządzanie kryzysowe.

12. Informacje o zagrożeniach w miejscach publicznych oraz w transporcie publicznym

a. Obywatele

Wykorzystanie potencjału ekranów umieszczonych w środkach transportu publicznego na stacjach metrach, przystankach autobusowo – tramwajowych oraz wielkich banerów reklamowych umożliwia kreowanie świadomości sytuacyjnej obywateli na temat zagrożeń poprzez wczesne ostrzeganie o możliwości ich wystąpienia za pośrednictwem krótkich poradników na temat zagrożeń prezentujących rodzaje zagrożeń oraz sposoby radzenia sobie z nimi.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Odpowiedzialność za przygotowanie treści komunikatów oraz poradników dla obywateli.

13. VR/AR

a. Obywatele

Wirtualna rzeczywistość może być wykorzystywana do edukacji obywateli w zakresie postępowania w przypadku zagrożeń. Dzięki interaktywnym wirtualnym lekcjom, obywatele mogą zdobyć wiedzę na temat procedur ewakuacji, udzielania pierwszej pomocy i innych kluczowych umiejętności. Ponadto w przypadku obywateli wirtualna rzeczywistość może być również używana do terapii i wsparcia psychologicznego dla osób dotkniętych kryzysem. Obywatele mogą uczestniczyć w sesjach terapeutycznych w wirtualnym środowisku, co może pomóc im radzić sobie ze stresem i traumą. Aplikacje AR mogą dostarczać użytkownikom wskazówek nawigacyjnych na ekranach ich urządzeń mobilnych, co może być szczególnie przydatne podczas ewakuacji z obszaru zagrożonego kryzysem. VR może wzbogacać te wska-

zówki o bardziej immersyjne doświadczenie. Ponadto obywatel korzystający z technologii AR mogą za pośrednictwem specjalistycznych okularów otrzymywać informacje na temat kryzysu, takie jak ostrzeżenia o pogodzie, alerty itp.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

W koncepcji przedstawiono potencjał wykorzystania wirtualne rzeczywistości (VR) i rozszerzonej rzeczywistości (AR), której potencjał może znacząco usprawnić działanie służb ratowniczych oraz ZZK. Jak wspomniano w rozdziale zastosowanie tej technologii umożliwia przeprowadzenie szkoleń i symulacji, które pozwalają zespołom zarządzania kryzysowego i służbom ratowniczym na praktyczne przygotowanie do różnych scenariuszy kryzysowych; zdalną komunikację z osobami na miejscu zdarzenia; pomoc w nawigacji na obszarze dotkniętym kryzysem, wskazując najlepsze trasy ewakuacji; lokalizacje schronienia czy punkty medycznej pomocy, współpracę na odległość co jest szczególnie przydatne w przypadku rozproszonych zespołów (komunikacja głosowa, wideokonferencje); wizualizację danych; zbieranie danych terenowych (ocena skali szkód oraz koordynacja działań); zarządzanie zasobami, takimi jak transport, zaopatrzenie medyczne i personel ratowniczy, poprzez wizualizację dostępności i lokalizacji tych zasobów.

14. Cloud Computing

a. Obywatele

Dzięki wykorzystaniu Cloud Computing eliminuje się wykluczenia informatyczne, a obywatele mogą uzyskiwać dostęp do aktualnych informacji na temat sytuacji kryzysowej za pośrednictwem aplikacji mobilnych lub stron internetowych opartych na chmurze. Za pośrednictwem Cloud Computing obywatele mogą otrzymywać powiadomienia i alerty dotyczące ewakuacji, zagrożeń pogodowych czy innych sytuacji. Ponadto chmura może zawierać mapy ewakuacyjne, które mogą zostać wykorzystane przez obywateli do planowania ewakuacji, a także sprawdzania dostępności schronień i tras ewakuacyjnych. Aplikacje i platformy oparte na chmurze umożliwiają obywatelom śledzenie rozwoju sytuacji kryzysowej oraz monitorowania pogody, poziomów rzek czy pożarów za pośrednictwem interaktywnych map i narzędzi. Oprócz w/w funkcji chmura obliczeniowa może zostać wykorzystana przez obywateli do przechowywania ważnych dokumentów i informacji osobistych, takich jak dokumenty tożsamości, ubezpieczenia czy dane medyczne. W przypadku ewakuacji możliwy jest do nich dostęp w dowolnym miejscu. Ponadto chmura umożliwia komunikację

w trakcie kryzysu. Obywatele mogą korzystać z aplikacji do wideokonferencji i wiadomości, aby utrzymywać kontakt z bliskimi.

Udostępnione za pośrednictwem Cloud Computing platformy e-learningowe mogą zawierać kursy i szkolenia z zakresu przygotowania do sytuacji kryzysowych, pierwszej pomocy i innych umiejętności potrzebnych w przypadku zagrożenia. Warto również podkreślić, że dzięki rozwiązaniu chmurowemu obywatele mogą korzystać z aplikacji mobilnych do zgłaszania incydentów, awarii czy potrzeby pomocy, co umożliwia służbom ratowniczym szybszą reakcję. Dodatkowo CC może zawierać bazę wiedzy i materiały edukacyjne dotyczące zarządzania kryzysowego, które obywatele mogą przeglądać i wykorzystywać w celu lepszego przygotowania się do sytuacji kryzysowej.

b. Zespoły Zarządzania Kryzysowego i służby ratownicze

Cloud computing oferuje wiele korzyści dla zespołów zarządzania kryzysowego i służb ratowniczych takich jak przechowywanie ogromnych ilości danych, w tym informacji na temat sytuacji kryzysowych; planów ewakuacji; map i dokumentów, co umożliwia zespołom zarządzania kryzysowego dostęp z dowolnego miejsca, a także dynamiczne dostosowywanie zasobów do potrzeb. W sytuacjach kryzysowych, gdy zapotrzebowanie na moc obliczeniową i przepustowość sieci może gwałtownie wzrosnąć, chmura pozwala na skalowanie zasobów w górę w celu obsłużenia wzmożonego ruchu. Ponadto dzięki zastosowaniu chmury obliczeniowej jak wspomniano w rozdziale zespoły zarządzania kryzysowego oraz służby ratownicze mają możliwość współpracy na odległość, co jest szczególnie przydatne, gdy różne służby ratownicze i zespoły pracują w różnych miejscach lub regionach kraju. W przypadku awarii lub utraty danych CC poprzez mechanizmy tworzenia kopii zapasowych i przywracania danych chmura obliczeniowa daje możliwość zespołom zarządzania kryzysowego zapewnienia ciągłości działania. Kolejne istotne funkcje Cloud Computing, o których wspomniano w koncepcji to analiza danych w czasie rzeczywistym, co pomaga zespołom zarządzania kryzysowego w monitorowaniu sytuacji i podejmowaniu szybkich decyzji na podstawie danych. Ponadto chmura może przechowywać dane przestrzenne i mapy, które są istotne dla zarządzania kryzysowego, w tym mapy zagrożeń, lokalizacje schronień, trasy ewakuacyjne. Dostęp do danych i narzędzi zarządzania kryzysowego możliwy jest z dowolnego miejsca za pomocą urządzenia z dostępem do internetu, co jest kluczowe w przypadku działań w terenie. Co istotne istnieją specjalne aplikacje i narzędzia dostępne w chmurze, które są przeznaczone

do zarządzania kryzysowego, takie jak platformy do koordynacji działań, systemy powiadamiania i komunikacji awaryjnej dzięki czemu możliwe jest usprawnienie działań służb ratowniczych i ZZK.

Ponadto należy zwrócić uwagę na fakt, że ZZK oraz służby ratownicze odpowiadają za treści udostępnione dla obywateli.

15. Blockchain

a. Zespoły Zarządzania Kryzysowego i służby ratownicze

Technologia blockchain ma potencjał do zastosowania w zarządzaniu kryzysowym dla służb ratowniczych i zespołów zarządzania kryzysowego. Zastosowanie omówionej w koncepcji technologii może znacząco usprawnić wszelkiego rodzaju działania zmierzające do zwalczania sytuacji kryzysowych. Technologia ta może zostać użyta do przechowywania i zarządzania danymi medycznymi pacjentów i rannych w sposób bezpieczny i niezmienny, co jest szczególnie istotne w sytuacjach kryzysowych, gdzie dostęp do historii medycznej może być kluczowy. Ponadto Blockchain może pomóc w weryfikacji tożsamości osób poszkodowanych, ewakuowanych lub zmarłych, dzięki czemu możliwe jest szybkie powiadomienie ich rodzin. Oprócz wyżej wymienionych funkcji, które znacząco mogą wspomóc działania ZZK oraz służb ratowniczych potencjał technologii Blockchain należy upatrywać w możliwości śledzenia dostaw medycznych, żywności, wody i innych zasobów w czasie kryzysu, zabezpieczeniu komunikacji między służbami ratowniczymi i ZZK, śledzeniu i analizie przebiegu sytuacji oraz dostarczaniu wiarygodnych danych do celów raportowania i oceny skutków kryzysu. Dla zespołów zarządzania kryzysowego, Blockchain może być wykorzystywany do przechowywania i udostępniania danych geoprzestrzennych, takich jak mapy zagrożeń czy lokalizacje schronień, śledzenia procesów ewakuacji, identyfikowania miejsc schronień i zarządzania informacjami o potrzebach poszkodowanych.

16. OLTP

a. Zespoły Zarządzania Kryzysowego i służby ratownicze

Służby ratownicze i zespoły zarządzania kryzysowego mogą korzystać z OLTP w celu poprawy swoich operacji i efektywności. A jej zastosowanie jak wspomniano w rozprawie odgrywa istotna rolę z zarządzaniu kryzysowym. OLTP może być używane do gromadzenia, przetwarzania i aktualizacji informacji o zdarzeniach kryzysowych w czasie rzeczywistym. Służby ratownicze i zespoły zarządzania kryzysowego mogą korzystać z systemów OLTP do śledzenia bieżącej sytuacji; rejestrowania

zgłoszeń i zarządzania dostępem do danych; zarządzania zasobami, takimi jak pojazdy ratownicze, personel medyczny i sprzęt; do zarządzania procesem dystrybucji pomocy humanitarnej, śledzenia dostaw i monitorowania potrzeb poszkodowanych; do komunikacji wewnętrznej i zewnętrznej, umożliwiającej zespołom zarządzania kryzysowego i służbom ratowniczym współpracę w czasie rzeczywistym; do zarządzania danymi medycznymi pacjentów i rannych w czasie rzeczywistym, co pomaga w zapewnieniu im odpowiedniej opieki; do zarządzania procesem ewakuacji, w tym śledzenia ilości ewakuowanych osób, lokalizacji schronienia i tras ewakuacyjnych. Ponadto OLTP umożliwia dostęp do danych i systemów, co jest istotne w przypadku wrażliwych informacji oraz dla zapewnienia bezpieczeństwa działań służb ratowniczych i zespołów zarządzania kryzysowego. Zastosowanie OLTP przez zespoły zarządzania kryzysowego oraz służby ratownicze umożliwia również zbieranie danych na potrzeby raportowania i analizy, co pomaga w ocenie skuteczności reakcji na kryzys, a także wspieranie systemów komunikacji awaryjnej, takich jak systemy powiadamiania publicznego i powiadamiania w sytuacjach kryzysowych.

17. OLAP

a. Zespoły Zarządzania Kryzysowego i służby ratownicze

Technologia OLAP jest przydatna dla służb ratowniczych i zespołów zarządzania kryzysowego w analizie danych oraz podejmowaniu decyzji w tym do oceny możliwości przeciwdziałania zagrożeniom i dostępności sił i środków niezbędnych do tego celu. Zespoły Zarządzania Kryzysowego mogą wykorzystać technologię OLAP do analizy danych przestrzennych, takich jak dane dotyczące lokalizacji zdarzeń kryzysowych, ewakuacji, schronień czy dostaw, co umożliwia identyfikację wzorców przestrzennych i pomaga w podejmowanie decyzji dotyczących alokacji zasobów oraz w celu identyfikacji trendów i tworzeniu prognoz dotyczących możliwych scenariuszy kryzysowych, co może ułatwić ZZK przygotowanie na ewentualne sytuacje kryzysowe i podejmowanie działań prewencyjnych. Ponadto dzięki technologii OLAP możliwe jest tworzenie interaktywnych pulpitów nawigacyjnych, które umożliwiają zespołom zarządzania kryzysowego monitorowanie bieżącej sytuacji w czasie rzeczywistym. Działa to na zasadzie przeglądania danych w wielu wymiarach, co pozwala na szybkie wykrywanie zmian. Dzięki zastosowaniu technologii OLAP zespoły zarządzania kryzysowego mogą ocenić priorytety i kierować działania ratownicze poprzez analizę skutków kryzysu, takich jak liczba poszkodowanych, zniszczeń mienia czy potrzeb humanitarnych. Warto również podkreślić, że OLAP może wspierać zarzą-

dzanie zasobami, takimi jak pojazdy ratownicze, sprzęt medyczny i zapasy żywności. Analiza ta pozwala na optymalizację wykorzystania dostępnych zasobów w czasie kryzysu co znacząco może usprawnić działanie służb ratowniczych oraz ZZK w sytuacjach kryzysowych. Potencjał technologii OLAP jak podkreślono w koncepcji pozwala również na generowanie zaawansowanych raportów i prezentacji na podstawie danych kryzysowych, monitorowania dostaw medycznych, żywności i innych zasobów, co jest istotne w przypadku zarządzania akcjami ratunkowymi, a także wspierać systemy komunikacji awaryjnej i analizować efektywność komunikatów. Zastosowanie technologii OLAP umożliwia również udostępnianie danych i współpracę z innymi służbami ratowniczymi i zespołami zarządzania kryzysowego, co jest istotne w sytuacjach wymagających skoordynowanej reakcji.

18. Big Data

a. Zespoły Zarządzania Kryzysowego i służby ratownicze

Big data może dostarczyć znacząco usprawnić działanie zespołów zarządzania kryzysowego i służb ratowniczych w sytuacjach kryzysowych. Analiza dużych ilości danych pochodzących z czujników, satelitów, kamer i innych źródeł pozwala na monitorowanie i przewidywanie katastrof naturalnych, takich jak np. trzęsienia ziemi, powodzie czy pożary lasów, co umożliwia ZZK wcześniejsze ostrzeganie i przygotowanie do działań. Ponadto wykorzystanie technologii Big Data umożliwia Zespołom Zarządzania Kryzysowego analizę treści generowanych przez społeczność w mediach społecznościowych, co może pomóc zespołom zarządzania kryzysowego w zrozumieniu reakcji społeczności na kryzys, identyfikacji obszarów wymagających pomocy i zarządzaniu dezinformacją. Wykorzystanie technologii Big Data umożliwia również zespołom zarządzania kryzysowego monitorowanie danych geoprzestrzennych co umożliwia gromadzenie i analizę danych związanych z lokalizacją, śledzeniem rozwoju sytuacji kryzysowej, identyfikacją obszarów zagrożonych i planowaniem ewakuacji. Technologia Big Data dostarcza również narzędzia do skutecznego zarządzania komunikacją i powiadamianiem w przypadku kryzysu, włączając w to automatyczne alerty i komunikaty awaryjne. W przypadku służb ratowniczych Big Data może być używane do analizy danych medycznych pacjentów, co pozwala na lepszą diagnozę i dostosowanie opieki medycznej do potrzeb poszkodowanych, monitorowania i zarządzania, dostawami medycznymi, żywnością i innymi zasobami niezbędnymi w przypadku kryzysów humanitarnych, a także może dostar-

czać informacje w czasie rzeczywistym o sytuacji na miejscu zdarzenia, dzięki czemu służby ratownicze mogą lepiej zrozumieć, jakie środki i zasoby są potrzebne.

19. Business Inteligence

a. Zespoły Zarządzania Kryzysowego i służby ratownicze

Technologia BI może dostarczyć zespołom zarządzania kryzysowego i służbom ratowniczym wartościowe informacje i narzędzia do podejmowania lepszych decyzji w sytuacjach kryzysowych. BI może dostarczać zespołom zarządzania kryzysowego bieżące dane sytuacji z różnorodnych źródeł takich jak czujniki, dane meteorologiczne itp. Dzięki temu można szybko zrozumieć rozwijającą się sytuację i podjąć odpowiednie działania. Ponadto technologia ta umożliwia analizę danych przestrzennych, co jest kluczowe w zarządzaniu kryzysowym. Dzięki czemu możliwe jest tworzenie map zagrożeń, tras ewakuacji, lokalizacja schronień itp. Technologia Big Data umożliwia również zespołom zarządzania kryzysowego tworzenie zaawansowanych raportów i analizowanie danych w celu identyfikacji trendów i wzorców w dziedzinie zarządzania kryzysowego i działań ratunkowych.

W przypadku służb ratunkowych BI może pomagać w analizie danych medycznych pacjentów, co pozwala na szybszą i bardziej dokładną diagnozę oraz dostosowanie opieki medycznej, dostarczać narzędzia do prognozowania rozwoju sytuacji kryzysowych, co pomaga w planowaniu działań i alokacji zasobów na przyszłość, wspierać systemy komunikacji awaryjnej i powiadamiania.

Ponadto Business Inteligence może usprawnić współpracę między różnymi służbami i zespołami zarządzania kryzysowego poprzez udostępnianie wspólnych narzędzi i danych, a także może analizować dane pochodzące z mediów społecznościowych, co pozwala na monitorowanie reakcji społeczności na sytuacje kryzysowe i zarządzanie informacjami w czasie rzeczywistym.

Zaprezentowane możliwości wykorzystania współczesnych oraz tradycyjnych technologii są różne dla wyszczególnionych grup i dotyczy takich aspektów jak akcje ratownicze, planowanie działań, przetwarzanie informacji i jej przekazywanie oraz gromadzenie i analiza danych. Warto jednak zwrócić uwagę na fakt, że brak odpowiedniej wiedzy na temat funkcjonowania technologii oraz odpowiedniej infrastruktury czyni ją bezużyteczną. Dlatego też niezbędne jest określenie zarówno urządzeń jaki aplikacji niezbędnych do wykorzystania omówionych współczesnych technologii (tab. 6.8).

Tabela 6.8. Urządzenia i aplikacje niezbędne przy wykorzystaniu i implementacji współczesnych technologii

URZĄDZENIA I APLIKACJE	
Internet rzeczy	**Czujniki i sensory** – urządzenia zdolne do wykrywania oraz śledzenie obiektów np. czujniki monitorujące infrastrukturę krytyczną, czytniki linii papilarnych, systemy rozpoznawania twarzy, inteligentne bramki na lotniskach, drony i urządzenia monitorujące smog w miastach, drony (wojskowe, cywilne)[373], czujniki (temperatury, poziomu wody, zanieczyszczenia powietrza ruchu itp., nadajniki umożliwiające komunikację, odbiór poleceń oraz gromadzenie i przekazywanie informacji, Sieci sensorów w budynkach umożliwiające detekcję i lokalizację ewentualnych ofiar w gruzowiskach. (obywatel, ZZK, służby ratownicze) **Mikrokontrolery i mikroprocesory** – układy elektroniczne kontrolujące działanie urządzeń *IoT* np. Raspberry Pi, Arduino, ESP8266, ESP32 itp. **Moduły komunikacyjne** – wspomaganie komunikacji między urządzeniami a internetem lub między samymi urządzeniami np. moduły Wi-Fi, Bluetooth, Zigbee, LoRa, NB-*IoT* itp. (obywatel, ZZK, służby ratownicze) **Bramki IoT** – urządzenia, które pozwalają starszym urządzeniom na raportowanie danych za pomocą Internetu, a także umożliwiają interakcję między urządzeniami np. bramki Wi-Fi, bramki LTE, bramki LoRa itp. **Chmura IoT** – gromadzenie, przetwarzanie i analiza danych zebranych przez urządzenia *IoT* oraz zarządzanie i monitorowanie urządzeń np. AWS *IoT*, Microsoft Azure *IoT* Hub, Google Cloud *IoT* Core itp. Aplikacje mobilne i interfejsy użytkownika: Pozwalają użytkownikom na zdalne zarządzanie i monitorowanie urządzeń *IoT* za pomocą smartfonów lub komputerów. **Systemy zarządzania danymi** – przechowywanie, analiza i interpretacja danych zebranych przez urządzenia *IoT* np. bazy danych , systemy *Big Data* oraz narzędzia analizy danych itp. **Zabezpieczenia IoT** – mechanizmy uwierzytelniania, szyfrowanie danych, firewall'e itp. **Zasilanie** – zasilanie bateryjne, zasilanie sieciowe lub zasilanie z energii słonecznej. **Wearable Tech** – sprawdzanie parametrów życiowych, stanu zdrowia oraz kondycji fizycznej. **Drony** – dostarczanie kluczowych informacji i obrazu z miejsca zagrożenia, przenoszenie sprzętu jedzenia itp. **Komunikacja i łączność** – usprawnienie koordynacji działań IoMT (Internet of Medical Things) – automatyczne wzywanie pomoc lub dostarczanie informacji medycznych służbom ratowniczym np. w przypadku zatrzymania akcji serca.
Sztuczna inteligencja	**Komputery –** komputery klasy PC z wysoką mocą obliczeniową do przetwarzania danych w algorytmach sztucznej inteligencji, a także karty graficzne do przetwarzania równoległego np. GPU (Graphics Processing Unit) lub TPU (Tensor Processing Unit). **Serwery** – efektywne przetwarzanie danych. **Sensory** – urządzenia do zbierania danych np. kamery wizyjne, mikrofony, czujniki ruchu, czujniki temperatury itp. **Internet rzeczy (IoT)** – przetwarzanie danych z czujników itp. **Roboty i urządzenia autonomiczne** – robotyka i autonomiczne (podejmowanie decyzji, nawigacja i interakcja z otoczeniem). **Aparaty fotograficzne i kamery** – analiza obrazów i wideo. **Chmura obliczeniowa** – przetwarzanie i analiza dużej ilości danych w skalowalny sposób.
Cloud Computing	**Komputer** – uruchomienie przeglądarki lub aplikacji umożliwiającej dostęp do zasobów w chmurze i zarządzanie nią. **Urządzenia mobilne** – dostęp do zasobów w chmurze oraz zarządzanie nią za pomocą takich urządzeń jak np. smartfon lub tablet. **Przeglądarka internetowa** – dostęp do aplikacji i danych w chmurze za pomocą przeglądarki np. Google Chrome, Mozilla Firefox czy Microsoft Edge. **Elementy sieciowe** – urządzenia sieciowe do zapewnienia stałego połączenia z chmurą np. routery, przełączniki i modemy. **Chmura publiczna lub prywatna** – dostawca udostępniający miejsce na przechowywane dane. **Aplikacje chmurowe** – oprogramowanie do używania usług w chmurze.

[373] M. Ogórek, P. Zaskórski, Internet rzeczy w integracji procesów zarządzania kryzysowego, Zeszyty naukowe Politechniki Poznańskiej Organizacja i Zarządzanie nr. 76, Poznań 2018 s. 202.

Tabela 6.8 cd. Urządzenia i aplikacje niezbędne przy wykorzystaniu i implementacji współczesnych technologii

Systemy informacji geoprzestrzennej	**Komputer** – przetwarzanie i analiza danych geoprzestrzennych np. stacjonarne komputery klasy PC, jak i serwery o większej mocy obliczeniowej. **Odbiorniki GPS** – odbieranie sygnałów z systemów nawigacji satelitarnej (np. GPS, GLONASS, Galileo) pozwalające na dokładne położenia geograficznego. **Czujniki terenowe** – czujniki zbierające dane o środowisku np. meteorologiczne, wilgotności gleby, jakości powietrza itp. **Aparaty fotograficzne i kamery** – zdjęcia satelitarne, lotnicze lub naziemne (ważne źródło danych w GIS). **Tablety i smartfony** – urządzenia mobilne np. smartfony i tablety umożliwiające zbieranie danych na temat terenu poprzez wbudowane funkcje takie jak np. GPS lub aparat. **Skanery QR kodów i kodów kreskowych** – zbieranie danych o obiektach ich znakowanie i identyfikacja. **Drukarki** – drukowanie raportów, map oraz analiz geoprzestrzennych. **Cyfrowe mapy i dane geoprzestrzenne** – bazy danych oraz mapy cyfrowe stanowiące podstawę do analizy geoprzestrzennej. **Oprogramowanie GIS** – obsługi rastrowanych map wojskowych (Pakiet Grafiki Operacyjnej 2003), zobrazowania zagrożeń zaistniałych na terenie województwa na podkładzie mapy cyfrowej (np. CorelDRAW Graphics Suite 2021, QGIS), gromadzące i aktualizujące dane o zdarzeniach obrazujących sytuację na szczeblu gminnym, powiatowym oraz wojewódzkim (np. Arcus 2015. NET, CAR), systemy reagowania kryzysowego (np. Alaska – opracowany przez resortowe Centrum Zarządzania Projektami Informatycznymi), kontroli funkcjonowania jednostek Państwowego Ratownictwa Medycznego (GPS Monitor Rejestr, SWD PRM), analizy geoprzestrzennej do wspomagania procesów decyzyjnych (Arcus-Geo, ArcGis, InterGraf). **Elementy sieciowe** – komunikacja między urządzeniami np. routery, przełączniki itp.
Blockchain	**Komputer –** komputer klasy PC lub laptop, dzięki któremu możliwy jest dostęp do aplikacji i usług *Blockchain*, co umożliwia generowanie, zarządzanie i przeglądanie portfela kryptowalutowego i przeprowadzanie transakcji. **Smartfon** – aplikacje umożliwiające generowanie, zarządzanie i przeglądanie portfela kryptowalutowego. **Portfel kryptowalutowy** – przechowywanie kryptowalut. Portfel może być dostępny w formie aplikacji na komputer, smartfon lub jako specjalne urządzenie fizyczne (hardware wallet). **Hardware Wallet (Portfel sprzętowy)** – urządzenie fizyczne służące do przechowywania kluczy prywatnych i zarządzania kryptowalutami. Portfele sprzętowe oferują zwiększoną ochronę przed potencjalnymi zagrożeniami związanymi z cyberbezpieczeństwem. **Sieć internetowa** – dostęp do technologii *Blockchain* możliwy jest za pośrednictwem internetu. **Przeglądarka internetowa** – przeglądarki internetowe z obsługą *Blockchain*. **Drukarka** – wydruk kluczy prywatnych i publicznych.
Big Data	**Serwer** – serwery o dużej mocy obliczeniowej oraz dużej pojemności pamięciowej do przechowywania, przetwarzania i analizowania danych. **Technologie i urządzenia do przechowywania danych** – dyski twarde, macierze dyskowe, systemy pamięci masowej (storage arrays) czy chmura obliczeniowa. **Bazy danych** – Bazy danych *Big Data*, takie jak Hadoop Distributed File System (HDFS), No*SQL*, Cassandra, MongoDB czy inne, są wykorzystywane do przechowywania i zarządzania złożonymi danymi w sposób umożliwiający szybki dostęp i skalowanie. **Klastry obliczeniowe (cluster computing)** – rozdzielanie zadań na wiele serwerów, co umożliwia przyśpieszenie obliczeń. **Infrastruktura sieciowa** – dostęp do Internetu umożliwiający przesyłanie danych między urządzeniami. **Komputer** – komputer klasy PC lub laptop wyposażony w oprogramowanie do analiz danych np. (GBDOT). **Aplikacje i narzędzia *Big Data*** – oprogramowanie do analizy i przetwarzania danych np. Hadoop, Spark, Apache Flink, Elasticsearch, Apache Kafka, itp. **Systemy wizualizacji danych** – prezentowanie danych w formie rysunków wykresów np. Excel, Tableau, Power BI, QlikView i Qlik Sense.

Tabela 6.8 cd. Urządzenia i aplikacje niezbędne przy wykorzystaniu i implementacji współczesnych technologii

Business Inteligence	**Serwery** – przetwarzanie i analiza dużych zbiorów danych. **Bazy danych** – a relacyjne bazy danych (My*SQL*, Microsoft *SQL* Server, Postgre*SQL*, Oracle Database itp.) hurtownie danych (Microsoft *SQL* Server, Oracle Database, Oracle Database, Talend, itp.) czy bazy danych OLAP. **Komputer** – komputer klasy PC lub laptop do analizy danych i generowania raportów. **Smartfony i tablety** – dostęp do danych i ich analiza z dowolnego miejsca. **Infrastruktura sieciowa** – zapewnienie szybkości transmisji danych między serwerami i urządzeniami użytkowników. **Technologie i urządzenia do przechowywania danych** – dyski twarde, macierze dyskowe, systemy pamięci masowej (storage arrays) czy chmura obliczeniowa. **Zabezpieczenie danych** – szyfrowanie danych (protokoły HTTPS/SS), bezpieczne hasła (własne lub generatory haseł), systemy zarządzania tożsamością (Identity and Access Management – IAM). **Elementy sieciowe** – routery, przełączniki i firewalle, do zapewnienia bezpiecznego i stabilnego połączenia sieciowego.
OLTP	**Serwery** – przechowywanie i obsługa danych. Baza danych – przetwarzanie i obsługa transakcji np. Oracle, My*SQL*, Microsoft *SQL* Server, Postgre*SQL* itp. **Infrastruktura sieciowa** – zapewnienie szybkości transmisji danych między serwerami i urządzeniami użytkowników. **Aplikacje klienta** – aplikacje do obsługi transakcji *OLTP* możliwe do wykorzystania za pośrednictwem komputerów stacjonarnych, smartfonów, tabletów lub przeglądarek internetowych. **Elementy sieciowe** – routery, przełączniki i firewalle, do zapewnienia bezpiecznego i stabilnego połączenia sieciowego. **Backup i Disaster Recovery** – zapewnienie ciągłości działania i zabezpieczenie przed utratą danych. **Zabezpieczenie danych** – szyfrowanie danych (protokoły HTTPS/SS), bezpieczne hasła (własne lub generatory haseł), systemy zarządzania tożsamością (Identity and Access Management – IAM) **Technologie i urządzenia do przechowywania** danych – dyski twarde, macierze dyskowe, systemy pamięci masowej (storage arrays) czy chmura obliczeniowa.
OLAP	**Serwery** – przetwarzanie i analiza dużych zbiorów danych. **Bazy danych** – analiza wielowymiarowych danych np. Microsoft Analysis Services, IBM Cognos TM1 i Oracle OLAP. **Aplikacje klienta** – aplikacje do obsługi transakcji *OLTP* możliwe do wykorzystania za pośrednictwem komputerów stacjonarnych, smartfonów, tabletów lub przeglądarek internetowych. **Elementy sieciowe** – routery, przełączniki i firewalle, do zapewnienia bezpiecznego i stabilnego połączenia sieciowego. **Systemy wizualizacji danych** – prezentowanie danych w formie rysunków wykresów np. Excel, Tableau, Power BI, QlikView i Qlik Sense. **Technologie i urządzenia do przechowywania danych** – dyski twarde, macierze dyskowe, systemy pamięci masowej (storage arrays) czy chmura obliczeniowa. **Zabezpieczenie danych** – szyfrowanie danych (protokoły HTTPS/SS), bezpieczne hasła (własne lub generatory haseł), systemy zarządzania tożsamością (Identity and Access Management – IAM)
VR\AR	**Gogle *VR*** – wyświetlanie wirtualnej rzeczywistości przed oczami za pomocą specjalistycznych okularów. **Systemy śledzenia ruchu** – śledzenie ruchów użytkowników wykorzystujących technologię *VR*. **Komputer lub konsola** – wysoko wydajnościowe urządzenie ze specjalistyczną karta graficzną do przetwarzania obrazu w czasie rzeczywistym, **Oprogramowanie** – zaawansowane programy do tworzenia scenariuszy zagrożeń np. Unity, Virtual Battlespace 2 (VBS2), Unreal Engine itp. **Urządzenia mobilne** – łączenie obrazów rzeczywistych z wirtualnymi na urządzeniach mobilnych takich jak np. smartfon lub tablet. **Okulary AR** – nakładanie obrazu wirtualnego na rzeczywisty za pomocą specjalistycznych okularów. **Szkła do projekcji AR** – wyświetlanie informacji i obrazów na tafli szkła. **Soczewki kontaktowe AR** – wyświetlanie informacji bezpośrednio na oku użytkownika. **Kamery** – rejestrowanie rzeczywistego obrazu otoczenia, na który nakładane są elementy wirtualne.

Źródło opracowanie własne.

W tabeli 6.8 zaprezentowano współczesne technologie, do których przypisane zostały urządzenia i aplikacje możliwe do wykorzystania przez zespoły zarządzania kryzysowego, służby ratownicze oraz obywateli. Zaprezentowane w tabeli rozwiązania nie określają całkowitego potencjału tych technologii, których możliwości są niemalże nieograniczone i podlegają ciągłemu rozwojowi

6.5. Podsumowanie rozdziału szóstego

W koncepcji przedstawiono współczesne i tradycyjne technologie możliwe do wykorzystania w celu usprawnienia działania służb ratowniczych, zwiększenia świadomości sytuacyjnej na temat zagrożeń oraz w procesie skutecznego przepływu informacji pomiędzy grupami zaangażowanymi w zarzadzanie kryzysowe w tym obywateli. Niemniej jednak należy zwrócić uwagę na fakt, że zaproponowane rozwiązania nie stanowią „złotego środku" na rozwiązanie wszystkich problemów związanych z zarządzaniem kryzysowym, z usprawnieniem działania zespołów zarządzania kryzysowego oraz służb ratowniczych, z obiegiem informacji oraz kształtowaniem świadomości sytuacyjnej na temat zagrożeń. Rozwiązania tego typu istotnie mogą usprawnić działania służb, członków zespołów zarządzania kryzysowego oraz obywateli, a także przyczynić się do zwiększenia świadomości sytuacyjnej interesariuszy zaangażowanych w zarządzanie kryzysowe pod warunkiem, że omówione w rozdziale koncepcyjnym technologie zostaną właściwie wykorzystane. Ponadto żadna z technologii nie jest w stanie zastąpić ludzkiego umysłu w podejmowaniu świadomych decyzji i może jedynie wesprzeć i ukierunkować oraz ułatwić działanie służb ratowniczych, zespołów zarządzania kryzysowego oraz obywateli. Jak wspomniano w rozprawie proces wdrożenia technologii wymaga przygotowania odpowiedniej infrastruktury, a więc i nakładów finansowych niezbędnych do wdrożenia technologii, a także czasu na ich poznanie oraz przeszkolenie osób, które będą je wykorzystywać. Pomimo iż w zarządzaniu kryzysowym czas odgrywa istotną rolę i odpowiednio szybka reakcja na zagrożenia może częściowo ograniczyć skutki zagrożeń, to w przypadku technologii nie należy ich wdrażać ad hoc. Każda z technologii powinna być wdrażana w sposób przemyślany i powinna stanowić uzupełnienie dla aktualnie wykorzystywanych rozwiązań, aby zapewnić ciągłość działania w zarządzaniu kryzysowym. Oczywiście w przyszłości niektóre z technologii mogą zastąpić aktualnie wykorzystywane technologie niemniej jednak zanim to się stanie należy odpowiednio je przygotować oraz poznać ich funkcjonalność tak, aby możliwe było w pełni wykorzystanie ich potencjału.

Warto w tym miejscu zauważyć, że technologie IT/ICT to wymuszenie tzw. ładu informacyjnego, a więc zarówno jednorazowa identyfikacja zagrożeń i ich potencjalnych oraz rzeczywistych skutków, a także świadomość fizycznego potencjału (niezbędnych sił i środków) do ich ograniczenia, likwidacji i odtworzenia utraconych zasobów (infrastruktury). Świadomość sytuacyjna to obraz zagrożeń i rzetelna ocena przeciwdziałania im. Narzędzia IT/ICT umożliwiają zatem ocenę i wskazanie wieloaspektowych działań oraz zachowań w konkretnej sytuacji kryzysowej.

ROZDZIAŁ VII

OCENA IMPLEMENTACYJNOŚCI OPRACOWANEJ KONCEPCJI

7.1. Wprowadzenie

W rozdziale VI wskazano możliwości rozwoju zarówno współczesnych jak i tradycyjnych technologii, a także kierunki ich doskonalenia. W celu oceny przydatności rozwiązań zawartych w koncepcji i możliwości implementacji poszczególnych technologii i platform IT/ICT przeprowadzony został wywiad ekspercki (pełny formularz wywiadu eksperckiego w załączniku nr 6), skierowany do różnych podmiotów. Biorąc pod uwagę cel badania, najważniejsze było, aby eksperci posiadali specjalistyczną wiedzę z zakresu zarządzania kryzysowego oraz tradycyjnych i współczesnych technologii IT/ICT. Grupę ekspercką reprezentowały osoby z obszaru bezpieczeństwa, informatyki i zarządzania (N=7). Ekspertom przedstawione zostało 11 pytań związanych z koncepcją doskonalenia systemu kreowania świadomości sytuacyjnej ludności.

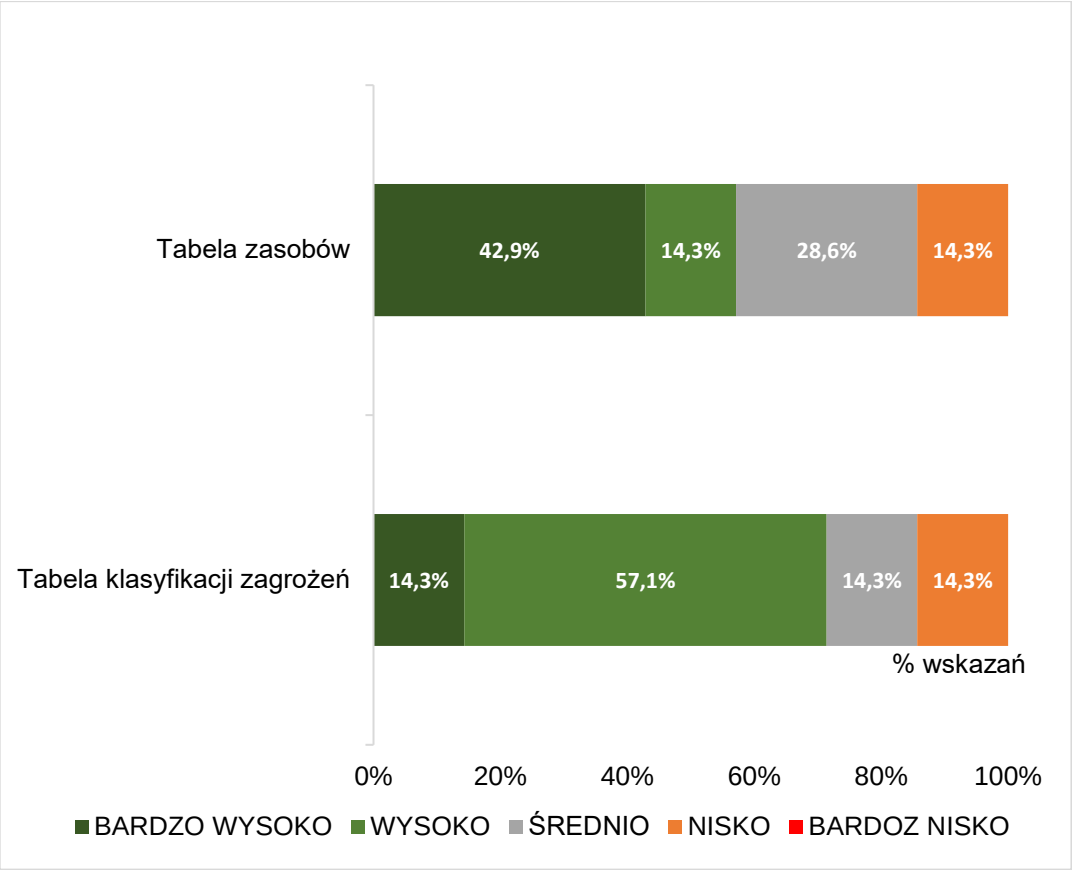
7.2. Ocena implementacyjności koncepcji na podstawie wywiadu eksperckiego

W wywiadzie poproszono ekspertów o ocenę zaproponowanych rozwiązań w 5 – stopniowej skali (bardzo wysoko, wysoko, średnio, nisko, bardzo nisko). Ponadto każdego eksperta poproszono o ocenę przydatności wskazanych rozwiązań oraz potencjalnych kierunków rozwoju wraz z uzasadnieniem dokonanego wyboru.

Kwestionariusze wywiadu eksperckiego nie są udostępnione w rozprawie ze względu na ochronę danych osobowych i są do wglądu u autora rozprawy.

W celu oceny przydatności zaproponowanych rozwiązań poproszono ekspertów o odpowiedź na sformułowane pytania dotyczące zarówno współczesnych jak i tradycyjnych technologii, a także rozwiązań wskazanych przez autora rozprawy.

1. Jak ocenia Pani/Pan możliwości wykorzystania zaproponowanej klasyfikacji zagrożeń z uwzględnieniem działań niezbędnych do wykonania oraz tabeli zasobów w aspekcie kreowania świadomości sytuacyjnej ludności na temat zagrożeń (wyk. 7.1)?



Wykres 7.1. Ocena przydatności wykorzystania tabeli zasobów oraz tabeli klasyfikacji zagrożeń (N = 7)

Źródło: opracowanie własne

Z przeprowadzonej analizy odpowiedzi można wywnioskować, że 3 (42,9%) ekspertów oceniło przydatność tabeli zasobów na bardzo wysokim poziomie, a 1 (14,3%) ekspert na wysokim poziomie, co pokazuje, że 57,2% uważa za przydatne wykorzystanie tego typu rozwiązania. Spośród wytypowanych ekspertów 2 (28,6%) oceniło przydatność tabeli zasobów na średnim poziomie oraz 1(14,3%) na niskim.

Klasyfikację zagrożeń 1 ekspert (14,3%) ocenił na bardzo wysokim poziomie, a 4 (57,1%) na wysokim co pokazuje, że 71,4% ekspertów uważa za przydatne wykorzystanie tego typu rozwiązania. Ponadto 1 (14,3%) z ekspertów ocenił przydatność zaproponowanych rozwiązań na średnim poziomie oraz 1 (14,3%) na niskim.

Na podstawie analizy odpowiedzi ekspertów można zauważyć że zaproponowana w koncepcji tabela zasobów (tab. 6.2) oraz tabela klasyfikacji zagrożeń (tab. 6.1) jest w stanie usprawnić działanie służb ratowniczych, zespołów zarządzania kryzysowego oraz obywateli w aspekcie zwiększenia świadomości sytuacyjnej na temat zagrożeń, a także usprawnić przygotowanie się na wypadek ich wystąpienia.

Ponadto w tabeli 7.1 przedstawiono opinię ekspertów na temat zaproponowanych rozwiązań oraz kierunki ich doskonalenia.

Tabela 7.1. Możliwości wykorzystania zaproponowanej klasyfikacji zagrożeń z uwzględnieniem działań niezbędnych do wykonania oraz tabeli zasobów (N = 7)

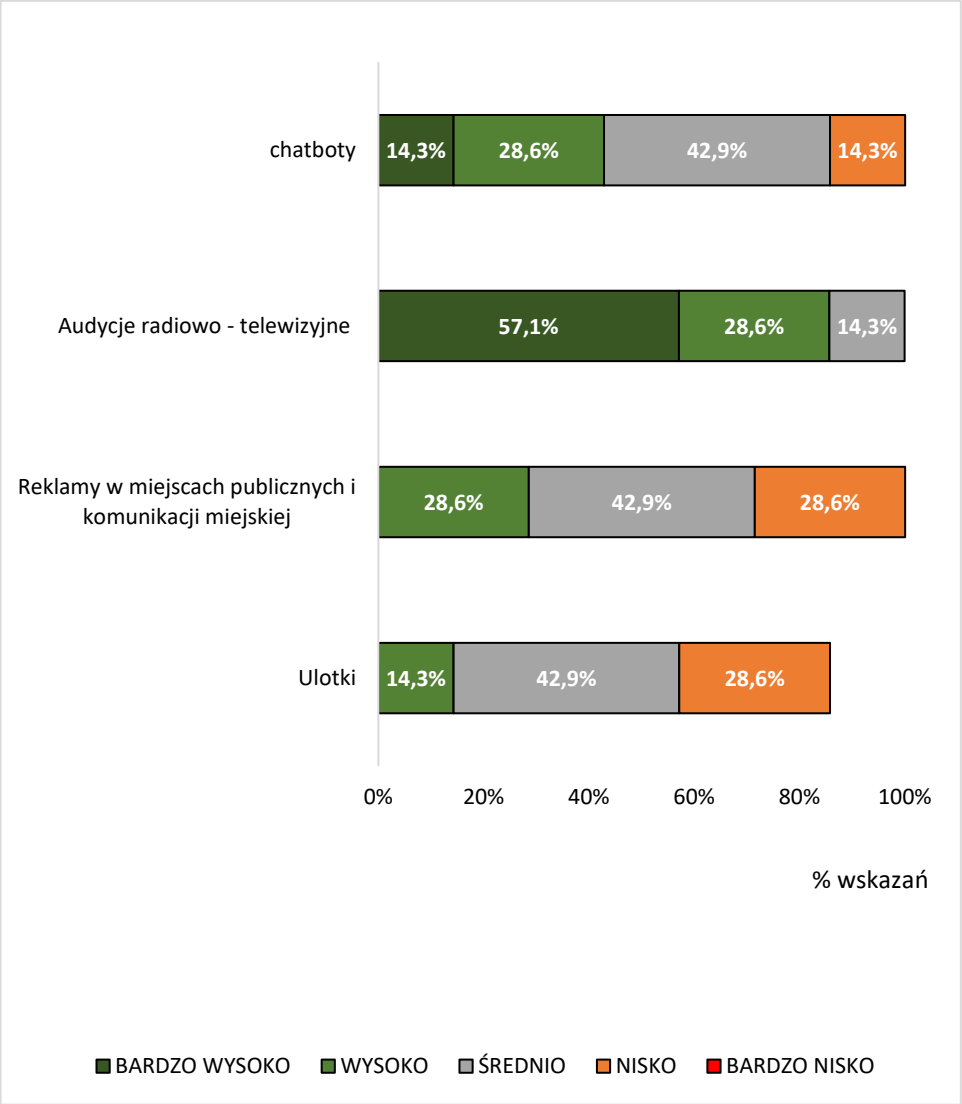
Odpowiedzi respondentów
• Uprościć klasyfikację zagrożeń oraz odnieść do dobrostanu człowieka i zwierząt domowych (często zapominany element), np. stopniowalne zagrożenie wprowadzeniem ograniczeń w korzystaniu z mediów, zagrożenie dla zdrowia, zagrożenia dla życia lub inne. • Określić co zwykły obywatel powinien zrobić (np. zgromadzenie zapasów, przygotowanie do czasowego pobytu poza miejscem zamieszkania, wykonywanie poleceń służb organizujących ewakuację itp.). • Konieczność rozróżnienia sposobu klasyfikowania zagrożeń (obywatel / służby ratownicze) znajduje swoje uzasadnienie w praktyce • Należy rozważyć np. utrzymywanie „zapasów" stosownie do kilku poziomów zagrożeń (np. stały i rozszerzanym o składniki wskazywane przez służby ratownicze). • Dodać opady (śniegu), oblodzenia, gołoledź na drogach oraz awarie w zakładach wytwarzania i dystrybucji energii, dodać coś na temat portów morskich i rurociągów, a także (patrząc w przyszłość) awarie zakładów energetyki jądrowej. • Dokonać weryfikacji relacji zagrożenie – wymagany zasób, • Klasyfikacja zawarta w tabeli 1 powinna obowiązywać w procesach analitycznych realizowanych przez ekspertów z zakresu zarządzania kryzysowego a nie zwykłych obywateli • Wyjaśnić pojęcia Izolacji • Uwzględnić przeciwdziałanie, przewidywanie, rozpoznawanie i ratowanie • Umiejętność identyfikacji ryzyka i wieloaspektowego jego zwymiarowania, powinno przybliżyć zarządzających do skutecznej i efektywnej odpowiedzi na każde ryzyko i na każdym etapie jego „życia". Propozycja jego klasyfikacji, poprzez właściwą identyfikację zagrożeń i zasobów naturalnie wpisuje się w proces zarządzania ryzykiem który permanentnie stymuluje działania systemu kryzysowego. Stąd, podjęcie sprawy klasyfikacji zagrożeń/zasobów z punktu widzenia przygotowania i funkcjonowania systemu zarządzania kryzysowego jest wysoce uzasadniona. • Umiejętność identyfikacji ryzyka i wieloaspektowego jego zwymiarowania, powinno przybliżyć zarządzających do skutecznej i efektywnej odpowiedzi na każde ryzyko i na każdym etapie jego „życia". Propozycja jego klasyfikacji, poprzez właściwą identyfikację zagrożeń i zasobów naturalnie wpisuje się w proces zarządzania ryzykiem który permanentnie stymuluje działania systemu kryzysowego. Stąd, podjęcie sprawy klasyfikacji zagrożeń/zasobów z punktu widzenia przygotowania i funkcjonowania systemu zarządzania kryzysowego jest wysoce uzasadniona.

Źródło: opracowanie własne

W tabeli 7.1 wskazano kierunki doskonalenia zaproponowanych rozwiązań, które zdaniem ekspertów mogą usprawnić zarządzanie kryzysowe. Zaproponowane przez ekspertów rozwiązania w perspektywie przyszłości wydają się zasadne, niemniej jednak zaproponowane w koncepcji zagrożenia bazują na powszechnie występujących oraz omówionych w literaturze przedmiotu. Sklasyfikowanie dodatkowych źródeł zagrożeń w tak przyjętej formie może znacznie poprawić świadomość sytuacyjną na temat rzadko występujących zagrożeń. Warto jednak podkreślić, że niemożliwe jest sklasyfikowanie wszystkich, ponieważ każda sytuacja czy zdarzenie może wywołać nowe zagrożenie.

2. Jak ocenia Pani/Pan możliwości rozszerzenia systemu informowania ludności o: ulotki, reklamy w miejscach publicznych i komunikacji miejskiej, audycje ra-

diowo telewizyjne, a także o technologie sztucznej inteligencji takie jak np. chatboty (rozumiany jako wirtualny asystent głosowo-tekstowy), których zadaniem jest udzielanie odpowiedzi na zadawane pytania (wyk. 7.2).



Wykres 7.2. Ocena przydatności chatbotów, ulotek, audycji radiowo-telewizyjnych oraz reklam w miejscach publicznych i komunikacji miejskiej w procesie informowania ludności o zagrożeniach (N = 7)

Źródło: opracowanie własne

W pytaniu 2 poproszono ekspertów o ocenę przydatności takich rozwiązań jak chatboty, ulotki, audycje radiowo-telewizyjne oraz reklamy w miejscach publicznych i komunikacji miejskiej w procesie informowania ludności o zagrożeniach.

Na podstawie odpowiedzi ekspertów można zauważyć, że 1 z (14,3%) ekspertów ocenił przydatność ulotek na bardzo wysokim poziomie, 2 na wysokim (28,6%), 3 (42,9%) na średnim oraz 1 (14,3%) ekspert ocenił nisko. Audycje radiowo-

telewizyjne zostały ocenione przez 4 (57,1%) ekspertów na bardzo wysokim poziomie, 2 (28,6%) na wysokim poziomie oraz przez 1 (14,3%) na niskim.

Rozwiązania takie jak reklamy w miejscach publicznych i komunikacji miejskiej ocenione zostały przez 2 (28,6%) ekspertów na wysokim poziomie, a spośród wybranych ekspertów 3 (42,9%) oceniło tego typu rozwiązanie na średnim poziomie oraz 2 (28,6%) na niskim. Rozwiązanie takie jak chatboty zostały przez 1 (14,3%) eksperta na bardzo wysokim poziomie, przez 2 (28,6%) na wysokim, przez 3 (42,9%) na średnim oraz 1 (14,3%) ekspert ocenił je nisko.

Na podstawie oceny ekspertów można zauważyć, że spośród zaproponowanych rozwiązań najwyżej zostały ocenione audycje radiowo-telewizyjne, które zadaniem niektórych ekspertów stanowią wiarygodne źródło informacji w procesie informowania ludności zagrożeniach. Na podstawie analizy odpowiedzi ekspertów można zauważyć, że zdania są podzielone, co wynika z faktu, że wśród ekspertów są osoby, które preferują zarówno tradycyjne jak i współczesne technologie IT/ICT.

Rozwiązania takie jak reklamy w miejscach publicznych i komunikacji miejskiej, ulotki oraz chatboty ocenione zostały nieco niżej co nie oznacza, że są niepotrzebne. Tego typu rozwiązania są coraz częściej wykorzystywane np. Alerty RCB na ekranach wielkoformatowych, chatboty, które zastępują człowieka w procesie przekazywania informacji oraz ulotki przekazują informacje na temat zagrożeń oraz sposobach radzenia sobie z nimi, niemniej jednej ta forma przekazu informacji wymaga skorygowania i zaktualizowania o nowe zagrożenia i nowe technologie możliwe do wykorzystania w zarządzaniu kryzysowym.

W koncepcji celowo przyjęto słowo reklama, aby odróżnić ją od informacji, która, zawiera krótkie informacje na temat zagrożeń i wysyłane są np. w formie alertów RCB lub wyświetlane za pośrednictwem ekranów wielkoformatowych. Spoty reklamowe związane z zagrożeniami np. wypadki drogowe czy kolejowe wielokrotnie wyświetlane były za pośrednictwem programów telewizyjnych, wielkich telebimów czy banerów.

W tabeli 7.2 przedstawiono ocenę ekspertów na temat możliwości wykorzystania takich rozwiązań jak chatboty, ulotki, audycje radiowo-telewizyjne oraz reklamy w miejscach publicznych i komunikacji miejskiej w procesie informowania ludności o zagrożeniach, a także wskazano kierunki ich doskonalenia w opinii ekspertów.

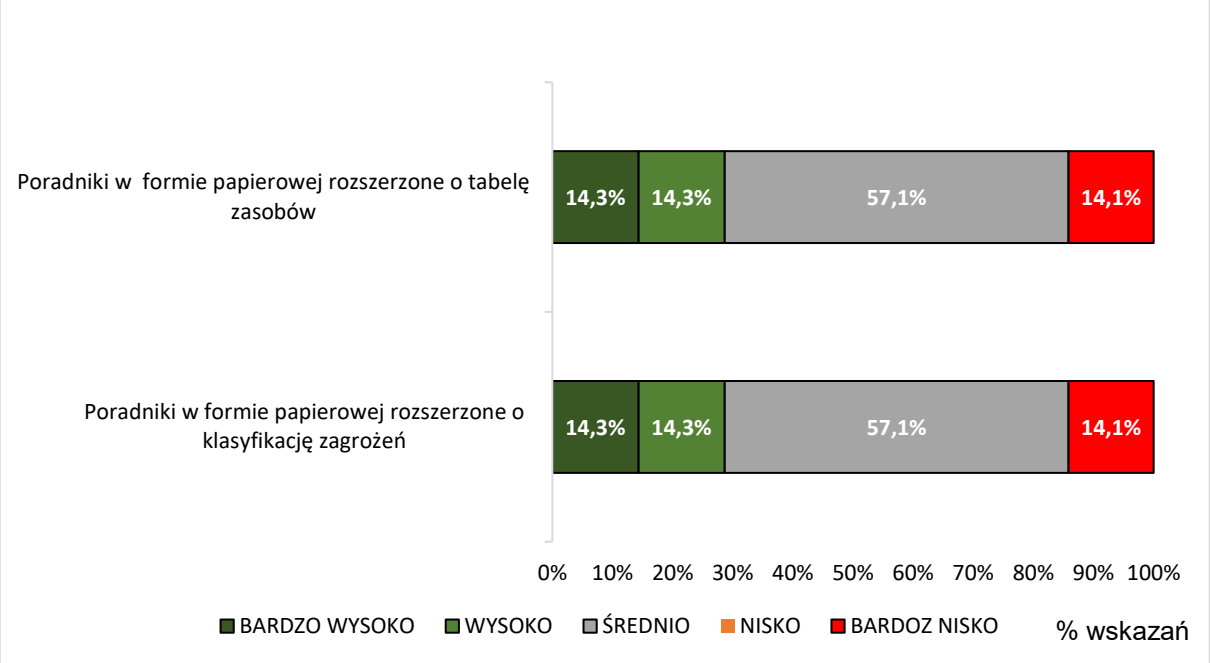
Tabela 7.2. Możliwości rozszerzenia systemu informowania ludności o: ulotki, reklamy w miejscach publicznych i komunikacji miejskiej, audycje radiowo telewizyjne, a także o technologie sztucznej inteligencji takie jak np. chatboty (rozumiany jako wirtualny asystent głosowo-tekstowy) (N = 7)

Odpowiedzi respondentów
• Słowo „Reklama" winno być skorygowane gdyż odnosi się ono do działalności komercyjnej. Dla potrzeb przeprowadzenia akcji informacyjnej możemy mówić o komunikatach, obwieszczeniach czy instrukcjach, publikowanych lub kolportowanych równolegle z reklamami komercyjnymi. • W dobie powszechnego dostępu do elektronicznych środków przekazywania informacji tradycyjne ulotki tracą swoje znaczenie. Mając na uwadze też dbałość o środowisko naturalne ten typ komunikacji powinien być starannie przemyślany. Nadal jednak celowym wydaje się ich przygotowywanie dla potrzeb osób nie korzystających z takich źródeł informacji jak Internet. • Treści propagowane za pomocą ulotek (forma umowna) winny być ponadczasowe, a samo wykonanie solidne i przyjazne do wykorzystania. Przykładem może być estetyczny plastik wielkości karty płatniczej z numerem alarmowym i prostą listą informacji jakie należy podać operatorowi systemu 112, aby zapewnić klarowne przekazanie wiadomości o wypadku lub magnes na lodówkę z listą artykułów stanowiących podstawowy zasób na wypadek sytuacji kryzysowej. • Audycje radiowe i chatboty stanowią trudne do przecenienia źródło informacji, o ile są właściwie przygotowane. • w sytuacji zagrożenia dostęp do pisanych źródeł informacji może być utrudniony. Równie ważne byłoby pokazanie kanałów przesyłania (proces: od nadawcy do odbiorcy) informacji o zagrożeniach. • Informowanie obecnie jest niskie i słusznie zasugerowane są wielorakie formy informowania • Należy uporządkować zagrożenia i przesyłaną informację za pomocą sygnałów, za która powinna być odpowiedzialna obrona cywilna nie istniejąca wg. eksperta. • Informacje o zagrożeniach oraz o sygnałach alarmowych powinny być udostępniane w miejscach publicznych i klatkach schodowych • Relatywnie niski koszt produkcji i kolportażu ulotki. • Ulotka pozwala przekazać więcej treści niż inne środki przekazywania informacji. • Można ją zrobić szybko, dostosowując zawartość do aktualnych wydarzeń. • Szeroki krąg odbiorców reklamy w środkach masowego przekazu, zwłaszcza w radiu i telewizji. • Chatbot jest przydatny podczas udzielania odpowiedzi na zadawane przez interesanta pytania. • Informacja o zagrożeniu musi być powszechna, szybka i właściwie wyeksponowana. Sposób jej dystrybucji powinien uwzględniać sytuację (możliwości przekazu, np.: uszkodzone BTS ograniczą przekaz przez sieć komórkową). Brakuje środków przekazu bezpośredniego – samochody z nagłośnieniem, systemy nagłośnienia zakładowego itp. • Ocenia się, że odsetek ludności nie potrafiący obsługiwać telefonu lub nie będący w jego posiadaniu jest znikomy (szacuje się że jest to kilka procent i wartość ta z roku na rok maleje) stąd należy ocenić że jest to medium wysoce efektywne w zakresie informowania ludności. W połączeniu z geolokalizacją abonenta zapewnia możliwość selektywnego wyboru grupy abonentów i przy założeniu ciągłości działania infrastruktury systemu powiadamiania aktualne rozwiązanie należy ocenić jako wysoce skuteczne. Pomimo powyższego, propozycja uzupełnienia szeroko rozumianego systemu informowania ludności o nowe kanały komunikacji ma również swoje uzasadnienie. Wykorzystanie technologii rozsiewczej (radiowo-telewizyjnej), to nie tylko optymalny stosunek kosztu do efektu, ale również wiarygodności kanału informowania (państwo-obywatel). Pozostałe formy, z uwagi na ich ograniczony zasięg, czas dystrybucji informacji ocenia się raczej jako formy uzupełniające, dla dużych aglomeracji (reklamy w miejscach publicznych i komunikacji miejskiej) lub dla ludzi poszukujących dodatkowej szczegółowej informacji (chatboty).

Źródło: opracowanie własne.

W tabeli 7.2 zaprezentowano opinię ekspertów na temat zaproponowanych rozwiązań, oraz sugestie na temat ich udoskonalenia. Dane zawarte w tabeli pokrywają się z zaproponowanymi w rozprawie możliwościami wykorzystania technologii oraz stanowią uzasadnienie istotności wykorzystania zaproponowanych rozwiązań w zarządzaniu kryzysowym.

3. Jak ocenia Pani/Pan przydatność poradników w formie papierowej zawierających informacje o zagrożeniach rozszerzonych o klasyfikację zagrożeń z uwzględnieniem działań niezbędnych do wykonania oraz tabeli zasobów w aspekcie kreowania świadomości sytuacyjnej ludności na temat zagrożeń (wyk. 7.3).



Wykres 7.3. Opinia ekspertów na temat rozszerzenia poradników w formie papierowej zawierających informacje o zagrożeniach rozszerzonych o klasyfikację zagrożeń z uwzględnieniem działań niezbędnych do wykonania oraz tabeli zasobów w aspekcie kreowania świadomości sytuacyjnej ludności na temat zagrożeń (N = 7)

Źródło: opracowanie własne

Na podstawie odpowiedzi ekspertów można wywnioskować, że propozycja rozszerzenia poradników w formie papierowej o tabelę zasobów jak i klasyfikację zagrożeń oceniona została bardzo pozytywnie. I tak 4 (57,1%) ekspertów uznało przydatność zaproponowanego rozwiązania na średnim poziomie, 1 (14,3%) na wysokim oraz 1 (14,3%) na bardzo wysokim. Spośród ekspertów tylko 1 osoba (14,3%) oceniła tego typu rozwiązania bardzo nisko, a jako argument wskazała, że obywatele nie preferują rozwiązań, które wymagają form wymagających czytania długich instrukcji i opisów. Zaproponowane w rozprawie rozwiązanie nie wymaga od obywatela analizowania wielostronicowego tekstu. Omówione w koncepcji rozwiązania zawierają istotne informacje na temat sposobów radzenia się z zagrożeniami i zachowania się w momencie ich wystąpienia formie tabeli.

W tabeli 7.3 przedstawiono opinię ekspertów na temat zaproponowanego rozwiązania oraz kierunki ich rozwoju.

Tabela 7.3. Przydatność poradników w formie papierowej zawierających informacje o zagrożeniach rozszerzonych o klasyfikację zagrożeń z uwzględnieniem działań niezbędnych do wykonania (tab. 1) oraz tabeli zasobów (tab. 2) w aspekcie kreowania świadomości sytuacyjnej ludności na temat zagrożeń (N = 7)

Odpowiedzi respondentów
• Należy prowadzić okresową aktualizację opracowanych już poradników. • Tego typu publikacje nie cieszą się dużym zainteresowaniem wśród obywateli. Wykorzystują je raczej osoby współpracujące w ramach działań antykryzysowych ze służbami odpowiedzialnymi za niesienie pomocy. • Przydatność poradników jako środka prewencji, budowania świadomości ocenić można wysoko. • W sytuacji wystąpienia zagrożeń ich przydatność wydaje się być dyskusyjna. • W okresie pokoju oraz braku zagrożeń naturalnych przydatność poradników w formie elektronicznych jest wystarczająca. W sytuacja kryzysowych, w których występują różne kategorie zagrożeń dostępne na stronach internetowych poradniki mogą okazać się niedostępne w momencie zaistnienia zagrożenia na skutek uszkodzenia infrastruktury krytycznej/teleinformatycznej. W tym kontekście przydatność poradników w formie papierowej, jako rezerwowych zawierających informacje o zagrożeniach rozszerzonych o klasyfikację zagrożeń z uwzględnieniem działań niezbędnych do wykonania oraz tabeli zasobów w aspekcie kreowania świadomości sytuacyjnej ludności na temat zagrożeń (postrzeganie, zrozumienie, prognozowanie należy uznać za konieczną. • Człowiek nie lubi czytać informacji oraz poradników. • Trzeba ćwiczyć zachowania przy pomocy treningów na sygnały alarmowania i ostrzegania w formie głosowej i wizualnej • Niezbędna jest znajomość powstawania i oddziaływania zagrożeń. • Należy określić grupę odbiorców do której ma być kierowana forma papierowa – bardzo często do tzw. grupy wykluczonej cyfrowo. • Informacja musi mieć formę prostą i zrozumiałą i spełniać wymagania dostępności zgodnie z WCAG 2.1, który opiera się na 4 zasadach**:** postrzegalność, funkcjonalność, zrozumiałość, solidność (w polskim i unijnym prawie określana jako kompatybilność). • Budowanie świadomości społeczeństwa w odniesieniu do reagowania ludności na sytuacje kryzysowe powinno być wpisane w system edukacji społeczeństwa i odbywać się zarówno na każdym poziomie szkolnictwa (w relacji szkoła - uczeń) jak również wymagań kodeksowych każdego stosunku pracy (w relacji pracodawca - pracownik). W tym rozumieniu poradniki, dostępne również powszechnie, jako pomoce dydaktyczne jak i do samodzielnego wykorzystania, traktować należy jako doskonałą formę kreowania świadomości społecznej w zakresie sytuacji kryzysowych zarówno w odniesieniu do określonego terytorium czy określonego rodzaju sytuacji.

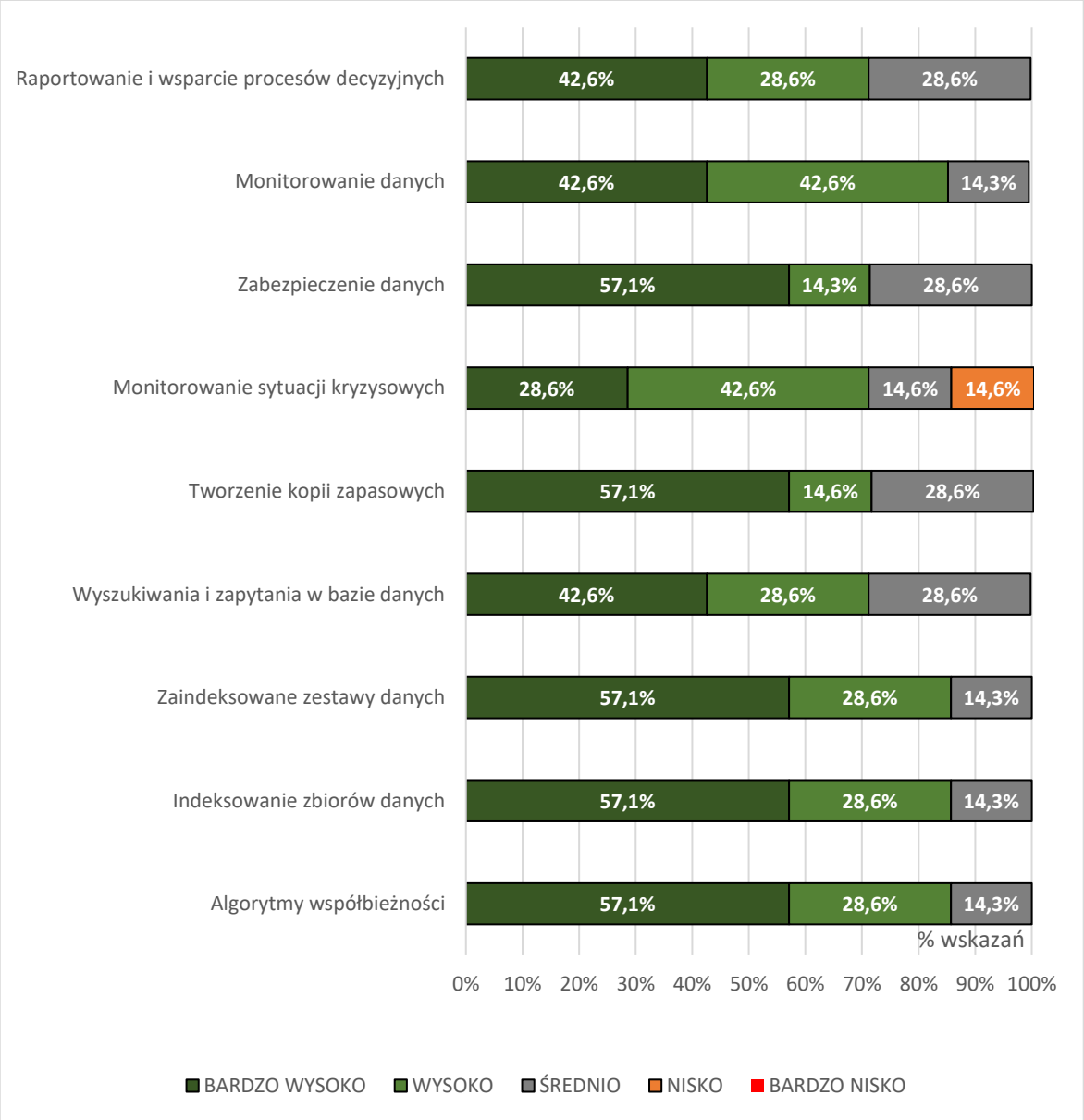
Źródło: opracowanie własne.

Pomimo iż tego typu sposoby edukowania w opinii niektórych ekspertów może okazać się nie przydatne w czasie zagrożenia, ponieważ zawarte informacje mogą wydawać się oczywiste warto rozważyć tego typu rozwiązanie, aby ułatwić przygotowanie się do zagrożenia, które może wywołać chaos, lęk oraz dezinformacje utrudniające podejmowanie decyzji.

4. Jak ocenia Pani/Pan możliwości wykorzystania technologii *OLTP* (wykres 7,4), *OLAP* (wykres 7.5), *Business Inteligence* (wykres 7.6) oraz *Big Data* (wykres 7.7) w odniesieniu do zwiększania poziomu świadomości sytuacyjnej na temat

zagrożeń, a w konsekwencji do usprawnienia procesu zarządzania kryzysowego.

- OLTP



Wykres 7.4. Opinia ekspertów na temat możliwości wykorzystania technologii *OLTP (N = 7)*

Źródło: opracowanie własne.

Analiza odpowiedzi ekspertów (wykres 7.4) potwierdza przydatność technologii *OLTP* w zarządzaniu kryzysowym. Na podstawie oceny poszczególnych funkcji technologii można określić przydatność zaproponowanego rozwiązania bardzo wysoko, co pokazują dane zawarte na wykresie. Przedstawione ekspertom możliwości wykorzystania *OTLP* takie jak raportowanie i wsparcie procesów decyzyjnych oraz wyszukiwania i zapytania w bazie danych ocenione zostały bardzo wysoko przez 3

ekspertów (42,6%), wysoko przez 2 ekspertów (28,6%) oraz średnio przez 2 ekspertów (28,6%). Funkcjonalność taka jak monitorowanie danych oceniona zostało bardzo wysoko przez 3 ekspertów (42,6%), wysoko przez 3 ekspertów (42,6%), a jeden ekspert ocenił wspomniane rozwiązanie na średni poziomie (1,6%). Zabezpieczenie danych w opinii ekspertów zostało bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez 1 eksperta (14,3%) oraz średnio przez 2 ekspertów (28,6%). W opinii ekspertów rozwiązanie takie jak monitorowanie sytuacji kryzysowych w ocenie ekspertów zostało ocenione bardzo wysoko przez 2 ekspertów (28,6%), wysoko przez 3 ekspertów (42,6%) średnio przez 1 eksperta (14,6%), a 1 z ekspertów (14,6%) ocenił zaproponowane rozwiązanie na niskim poziomie. Ponadto funkcje takie jak zindeksowane zestawy danych, indeksowanie zbiorów danych oraz algorytmy współbieżności w opinii ekspertów zostały ocenione bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez 2 ekspertów (28,6%) oraz średnio przez 1 eksperta (14,6%).

Przedstawione na wykresie wyniki ukazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.4.

W tabeli 7.4 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii OLTP w zarządzaniu kryzysowym oraz kierunki doskonalenia.

Tabela 7.4. Możliwości wykorzystania OLTP

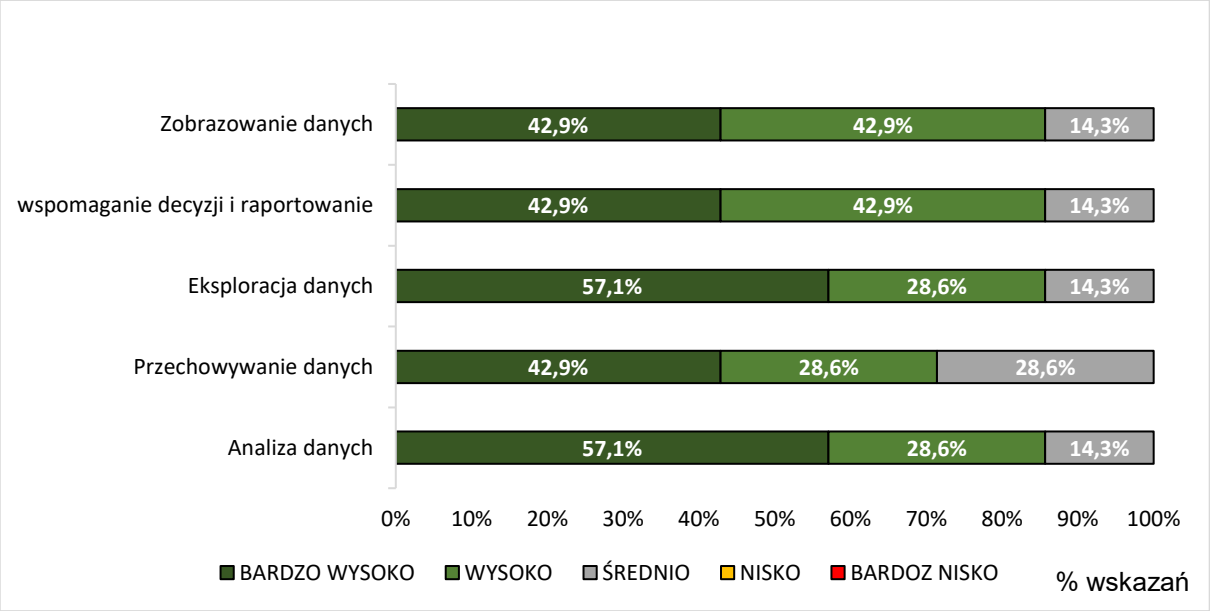
Odpowiedzi respondentów
• *OLTP* w kontekście zarządzania kryzysowego, *OLTP* może być używany do gromadzenia i przetwarzania informacji o bieżącej sytuacji, takiej jak ilość poszkodowanych, lokalizacja i rozmiar zniszczeń, informacje o zasobach, itp. Dzięki temu *OLTP* może pomóc w szybkim i skutecznym zarządzaniu kryzysowym poprzez zapewnienie w czasie rzeczywistym informacji, które są kluczowe dla podejmowania decyzji. Za pomocą *OLTP* można np.: o Gromadzić i monitorować informacje o zasobach o Analizować bieżącą sytuację poprzez gromadzenie informacji o liczbie poszkodowanych, nieruchomościach lub infrastrukturze, a także o wszelkich innych zdarzeniach związanych z kryzysem. o Zarządzać komunikacją między różnymi służbami ratunkowymi • *OLTP* umożliwia szybką reakcję na sytuacje kryzysowe i umożliwia podejmowanie skutecznych działań. • Zaproponowane technologie, ze względu na ich istotę i komplementarność, ocenić należy jako wysoce zasadne. Możliwość gromadzenia danych bieżących z zachowaniem historyczności danych oraz prognozowania w połączeniu z zapewnieniem przetwarzania wielkoskalowych wolumenów danych tworzy optymalne warunki dla procesów zarządzania kryzysowego. W efekcie proponowanych technologii można uzyskać spójne, niesprzeczne i wiarygodne dane a w konsekwencji wiedzę pozwalającą na właściwą ocenę stanu bieżącego oraz zwiększenie prawdopodobieństwa podjęcia adekwatnych działań do sytuacji kryzysowych. Stąd generalnie wysoka ocena każdej technologii i każdej wyróżnionej funkcji, bez względu na zasadnicze natywne funkcje dostarczane przez praktyczne rozwiązania poszczególnych technologii.

Źródło: opracowanie własne.

Zarówno dane w tabeli 7.4 jak i ocena ekspertów (wyk. 7.4) wskazują na ogromny potencjał zaproponowanego rozwiązania. Uzasadnienie słuszności wykorzystania

technologii OLTP zawarte w tabeli 7.4 pokrywa się z rozwiązaniami zaproponowanymi w rozdziale VI, a także rozszerza je o nowe możliwości.

- OLAP



Wykres 7.5. Opinia ekspertów na temat możliwości wykorzystania technologii OLAP

Źródło: opracowanie własne.

Analiza odpowiedzi ekspertów (wyk. 7.5) potwierdza przydatność technologii *OLAP* w zarządzaniu kryzysowym. W opinii ekspertów rozwiązania takie jak zobrazowanie danych oraz wspomaganie decyzji raportowania w zdaniem ekspertów ocenione zostały bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 3 ekspertów (42,9%), a 1 z ekspertów (14,3%) ocenił wskazane funkcje technologii *OLAP* na średnim poziomie. Przechowywanie danych ocenione zostało przez 3 ekspertów (42,9%) na bardzo wysokim poziomie, przez 2 ekspertów (28,6%) na wysokim poziomie oraz przez 2 (28,6%) na niskim. Ponadto rozwiązanie takie jak eksploatacja danych oraz analiza danych w opinii ekspertów została oceniona bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez 2 ekspertów (28,6%) oraz nisko przez 1 eksperta (14,9%). Wysoka ocena funkcjonalności zaproponowanych rozwiązań wskazuje na potrzebę wykorzystania technologii *OLAP* w zarządzaniu kryzysowym.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.5.

W tabeli 7.5 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii OLAP w zarządzaniu kryzysowym.

Tabela 7.5. Możliwości wykorzystania, OLAP

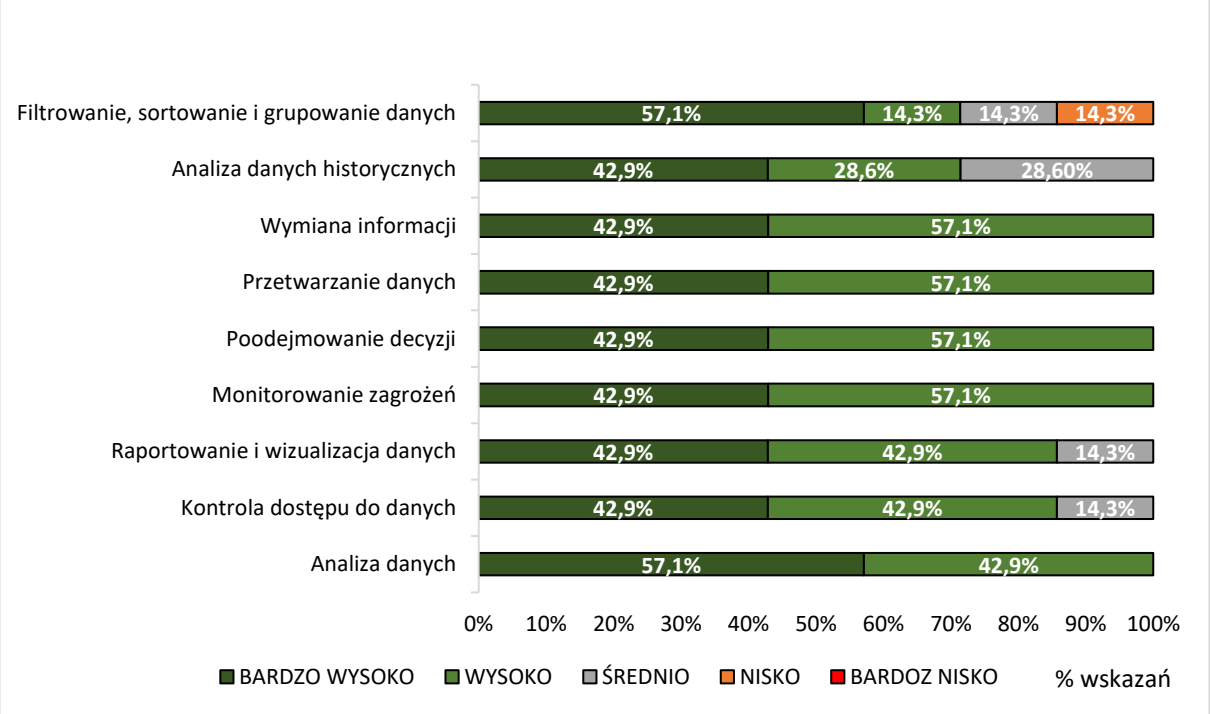
Odpowiedzi respondentów

• OLAP może być wykorzystywany do:
  ○ analizy i wizualizacji danych z różnych źródeł, takich jak kamery przemysłowe, systemy monitoringu i czujniki,
  ○ analizy trendów i prognozowania przyszłych wydarzeń na podstawie zebranych danych
• Zaproponowane technologie, ze względu na ich istotę i komplementarność, ocenić należy jako wysoce zasadne. Możliwość gromadzenia danych bieżących z zachowaniem historyczności danych oraz prognozowania w połączeniu z zapewnieniem przetwarzania wielkoskalowych wolumenów danych tworzy optymalne warunki dla procesów zarządzania kryzysowego. W efekcie proponowanych technologii można uzyskać spójne, niesprzeczne i wiarygodne dane a w konsekwencji wiedzę pozwalającą na właściwą ocenę stanu bieżącego oraz zwiększenie prawdopodobieństwa podjęcia adekwatnych działań do sytuacji kryzysowych. Stąd generalnie wysoka ocena każdej technologii i każdej wyróżnionej funkcji, bez względu na zasadnicze natywne funkcje dostarczane przez praktyczne rozwiązania poszczególnych technologii.

Źródło: opracowanie własne.

Zarówno dane w tabeli 7.5 jak i ocena ekspertów (wyk. 7.5) wskazują na potencjał zaproponowanego rozwiązania. W tabeli 7.5 eksperci wyrazili opinię na temat zaproponowanego rozwiązania wskazując możliwości wykorzystania technologii OLAP w zarządzaniu kryzysowym. Wskazana przez ekspertów perspektywa rozwoju Systemu Zarządzania Kryzysowego poprzez wykorzystanie *OLAP* pokrywa się z kierunkami rozwoju zaproponowanymi w rozprawie, a także wskazuje możliwości udoskonalenia zaproponowanych w koncepcji rozwiązań.

- Business Inteligence



Wykres 7.6. Opinia ekspertów na temat możliwości wykorzystania technologii Business Inteligence (N = 7)

Źródło: opracowanie własne.

Analiza odpowiedzi ekspertów (wyk. 7.6) potwierdza przydatność technologii Busines Inteligence w zarządzaniu kryzysowym. W opinii ekspertów funkcja taka jak filtrowanie, sortowanie i grupowanie danych oceniona została bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez 1 eksperta (14,9%), średnio przez 1 eksperta (14,9%) oraz nisko przez 1 eksperta (14,9%). Funkcja taka jak analiza danych historycznych w opinii ekspertów została oceniona bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 2 ekspertów (28,6%) oraz średnio przez 2 ekspertów (28,6%). Rozwiązania takie jak wymiana informacji, przetwarzanie danych, podejmowanie decyzji oraz monitorowanie zagrożeń w opinii ekspertów zostały ocenione bardzo wysoko przez 3 ekspertów (42,9%) oraz wysoko przez 4 ekspertów (57,1%). Ponadto wykorzystanie takiej funkcjonalności jak raportowanie i wizualizacja kontrola danych oraz kontrola dostępu do danych w opinii ekspertów została oceniona bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 2 ekspertów (42,9%), a przez 1 (14,3%) eksperta na średnim poziomie. Eksperci ocenili również taką funkcję jak analiza danych i tak 4 ekspertów (57,1%) oceniło zaproponowaną funkcję bardzo wysoko, a 3 (42,9%) wysoko.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.6.

Tabela 7.6. Możliwości wykorzystania, Business Intelligence (N = 7)

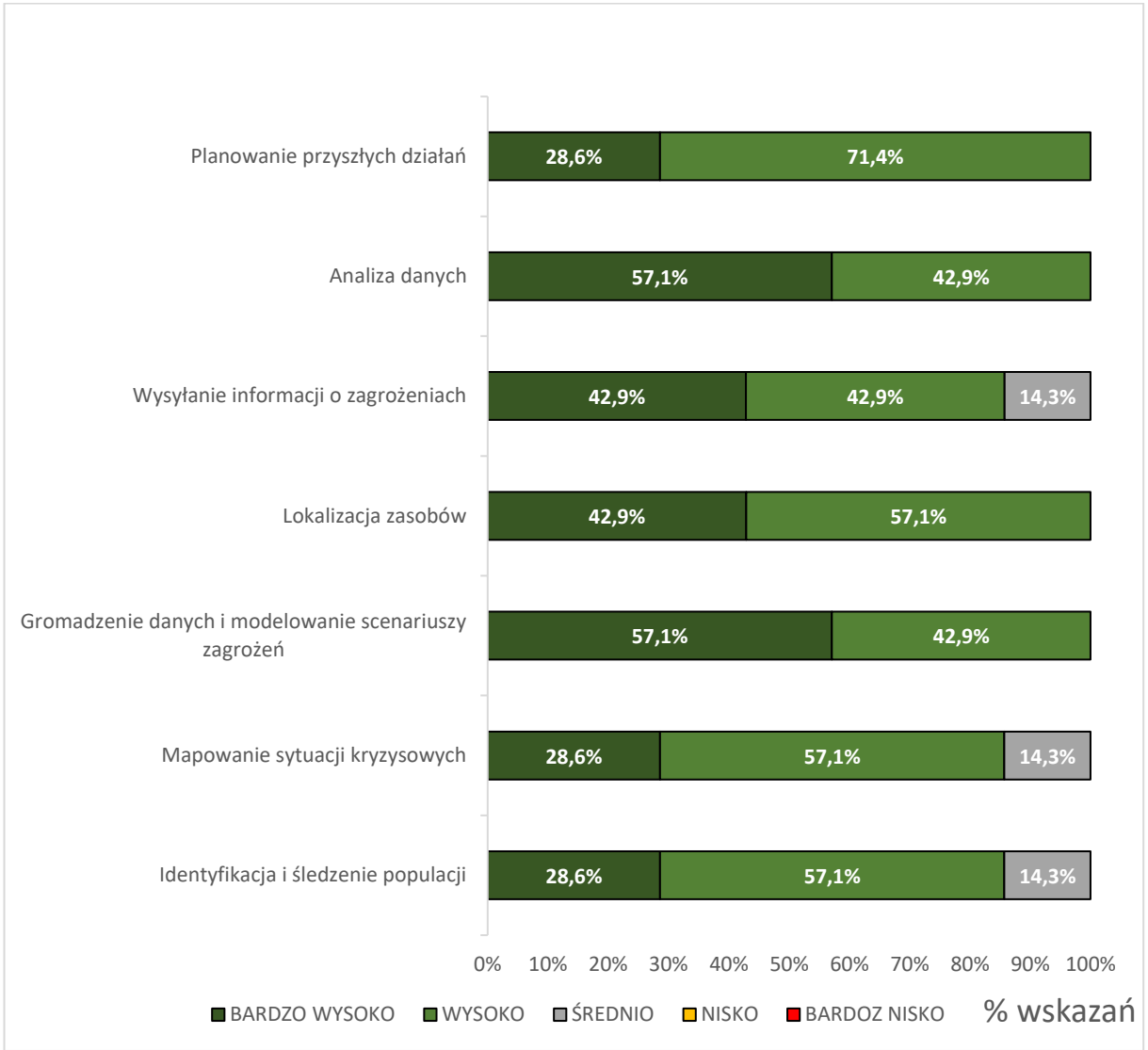
Odpowiedzi respondentów
• BI może być też wykorzystywany do: o zbierania i analizowania danych z różnych źródeł, takich jak systemy monitorowania, różnego rodzaju czujniki, media społecznościowe, czy dane ekonomiczne. o do szybkiego przetwarzania dużych ilości danych w czasie o do analizy trendów i prognozowania przyszłych wydarzeń na podstawie zebranych danych. o do analizę danych pochodzących z systemów monitorowania zdrowia publicznego • proces implementacji technologii jest na początku drogi, zarówno ze względów technologicznych, zasobów osobowych (brak wykfalifikowanych kadr IT), oraz ze względu na brak kontraktów na zabezpieczenie tych obszarów. • Baza danych o zagrożeniach musi być przemyślana i zawierać istotne praktyczne dane niezbędne do wsparcia procesu decyzyjnego. • Zaproponowane technologie, ze względu na ich istotę i komplementarność, ocenić należy jako wysoce zasadne. Możliwość gromadzenia danych bieżących z zachowaniem historyczności danych oraz prognozowania w połączeniu z zapewnieniem przetwarzania wielkoskalowych wolumenów danych tworzy optymalne warunki dla procesów zarządzania kryzysowego. W efekcie proponowanych technologii można uzyskać spójne, niesprzeczne i wiarygodne dane a w konsekwencji wiedzę pozwalającą na właściwą ocenę stanu bieżącego oraz zwiększenie prawdopodobieństwa podjęcia adekwatnych działań do sytuacji kryzysowych. Stąd generalnie wysoka ocena każdej technologii i każdej wyróżnionej funkcji, bez względu na zasadnicze natywne funkcje dostarczane przez praktyczne rozwiązania poszczególnych technologii.

Źródło: opracowanie własne.

W tabeli 7.6 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii *Business Inteligence* w zarządzaniu kryzysowym.

Zarówno dane w tabeli 7.6 jak i ocena ekspertów (wyk. 7.6) wskazują na potencjał zaproponowanego rozwiązania. W tabeli 7.6 eksperci wyrazili opinię na temat zaproponowanego rozwiązania wskazując możliwości wykorzystania technologii *Business Inteligence* w zarządzaniu kryzysowym. Zaproponowane przez ekspertów kierunki doskonalenia Systemu Zarządzania Kryzysowego poprzez wykorzystanie *Business Inteligence* pokrywa się z rozwiązaniami zaproponowanymi w rozprawie, a także wskazuje na możliwości udoskonalenia zaproponowanych w koncepcji rozwiązań.

- Big Data



Wykres 7.7. Opinia ekspertów na temat możliwości wykorzystania technologii Big Data (N = 7)

Źródło: opracowanie własne.

Analiza odpowiedzi ekspertów (wyk. 7.7) potwierdza przydatność technologii *Big Data* w zarządzaniu kryzysowym. Spośród zaproponowanych funkcji technologii *Big Data* funkcja taka jak planowanie przyszłych działań oceniona została bardzo wysoko przez 2 ekspertów (28,6%) oraz wysoko przez 5 ekspertów (71,4%). W opinii ekspertów funkcjonalność taka jak analiza danych oraz gromadzenie danych i modelowanie scenariuszy zagrożeń oceniona została bardzo wysoko przez 4 ekspertów (57,1%) oraz wysoko przez 3 ekspertów (42,9%). Funkcja taka jak wysyłanie informacji o zagrożeniach oceniona została przez 3 ekspertów (42,9%) na bardzo wysokim, 3 ekspertów (42,9%) oceniło ją na wysokim poziomie, natomiast 1 ekspert (14,9%) ocenił na średnim poziomie. Lokalizacja zasobów oceniona została na bardzo wysokim poziomie przez 3 ekspertów (42,9%) oraz na wysokim przez 4 (57,1%). Ponadto funkcje takie jak mapowanie sytuacji kryzysowych oraz identyfikacja i śledzenie populacji oceniona została na bardzo wysokim poziomie przez 2 ekspertów, 3 ekspertów (57,1%) oceniło na wysokim poziomie, a 1 ekspert (14,9%) ocenił na niskim poziomie.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.7.

W tabeli 7.7 przedstawiono opinię ekspertów na temat zaproponowanych rozwiązań oraz kierunki doskonalenia.

Tabela 7.7. Możliwości wykorzystania, Big Data (N = 7)

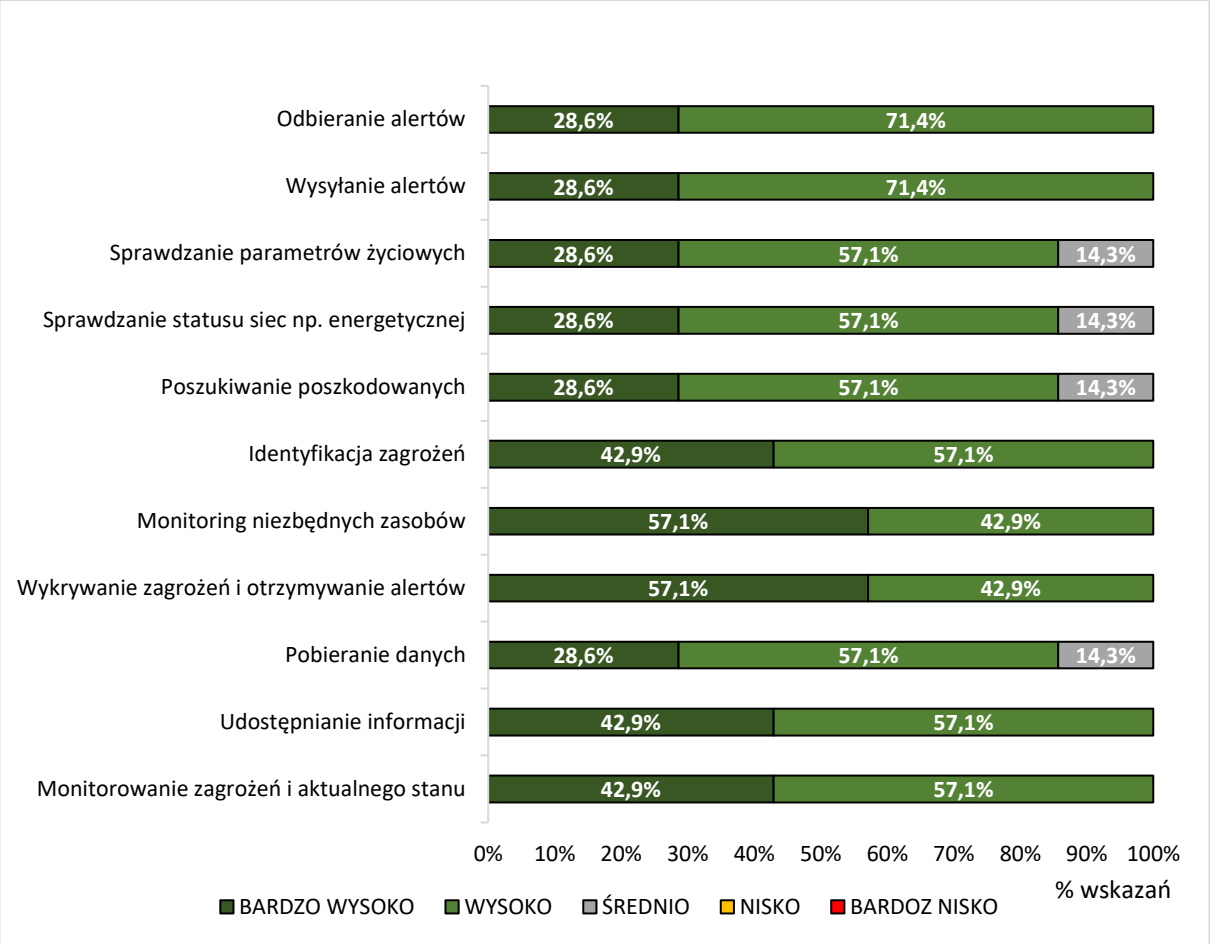
Odpowiedzi respondentów
• *Big Data* może być przydatna do: o wiedzy czerpanej z dużych zbiorów danych właśnie do utrzymania odpowiedniej jakości i skuteczności pierwszej fazy procesu zarządzania kryzysowego, a więc prewencji i ostrzegania. o do odnajdywania oraz neutralizowania syndromów i pierwszych objawów kryzysu lub nieciągłości. • Zaproponowane technologie, ze względu na ich istotę i komplementarność, ocenić należy jako wysoce zasadne. Możliwość gromadzenia danych bieżących z zachowaniem historyczności danych oraz prognozowania w połączeniu z zapewnieniem przetwarzania wielkoskalowych wolumenów danych tworzy optymalne warunki dla procesów zarządzania kryzysowego. W efekcie proponowanych technologii można uzyskać spójne, niesprzeczne i wiarygodne dane a w konsekwencji wiedzę pozwalającą na właściwą ocenę stanu bieżącego oraz zwiększenie prawdopodobieństwa podjęcia adekwatnych działań do sytuacji kryzysowych. Stąd generalnie wysoka ocena każdej technologii i każdej wyróżnionej funkcji, bez względu na zasadnicze natywne funkcje dostarczane przez praktyczne rozwiązania poszczególnych technologii.

Źródło: opracowanie własne.

Dane zawarte w tabeli 7.7 pokrywają się z rozwiązaniami zaproponowanymi w rozprawie, a eksperci ocenili je jako wysoce zasadne.

5. Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania Internetu Rzeczy (IoT, czyli łączenia różnych urządzeń/sensorów/czujników z systemami nadrzędnymi lub między sobą) w zarządzaniu kryzysowym oraz w kreowaniu świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli?

a. Dla zespołów zarządzania kryzysowego



Wykres 7.8. Wykorzystanie *IoT* przez ZZK (odpowiedzi ekspertów) (N = 7)

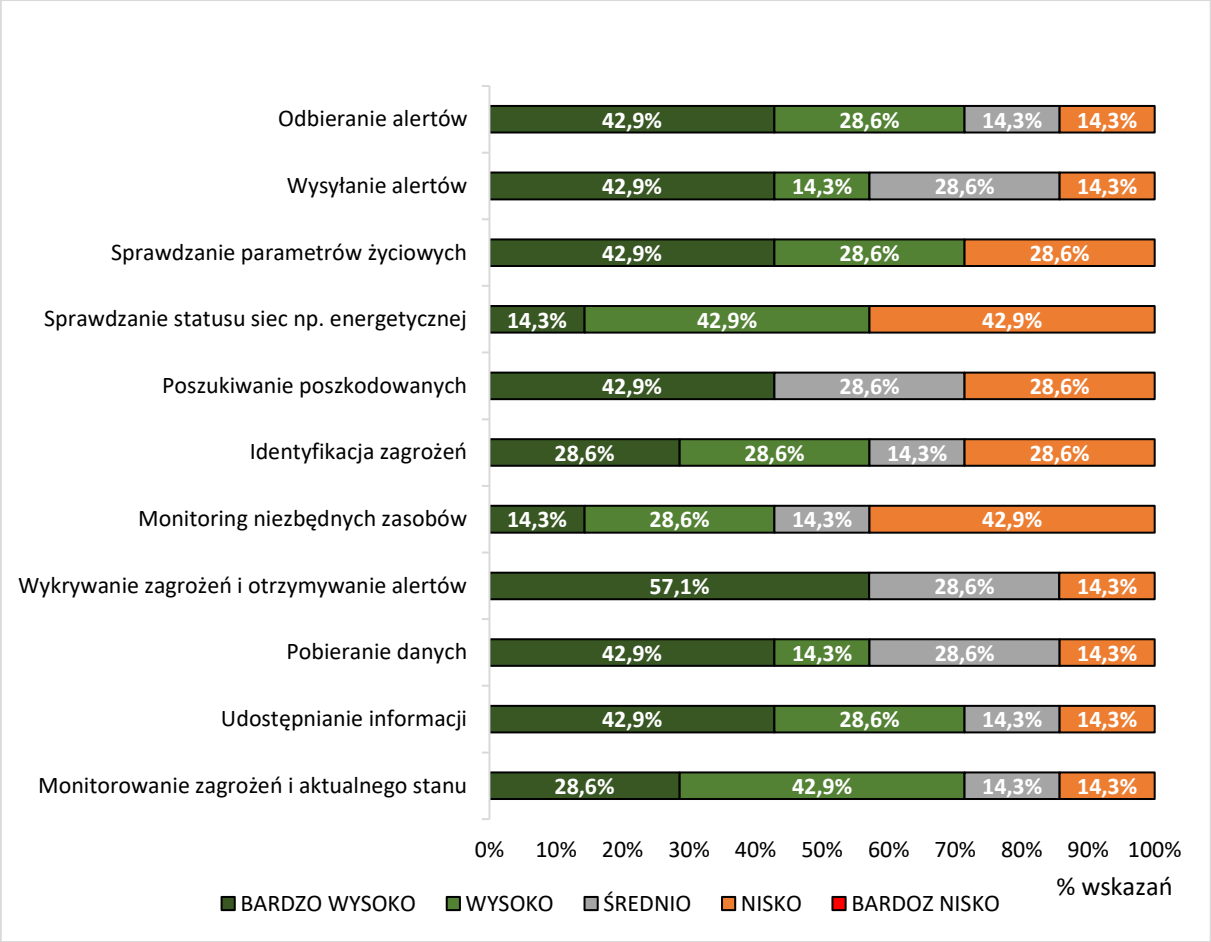
Źródło: opracowanie własne.

Przedstawiona na wykresie 7.8 funkcjonalność Internetu Rzeczy dla zespołów zarządzania kryzysowego została oceniona przez ekspertów bardzo wysoko, co pokazuje jak istotną rolę w zarządzaniu kryzysowym może odegrać technologia IoT. W opinii ekspertów funkcje takie jak odbieranie alertów oraz wysyłanie alertów ocenione zostało bardzo wysoko przez 2 ekspertów (28,6%), a 5 ekspertów (71,4%) oceniło przydatność zaproponowanej technologii na wysokim poziomie. Funkcje takie jak sprawdzanie parametrów życiowych, sprawdzanie statusu sieci np. energetycznej, poszukiwanie poszkodowanych oraz pobieranie danych ocenione zostały bardzo wysoko przez 2 ekspertów (28,6%), 4 ekspertów (57,1%) oceniło zastosowanie wy-

korzystanych rozwiązań wysoko, a 1 ekspert średnio (14,3%). Identyfikacja zagrożeń w opinii ekspertów oceniona została bardzo wysoko przez 3 osoby (42,9%), wysoko przez 4 osoby (57,1%). Monitoring niezbędnych zasobów oraz wykrywanie zagrożeń i otrzymywanie alertów ocenione zostało przez ekspertów bardzo wysoko przez 4 osoby (57,1%) oraz wysoko przez 3 osoby (42,9%). Ponadto funkcjonalność taka jak udostępnianie informacji oraz monitorowanie zagrożeń i aktualnego stanu oceniona została bardzo wysoko przez 3 ekspertów (42,9%) oraz wysoko przez 4 ekspertów (57,1%).

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.8.

b. Dla obywateli



Wykres 7.9. Wykorzystanie IoT przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło: opracowanie własne.

Na wykresie 7.9 przedstawiono opinię ekspertów na temat możliwości wykorzystania IoT przez obywateli. Zdania na temat funkcjonalności Internetu Rzeczy są podzielone. W opinii ekspertów funkcje takie jak odbieranie alertów oraz udostępnianie informacji ocenione zostały bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 2 ekspertów (28,6%), średnio przez 1 eksperta (14,9%) oraz 1 z ekspertów (14,9%) ocenił zaproponowane rozwiązanie na niskim poziomie. Funkcjonalność taka jak wysyłanie alertów oraz pobieranie danych ocenione zostały na bardzo wysokim poziomie przez 3 ekspertów (42,9%), na wysokim przez 1 eksperta (14,3%), 2 ekspertów (28,6%) oraz 1 (14,3%) na niskim. Sprawdzanie parametrów życiowych oraz poszukiwanie poszkodowanych ocenione zostało przez 3 osoby (42,9%) na bardzo wysokim poziomie, 2 osoby (28,6%) oceniły zaproponowaną funkcjonalność na średnim poziomie oraz 2 (28,6%) na niskim. Monitoring niezbędnych zasobów oceniony został bardzo wysoko przez 1 eksperta (14,9%), wysoko przez 2 ekspertów (28,6%), średnio przez 1 eksperta (14,9%), a 3 (42,9%) oceniło zastosowanie monitoringu na niskim poziomie. Ocenie poddano również wykrywanie zagrożeń i otrzymywanie alertów i tak w opinii ekspertów funkcjonalność ta została oceniona bardzo wysoko przez osoby (57,1%), średnio przez 2 osoby (28,6%) oraz nisko przez 1 osobę (14,3%). Ponadto według ekspertów funkcja taka jak monitorowanie zagrożeń i aktualnego stanu oceniona została bardzo wysoko przez 2 osoby (28,6%), wysoko przez 3 osoby (42,9%), średnio przez 1 osobę (14,3%) oraz nisko przez 1 osobę (14,3%).

Przedstawione na wykresie wyniki pokazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.8.

W tabeli 7.8 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii IoT w zarządzaniu kryzysowym przez zespoły zarządzania kryzysowego oraz obywateli i wskazano kierunki doskonalenia zaproponowanych rozwiązań IoT, które zdaniem ekspertów mogą usprawnić zarządzanie kryzysowe oraz zwiększyć poziom świadomości sytuacyjnej obywateli oraz członków zespołów zarządzania kryzysowego. Pomimo iż większość ekspertów oceniła bardzo wysoko wykorzystanie Internetu Rzeczy to zdaniem niektórych z nich część rozwiązań takich jakich jak sprawdzanie statusu np. sieci energetycznej lub monitoring zasobów jest nieprzydatny dla obywateli. Ponadto funkcje takie jak odbieranie alertów, wysyłanie alertów lub identyfikacja zagrożeń w opinii niektórych ekspertów również określone zostały jako nieprzydatne. Niemniej jednak należy zwrócić uwagę na fakt, że w przypadku urzą-

dzeń IoT czujniki dla zespołów zarządzania kryzysowego oraz obywateli różnią się między sobą.

Tabela 7.8. Wykorzystania Internetu Rzeczy (IoT, czyli łączenia różnych urządzeń/sensorów/czujników z systemami nadrzędnymi lub między sobą) w zarządzaniu kryzysowym oraz w kreowaniu świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli (N = 7)

Odpowiedzi respondentów

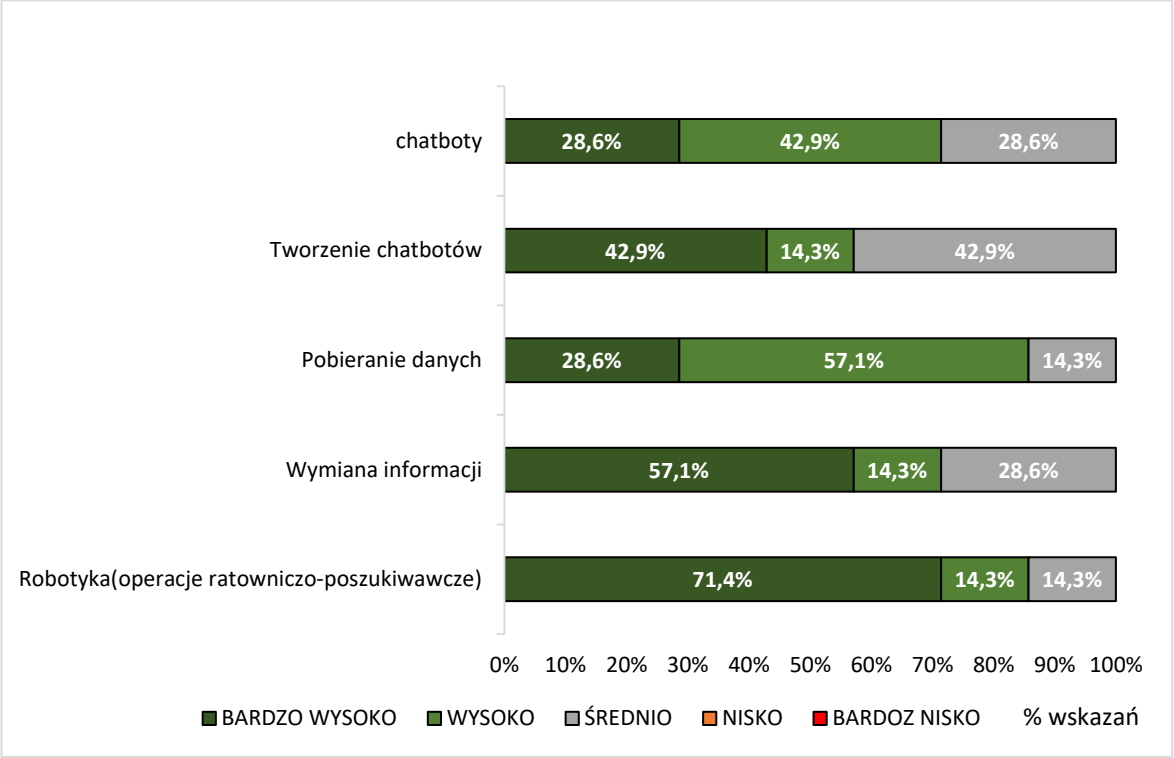
• Dzięki *IoT* możliwe jest:
  o Monitorowanie i wczesne wykrywanie sytuacji kryzysowych.
  o Koordynowanie działań ratunkowych: Dzięki IoT można koordynować i monitorować działania ratunkowe, np. poprzez wykorzystanie urządzeń do komunikacji między służbami ratowniczymi czy włączenie dronów do dostarczania sprzętu lub leków na tereny trudno dostępne.
  o Optymalizowanie działań logistycznych: IoT może pomóc w optymalizacji działań logistycznych, umożliwiając np. szybsze i bardziej efektywne dostarczanie pomocy medycznej czy żywności na tereny kryzysowe.
• Dzięki tej technologii otoczenie obywatela może zostać „wpięte" w system alarmowania, co może zostać wykorzystane do przekazywania precyzyjnych instrukcji odnośnie sposobu zachowania w poszczególnych sytuacjach kryzysowych. Ponadto, poprzez stworzenie możliwości oddziaływania na otoczenie obywatela rozszerzony zostaje wachlarz działań jakie mogą zostać podjęte dla zażegnania sytuacji kryzysowej
• Jest to jedna z technologii przed którą ogromna przyszłość jednak mocno powiązana z możliwościami technicznymi wdrażanych nowych rozwiązań w zakresie technologii mobilnych – sieci 5G i 6G (perspektywa 10-15lat).
• Wszystkie wskazane w tabeli funkcje są pożądane i istotne z procesie zarządzania kryzysowego, ale droga do ich implementacji wymaga ogromnych nakładów finansowych oraz integracji wielu rozwiązań w różnych standardach.
• Podobnie jak dla zespołów zarządzania kryzysowego tak dla obywateli możliwość wykorzystania danych z czujników *IoT*, daje sporo możliwości jednak z ciężarem przeniesionym na personalne potrzeby np.: w przypadku seniorów monitorowanie stanu zdrowia osób samotnych w okresie klęsk żywiołowych, ich poszukiwanie.
• Podzielam pogląd doktoranta, iż skuteczne zarządzanie kryzysowe opiera się na wykorzystaniu narzędzi i technologii ICT w celu zwalczania skutków zagrożeń.
• Należy jednak spojrzeć na zarządzanie kryzysowe nie jak na zbiór procedur i technik, jakie należy zastosować w przypadku pojawienia się kryzysu, ale całą siłę i możliwości działania należy skierować na przewidywanie i przeciwdziałanie zagrożeniom,
• Wykorzystanie technologii ICT, w tym *Big Data* wydaje się być jednym z elementów umożliwiających zmianę podejścia, dzięki ogromnemu potencjałowi oraz ciągle nie do końca określonym możliwościom, jakie idą za zastosowaniem zaawansowanych analiz danych.
• Przyjęte przez Doktoranta czynniki do oceny są wg mnie reprezentatywne

Źródło opracowanie własne

W przypadku ZZK czujniki te stanowią zaawansowane technologie w przypadku obywateli mogą to być proste czujniki stanowiące wyposażenie inteligentnego domu. Jednakże w przypadku obu rodzajów czujników funkcjonalność jest do siebie na tyle zbliżona, że zarówno jedne jak i drugie są w stanie wysyłać i odbierać alerty, a na ich podstawie umożliwić identyfikację zagrożeń.

6. Jak ocenia Pani/Pan przedstawione w poniższych tabelach możliwości wykorzystania sztucznej inteligencji w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli?

a. Dla zespołów zarządzania kryzysowego



Wykres 7.10. Wykorzystanie IoT przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło: opracowanie własne.

Analiza odpowiedzi ekspertów (wyk. 7.10) potwierdza przydatność technologii sztucznej inteligencji. W opinii ekspertów funkcja taka jak robotyka(operacje ratowniczo – poszukiwawcze) oceniona została bardzo wysoko przez 5 osób (71,4%), wysoko przez 1 osobę (14,3%) oraz 1 osoba (14,3%) oceniła na średnim poziomie. .Zdaniem ekspertów chatboty ocenione zostały bardzo wysoko przez 2 osoby (28,6%), wysoko przez 3 osoby (42,9%) oraz średnio przez 2 osoby (28,6%). Funkcja tworzenia chatbotów oceniona została bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 1 eksperta (14,3%) oraz na średnim poziomie przez 3 ekspertów (42,9%). Pobieranie danych ocenione zostało bardzo wysoko przez 2 ekspertów (28,6%), wysoko przez 4 (42,9%) oraz średnio przez 1 (14,3%)eksperta. Ponadto eksperci ocenili możliwość wykorzystania takiej funkcji jak wymiana informacji i tak 4 ekspertów oceniło tego typu rozwiązanie bardzo wysoko (57,1%) 1 ekspert wysoko (14,3%) oraz 2 na średnim poziomie (28,6%)

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.9.

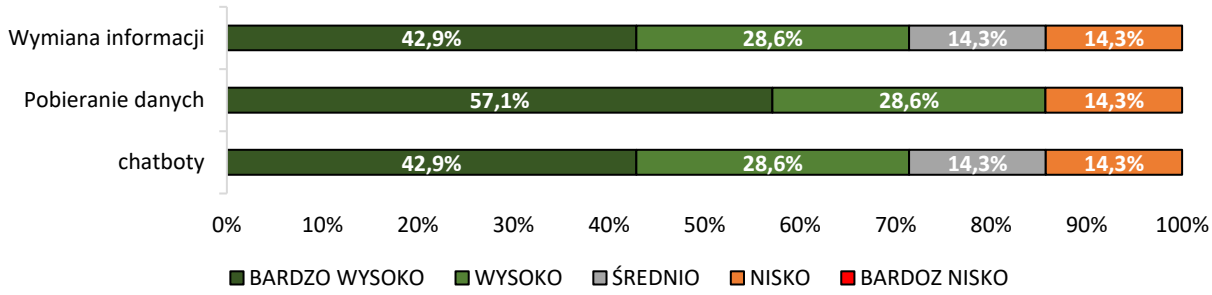
Tabela 7.9. Możliwości wykorzystania sztucznej inteligencji w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli (N = 7)

Odpowiedzi respondentów
• Wykorzystanie SI zwłaszcza przy budowie algorytmów i projektowaniu działań na podstawie dużej ilości danych bazowych będzie miało fundamentalne znaczenie dla przyszłych systemów reagowania kryzysowego i efektywnej budowy scenariuszy postępowania w czasie trwania rzeczywistych działań antykryzysowych. • Rozwój sztucznej inteligencji jest faktem a jej zastosowanie również w systemach zarządzania kryzysowego jest możliwe i wskazane. Ostatecznie, tylko od dojrzałości tej technologii i potrzeb jej faktycznego zastosowania do realizacji danej funkcji uzależnić należy zakres implementacji czy to w robotyce czy w zakresie szeroko rozumianej wymianie informacji.

Źródło opracowanie własne

W tabeli 7.9 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii sztucznej inteligencji w zarządzaniu kryzysowym możliwych do wykorzystania przez zespoły zarządzania kryzysowego.

b. dla obywateli



Wykres 7.11. Wykorzystanie sztucznej inteligencji przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Na wykresie 7.11 przedstawiono opinię ekspertów na temat możliwości wykorzystania sztucznej inteligencji przez obywateli. W opinii ekspertów możliwości wykorzystania chatbotów oraz funkcja wymiany informacji oceniona została bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 2 ekspertów (28,6%), średnio przez 1 eksperta (14,3%) ponadto 1 ekspert (14,3%) ocenił tego typu rozwiązanie na niskim poziomie. Możliwości pobierania danych w opinii ekspertów ocenione zostały bardzo wysoko przez 4 osoby (57,1%), wysoko przez 2 osoby (28,6%) oraz nisko przez 1 osobę (14,3%).

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.10.

W tabeli 7.10 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii sztucznej inteligencji możliwych do wykorzystania przez obywateli.

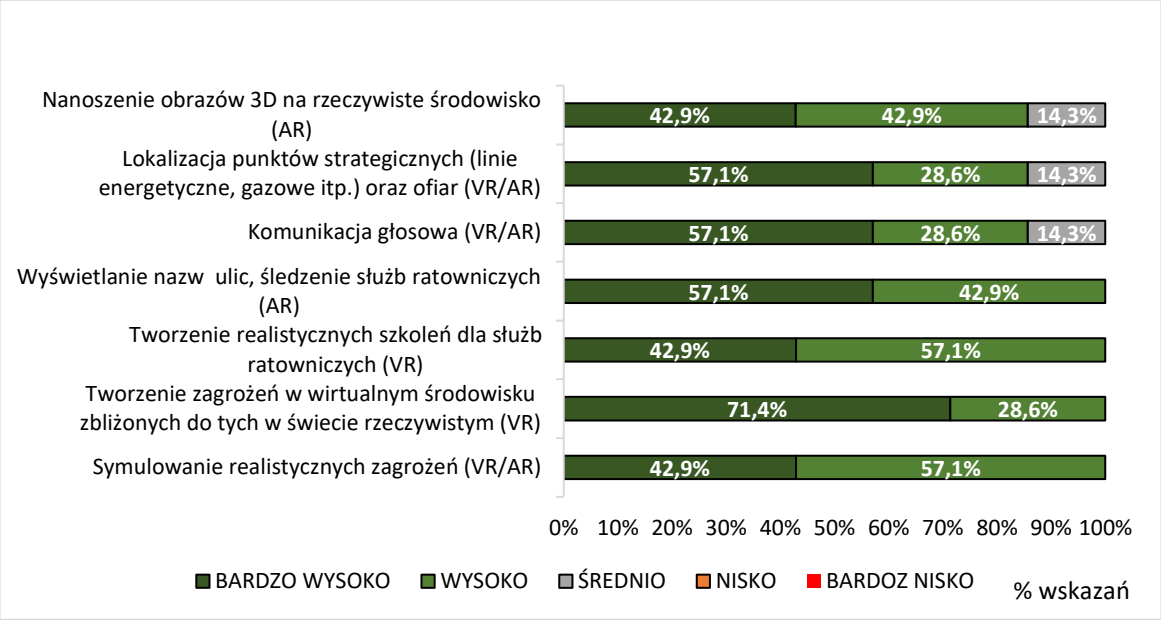
Tabela 7.10. Możliwości wykorzystania sztucznej inteligencji w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli (N = 7)

Odpowiedzi respondentów
• Dla obywatela istotny szybki, dedykowany dostęp do informacji. • Chatboty gwarantują obsługę bez względu na czas i zagrożenia, a wsparcie ich sztuczną inteligencją, maszynowym uczeniem gwarantuje podobny poziom obsługi wolny jednak od presji i emocji właściwych dla osób w stanie zagrożenia. • Z punktu widzenia obywatela, możliwa rola sztucznej inteligencji jest nie mniejsza jak z punktu widzenia zarządzających w zapewnieniu wymienionych.

Źródło opracowanie własne

Opinia ekspertów zawarta w tabeli 7.10 na temat możliwości wykorzystania sztucznej inteligencji przez obywateli pokrywa się z rozwiązaniami zawartymi w rozprawie.

7. Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania *VR* i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego?
    a. Zespoły zarządzania kryzysowego



Wykres 7.12. Wykorzystanie *VR/AR* przez zespoły zarządzania kryzysowego (odpowiedzi ekspertów) (N = 7)
Źródło opracowanie własne

Na wykresie 7.12 przedstawiono opinię ekspertów na temat możliwości wykorzystania technologii *VR/AR* przez zespoły zarządzania kryzysowego. W opinii ekspertów wykorzystanie takiej funkcji *VR/AR* jak nanoszenie obrazów 3D na rzeczywiste środowisko (*AR*) ocenione zostało bardzo wysoko przez 3 osoby (42,9%), wysoko przez 3 osoby (42,9%) oraz średnio przez 1 osobę (14,3%). Zdaniem ekspertów funkcje taki jak lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.)

oraz ofiar (*VR/AR*), a także komunikacja głosowa (*VR/AR*) ocenione zostały bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez 2 ekspertów (28,6%) oraz średnio przez 1 eksperta (14,3%). Wyświetlanie nazw ulic, śledzenie służb ratowniczych (AR) ocenione zostało przez ekspertów bardzo wysoko przez 4 osoby (57,1%) oraz wysoko przez 3 osoby (42,9%). Ponadto tworzenie realistycznych szkoleń dla służb ratowniczych (*VR*) oraz symulowanie realistycznych zagrożeń (*VR/AR*) 3 ekspertów oceniło bardzo wysoko (42,9%), a 4 ekspertów (57,1%) wysoko. Ekspertów poproszono również o ocenę możliwości tworzenia zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym (*VR*). W opinii ekspertów funkcja ta została oceniona bardzo wysoko przez 5 ekspertów (71,4%) oraz wysoko przez 2 (28,6%).

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.11.

W tabeli 7.11 przedstawiono opinię ekspertów na temat zaproponowanych rozwiązań oraz kierunki doskonalenia.

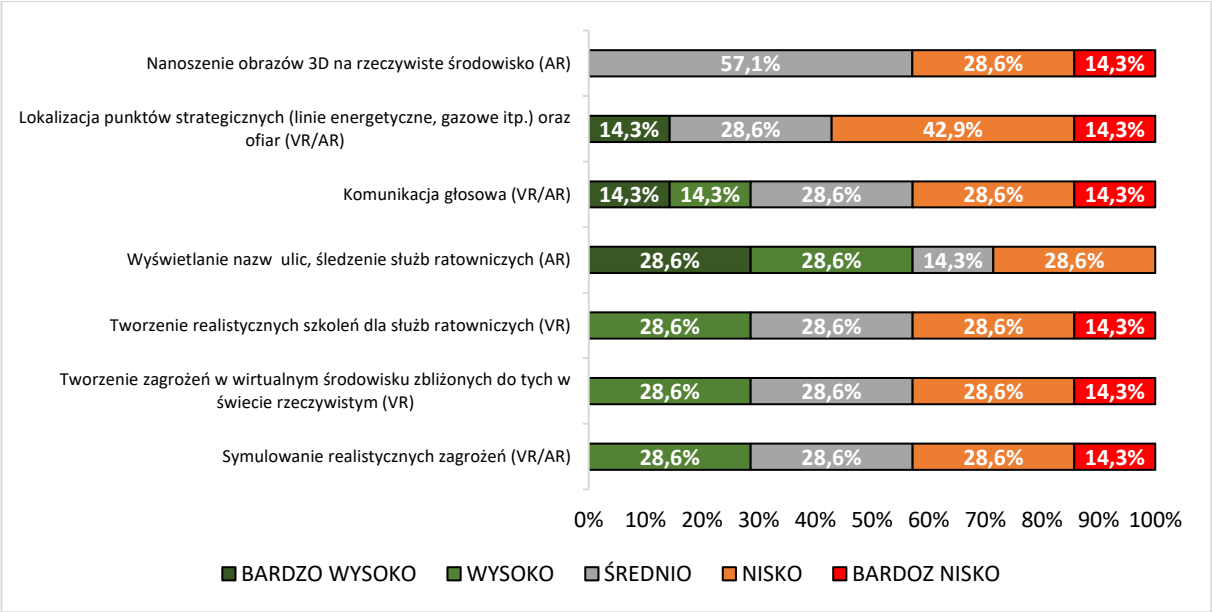
Tabela 7.11. Możliwości wykorzystania VR i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego (N = 7)

Odpowiedzi respondentów
• Wykorzystanie wirtualnej rzeczywistości (*VR*) i rozszerzonej rzeczywistości (AR) w zarządzaniu kryzysowym może zwiększyć efektywność działań i poprawić bezpieczeństwo interwencji. *VR* i AR mogą być wykorzystane np. w celu: o Symulacje szkoleń o Planowaniu działań o Monitorowaniu sytuacji o Komunikacji i koordynacji • *VR* i AR może się przyczynić do ograniczenia kosztów szkolenia choć nie powinien zastępować ćwiczeń praktycznych. • Wprowadzenie w pytaniu tych samych funkcji dla zespołów zarządzania kryzysowego i dla obywateli wydaje się być niezasadne. trudność interpretacji intencji pytania dotyczy np. powodów dla których statystyczny Kowalski miałby lokalizować punkty strategiczne. • Zbudowanie określonych symulatorów dla zespołów zarządzania kryzysowego jest zadaniem niezwykle kosztownym i w mojej ocenie powinno być realizowane na szczeblu centralnym. • Technologie *VR/AR* pozwalają w pełni na zastosowanie rozwiązań w wybranych obszarach zarządzania kryzysowego. • Zaproponowane w powyższej tabeli możliwości wykorzystania *VR* i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego uznaję za zasadne.

Źródło opracowanie własne

W tabeli 7.11 przedstawione zostały możliwości wykorzystania technologii *VR/AR* przez zespoły zarządzania kryzysowego, które zdaniem ekspertów mogą usprawnić działanie zespołów zarządzania kryzysowego. Przedstawione przez ekspertów rozwiązania pokrywają się z zaprezentowanymi w rozprawie.

b. Obywatele



Wykres 7.13. Wykorzystanie *VR/AR* przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Na wykresie 7.13 przedstawiono opinię ekspertów na temat możliwości wykorzystania technologii *VR/AR* przez obywateli. Na podstawie otrzymanych wyników można zauważyć, że zdania ekspertów na temat potencjału technologii są podzielone. Według ekspertów funkcja taka jak nanoszenie obrazów 3D na rzeczywiste środowisko (AR) oceniona została przez 4 osoby (57,1%) na średnim poziomie, 2 osoby oceniły na niskim (28,6%) poziomie oraz 1 (14,3%) na bardzo niskim. Lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar (*VR/AR*) w opinii ekspertów oceniona została bardzo wysoko przez 1 osobę (14,3%), średnio przez 2 osoby (28,6%), nisko przez 3 osoby (42,9%) oraz bardzo nisko przez 1 (14,3%) eksperta. Komunikacja głosowa (*VR/AR*) została oceniona przez 1 osobę (14,3%) bardzo wysoko, 1 ekspert ocenił wysoko (14,3%), 2 ekspertów (28,6%) oceniło na średnim poziomie, 2 na niskim (28,6%) oraz 1 ekspert (14,3%) na bardzo niskim. Ponadto ocenie poddana została możliwość wyświetlania nazw ulic, śledzenie służb ratowniczych (AR), która w opinii ekspertów oceniona została bardzo wysoko przez 2 ekspertów (28,6%), wysoko przez 2 ekspertów (28,6%), 1 ekspert (14,3%) ocenił tego typu funkcje na średnim poziome oraz 2 nisko (28,6%). Ekspertom przedstawiono również takie funkcje jak tworzenie realistycznych szkoleń dla służb ratowniczych (*VR*), tworzenia zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym (*VR*) oraz symulowanie realistycznych zagrożeń (*VR/AR*) i tak w opinii ekspertów 2 osoby (28,6%) oceniły tego typu rozwiązania bardzo wysoko, 2 (28,6%)

osoby na wysokim poziomie, 2 (28,6%) na średnim poziomie oraz 1 (14,3%) na niskim.

Na podstawie otrzymanych wyników można stwierdzić, że część ekspertów dostrzega potencjał w technologii *VR/AR*, inni natomiast uważają, że niektóre funkcje taki jak np. lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar (*VR/AR*), komunikacja głosowa *VR/AR* jest zbędna dla obywateli.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.12.

Tabela 7.12. Możliwości wykorzystania VR i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego (N = 7)

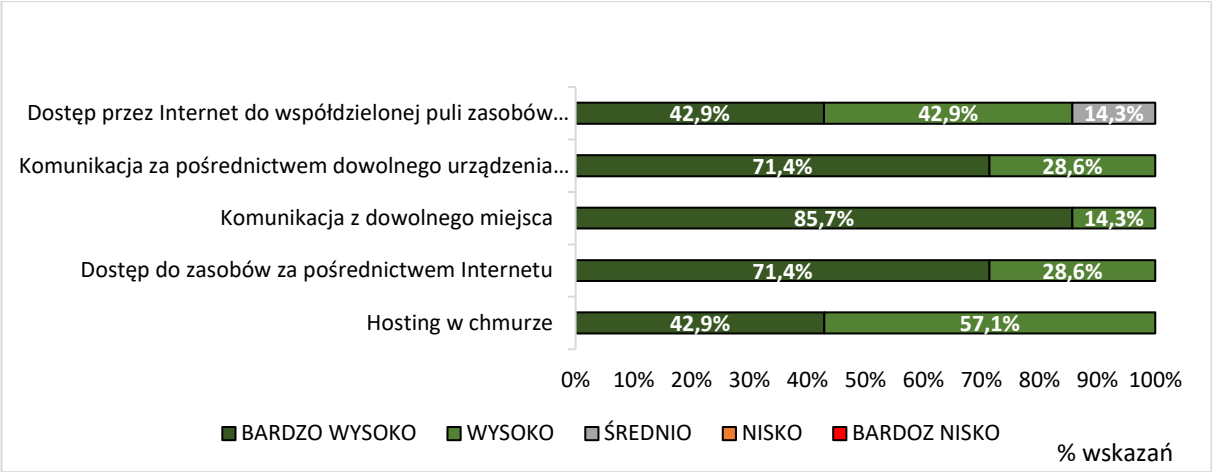
Odpowiedzi respondentów
• Wprowadzenie w pytaniu tych samych funkcji dla zespołów zarządzania kryzysowego i dla obywateli wydaje się być niezasadne. trudność interpretacji intencji pytania dotyczy np. powodów dla których statystyczny Kowalski miałby lokalizować punkty strategiczne. • Wykorzystanie w/w technologii w szkoleniach jest celowe; w innych sytuacjach (szczególnie zagrożeń) ich przydatność jest dyskusyjna. • Możliwości wykorzystania *VR* i AR oceniam bardzo wysoko. • Wykorzystanie *VR* i AR dla obywateli oceniam dość jako średnio potrzebne. Raczej są to rozwiązania ukierunkowane dla zespołów zarządzania kryzysowego. • Ewentualnie zastanowił bym się nad włączeniem *VR* i AR do budowania rozwiązań dla edukacji (szkoły) by uczyć dzieci i młodzież określonych reakcji w wirtualnej rzeczywistości. • Trzeba szukać mechanizmów dotarcia do świadomości poprzez uwiarygodnienie potrzeb i skutków ewentualnych zagrożeń. • System *VR* można użyć bardzo prosto i bez zaawansowanej wiedzy uzyskując bardzo ciekawe efekty edukacyjne. • Zaproponowane w powyższej tabeli możliwości wykorzystania *VR* i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej obywateli uznaję za zasadne.

Źródło opracowanie własne

W tabeli 7.12 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii *VR/AR* możliwych do wykorzystania przez obywateli.

Eksperci bardzo wysoko ocenili możliwości wykorzystania *VR* i AR dla zespołów zarządzania kryzysowego, w przypadku obywateli zwrócono uwagę na fakt, że może stanowić formę szkolenia jak i edukacji przez zabawę dla zróżnicowanych grup wiekowych.

8. Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania chmury obliczeniowej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego i obywateli?
    a. dla zespołów zarządzania kryzysowego



Wykres 7.14. Wykorzystanie CC przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Na wykresie 7.14 przedstawiono opinię ekspertów na temat możliwości wykorzystania technologii *CC* przez zespoły zarządzania kryzysowego. W opinii ekspertów funkcja taka jak dostęp przez internet do współdzielonej puli zasobów obliczeniowych oceniona została bardzo wysoko przez 3 ekspertów (42,9%), wysoko przez 3 ekspertów (42,9%) oraz średnio przez 1 eksperta (14,3%). Funkcje takie jak komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer) oraz dostęp do zasobów za pośrednictwem internetu ocenione zostały przez 5 ekspertów (71,4%) bardzo wysoko oraz wysoko przez 2 ekspertów (28,6%). Zdaniem ekspertów funkcja taka jak komunikacja z dowolnego miejsca oceniona została bardzo wysoko przez 6 ekspertów (85,7%) oraz wysoko przez 1 eksperta (14,3%). Ponadto w opinii ekspertów wykorzystanie hostingu w chmurze ocenione zostało bardzo wysoko przez osoby (42,9%) oraz wysoko przez 4 (57,1%). Na podstawie otrzymanych wyników można zauważyć, że eksperci zgodnie ocenili bardzo wysoko możliwości wykorzystania *Cloud Computing* w zarządzaniu kryzysowym.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.13.

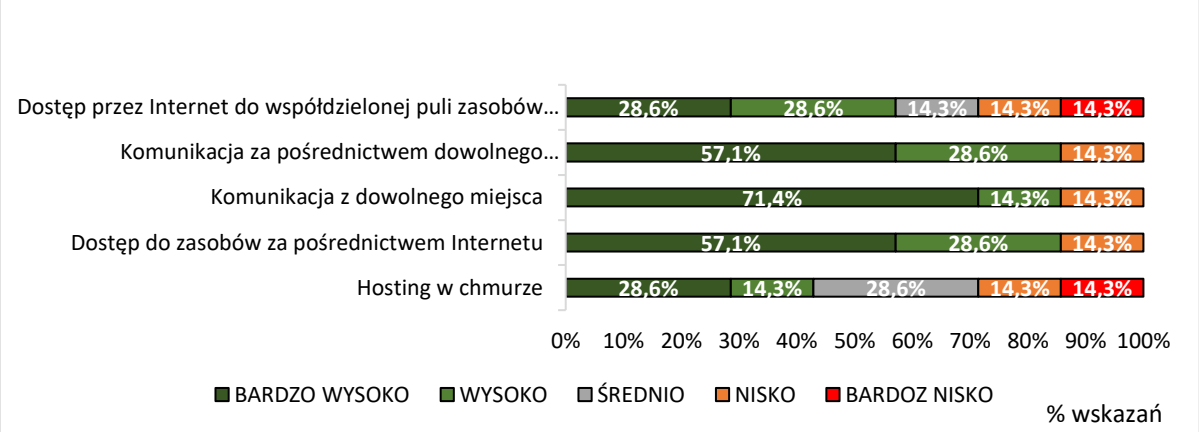
Tabela 7.13. Możliwości wykorzystania CC w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego (N = 7)

Odpowiedzi respondentów
• Wojna w Ukrainie, pandemia Covid pokazały jak istotny dla funkcjonowania państwa jest dostęp do danych, do informacji w sytuacji zniszczenia lub braku dostępu do infrastruktury lokalnej, centrów przetwarzania. Odmiejscowienie danych pozwala zachować ciągłość działania, usprawnia komunikację i wspomaga proces podejmowania decyzji • Chmura obliczeniowa może znacznie zwiększyć efektywność działań w zarządzaniu kryzysowym i być wykorzystywana w celu: • Przechowywania, analizy i udostępniania danych • Wsparcia komunikacji pomiędzy interesariuszami procesu reagowania kryzysowego, umożliwiając współpracę i zapewniając koordynację działań • Optymalizacji sposobu wykorzystania zasobów • Zwiększa swobodę i elastyczność działania, szczególnie w sytuacji zagrożeń • Walory rozwiązania chmurowego nie wymagają uzasadnienia i przy warunku dostępności/ciągłości działania chmury jest to architektura korzystna z punktu widzenia każdej wyróżnionej funkcji z bardzo wysoką oceną przydatności dla zarządzających. • Technologia *Cloud Computing* pozwala na gromadzenie danych i ich przetwarzanie w chmurze obliczeniowej. Nie trzeba martwić się o to, czy są odpowiednio zabezpieczone serwery przed zewnętrznymi atakami. Dostawcy usług chmury obliczeniowej, odpowiadają między innymi za bezpieczeństwo przechowywanych i przetwarzanych danych, a także za to, aby infrastruktura była na bieżąco modernizowana. Zaproponowane w tabeli powyżej możliwości wykorzystania chmury obliczeniowej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego uznaję za poprawne.

Źródło opracowanie własne

W tabeli 7.13 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii *CC* możliwych do wykorzystania przez zespoły zarządzania kryzysowego. Zaproponowane przez ekspertów rozwiązania pokrywają się z tymi przedstawionymi w rozdziale koncepcyjnym.

b. Dla obywateli



Wykres 7.15. Wykorzystanie CC przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Zdania ekspertów na temat możliwości wykorzystania *Cloud Computing* przez obywateli są podzielone. I tak w opinii ekspertów funkcja taka dostęp do internetu do współdzielonej puli zasobów obliczeniowych oceniona została bardzo wysoko przez

2 osoby (28,6%), wysoko przez 2 osoby (28,6%), średnio przez 1 osobę (14,6%), nisko przez 1 osobę (14,3%) oraz bardzo nisko przez 1 osobę (14,3%). Zdaniem ekspertów komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer) oraz dostęp do zasobów za pośrednictwem internetu oceniony został przez 4 osoby (57,1%) bardzo wysoko, 2 osoby (28,6%) oceniły wysoko, a 1 na średnim poziomie (14,3%). Funkcję taką jak komunikacja z dowolnego miejsca 5 ekspertów (71,4%) oceniło na bardzo wysokim poziomie, 1 na wysokim (14,3%) oraz 1 na średnim (14.3%). Ponadto funkcja taka jak hosting w chmurze oceniony został przez ekspertów na bardzo wysokim poziomie przez 2 ekspertów (28,6%), na wysokim przez 1 osobę (14,3%) na średnim przez 2 osoby (28,6%), niskim przez 1 osobę 14,3%) oraz na bardzo niskim przez1 osobę (14,3%).

Pomimo iż większość ekspertów oceniła funkcjonalność *Cloud Computing* bardzo wysoko to w opinii niektórych ekspertów funkcje takie jak hosting w chmurze, komunikacja z dowolnego miejsca, komunikacja za pośrednictwem dowolnego urządzenia mobilnego czy dostęp do zasobów za pośrednictwem internetu oceniona została przez niektórych ekspertów nisko co może wynikać z zależności technologii od dostępu do internetu.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.14.

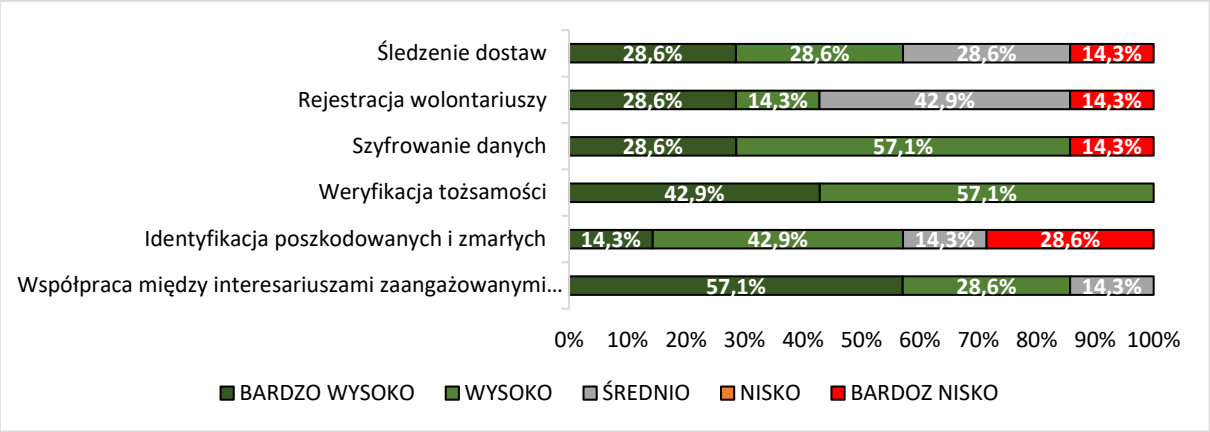
Tabela 7.14. Możliwości wykorzystania CC w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego (N = 7)

Odpowiedzi respondentów
• Wojna w Ukrainie, pandemia Covid pokazały jak istotny dla obywateli jest dostęp do danych, do informacji w sytuacji zniszczenia lub braku dostępu do infrastruktury lokalnej, centrów przetwarzania. Odmiejscowienie danych pozwala zachować bezpiecznie dane prywatne, usprawnia komunikację i wspomaga możliwość codziennego funkcjonowania. • Zaproponowane w tabeli powyżej możliwości wykorzystania chmury obliczeniowej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej obywateli uznaję za wystarczające. • Możliwość komunikowania się z dowolnego miejsca z dowolna osobą (organizacją) , w dowolnym czasie. • Z punktu widzenia działań obywatela w systemie zarządzania kryzysowego, nie wszystkie z wykazanych funkcji mają tą samą ocenę przydatności jak z punktu widzenia zarządzających. Wydaje się, że niektóre z nich jak hosting czy wykorzystanie mocy obliczeniowych są dla obywatela nadmiarowe.

Źródło opracowanie własne

W tabeli 7.14 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii CC możliwych do wykorzystania przez obywateli. Przedstawiona w tabeli opinia ekspertów na temat możliwości wykorzystania *Cloud Computing* pokrywa się z rozwiązaniami zaproponowanymi w rozdziale VI.

9. Jak ocenia Pani/Pan możliwości wykorzystania *Blockchain* w zarządzaniu kryzysowym oraz w aspekcie zapewniania świadomości sytuacyjnej zespołów zarządzania kryzysowego?



Wykres 7.16. Wykorzystanie *Blockchain* przez obywateli (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Zdania ekspertów na temat możliwości wykorzystania *Blockchain* przez zespoły zarządzania kryzysowego. W opinii ekspertów funkcja śledzenia dostaw oceniona została przez 2 osoby (28,6%) na bardzo wysokim poziomie, na wysokim 2 osoby (28,6%), średnim 2 osoby (28,6%) oraz bardzo niskim przez 1 osobę (14,3%). Funkcjonalność taka jak rejestracja wolontariuszy w opinii ekspertów oceniona została bardzo wysoko przez 2 osoby (28,6%), wysoko przez 1 osobę (14,3%), średnio przez 3 osoby (42,9%) oraz bardzo nisko przez 1 osobę 14,3%).Szyfrowanie danych ocenione zostało bardzo wysoko przez 2 osoby (28,6%), wysoko przez 4 osoby (57,1%) oraz nisko przez 1 osobę (14,3%). Najwyżej oceniona została weryfikacja tożsamości, która w opinii ekspertów oceniona została bardzo wysoko przez 3 osoby (42,9%) oraz wysoko przez 4 (57,1%). Funkcjonalność taka jak identyfikacja poszkodowanych i zmarłych w opinii ekspertów oceniona została bardzo wysoko przez 1 osobę (14,3%), wysoko przez 3 osoby (42,9%), średnio przez 1 osobę (14,3%) oraz bardzo nisko przez 2 osoby (28,6%). Ponadto ocenie poddano możliwość współpracy miedzy interesariuszami zaangażowanymi w proces reagowania na katastrofy i tak w opinii ekspertów 4 osoby (57,1%) oceniły tego typu rozwiązanie bardzo wysoko, 2 osoby wysoko (28,6%) oraz 1 średnio (14,3%).

Pomimo iż większość ekspertów oceniła funkcjonalność *Blockchain* bardzo wysoko to w opinii niektórych ekspertów funkcje takie jak śledzenie dostaw, rejestracja wolontariuszy, szyfrowanie danych oraz identyfikacja poszkodowanych i zmarłych

w opinii niektórych ekspertów została oceniona bardzo nisko co może wynikać z faktu, że zaproponowane rozwiązanie stanowi nowatorskie podejście do zarządzania kryzysowego oraz sposobu zabezpieczenia i wykorzystania danych.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.15.

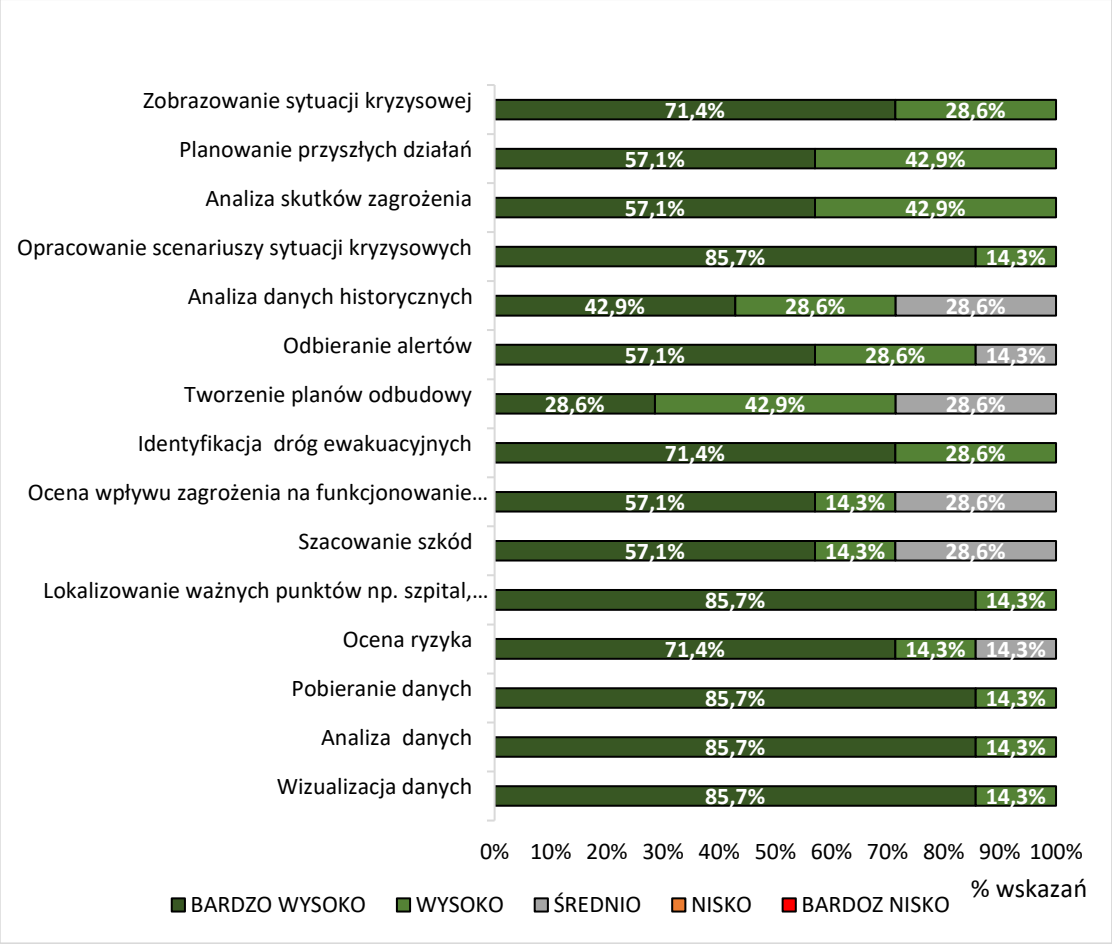
Tabela 7.15. Możliwości wykorzystania Blockchain w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego

Odpowiedzi respondentów
• Technologia *Blockchain* daje duże możliwości, jednak tak jak przy poprzednich technologiach można stwierdzić że świadomość rośnie ale możliwości operacyjnego wykorzystania ciągle w mojej ocenie są w warstwie czysto teoretycznej. • *Blockchain* to technologia, która umożliwia bezpieczne przechowywanie i udostępnianie danych, a także śledzenie ich historii i kontroli nad nimi. W związku z tym, *Blockchain* może być wykorzystany w różnych obszarach zarządzania kryzysowego tj.: • Zarządzanie dostawami: W przypadku kryzysu, takiego jak pandemia, *Blockchain* może być wykorzystany do zarządzania dostawami medycznymi. Dzięki *Blockchain*, można by śledzić historię każdej dostawy, od producenta do pacjenta, zapewniając przez to pełną kontrolę nad całym łańcuchem dostaw. • Zarządzanie funduszami: *Blockchain* może być również wykorzystany do zarządzania funduszami w czasie kryzysu. Dzięki *Blockchain*, można by łatwo śledzić przepływ pieniędzy, co pozwala na skuteczniejsze zarządzanie finansami i eliminację oszustw. • Weryfikacja informacji: W czasie kryzysu, ważne jest, aby mieć dostęp do rzetelnych i wiarygodnych informacji. Dzięki *Blockchain*, można by weryfikować źródło informacji i kontrolować jej autentyczność, co pozwala na szybsze i bardziej efektywne podejmowanie decyzji. • Zarządzanie danymi medycznymi: W przypadku kryzysów zdrowotnych, takich jak pandemia, *Blockchain* może być wykorzystany do przechowywania danych medycznych pacjentów. Dzięki temu, można by szybko i bezpiecznie udostępniać informacje o stanie zdrowia pacjenta różnym służbom i władzom odpowiedzialnym za zarządzanie kryzysowe. • Współpraca i koordynacja: *Blockchain* może być również wykorzystany do usprawnienia współpracy między różnymi służbami ratowniczymi i władzami odpowiedzialnymi za zarządzanie kryzysowe. Dzięki *Blockchain*, można by łatwo udostępniać informacje między różnymi służbami, co pozwala na szybsze i bardziej skuteczne reagowanie na kryzys. • *Blockchain* to tzw. łańcuch bloków, który zdolny jest do przechowywania oraz przesyłania w sposób rozproszony różnorodnych informacji. Informacje te zestawiane są w blokach danych będących częściami składowymi całego łańcucha. System taki może tworzyć całkowicie zdecentralizowany rejestr lub bazę danych. Technologia *Blockchain* wykorzystywana jest też do ochrony zasobów informacyjnych z wykorzystaniem metod szyfrowania danych w taki sposób, aby niezbędne informacje i dane nie dostały się w niepowołane ręce. • Zaproponowane w powyższej tabeli możliwości wykorzystania technologii *Blockchain* w zarządzaniu kryzysowym oraz w aspekcie zapewniania świadomości sytuacyjnej zespołów zarządzania kryzysowego uznaję za zasadne. Należy jednak zaznaczyć, że wszystkie powyższe rozwiązania są dość skomplikowane i mogą okazać się bardzo trudne do wprowadzenia w życie. • Zastosowanie technologii *Blockchain* w kontekście systemu zarządzania kryzysowego może wzmocnić procesy weryfikacji, przechowywania i udostępniania danych cyfrowych, szczególnie w kontekście budowania korporacyjnych mechanizmów wymiany danych pomiędzy różnymi instytucjami systemu zarządzania kryzysowego.

Źródło opracowanie własne

W tabeli 7.15 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii *Blockchain* możliwych do wykorzystania przez zespoły zarządzania kryzysowego. Zaproponowane przez ekspertów kierunki rozwoju technologii oraz sposoby jej udoskonalenia pokrywają się funkcjonalnością opisaną w rozdziale VI.

10. Jak ocenia Pani/Pan możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego oraz obywateli?
    a. dla zespołów zarządzania kryzysowego



Wykres 7.17. Możliwości wykorzystania Systemów Informacji Geoprzestrzennej (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

W opinii ekspertów funkcje takie zobrazowanie sytuacji kryzysowych oraz ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli ocenione zostało bardzo wysoko przez 5 osób (71,4%) oraz wysoko przez 2 osoby (28,6%). Funkcje takie jak planowanie przyszłych działań oraz analiza skutków zagrożeń oceniona została bardzo wysoko przez 4 ekspertów (57,1%) oraz wysoko przez 3 ekspertów (42,9%).

Rozwiązania takie jak opracowanie scenariuszy sytuacji kryzysowych, lokalizowanie ważnych punktów np. szpital, komisariat policji itp. za pomocą zapytań *SQL*, pobieranie danych, analiza danych oraz wizualizacja danych w opinii ekspertów zostało ocenione bardzo wysoko 6 osób oraz nisko przez 1 osobę (14,3%).

Tworzenie planów odbudowy ocenione zostało bardzo wysoko przez 2 osoby (28,6%), wysoko przez 3 osoby (42,9%) oraz średnio przez 2 osoby (28,6%). Ponadto funkcje takie jak ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli oraz szacowanie szkód w opinii ekspertów zostało ocenione bardzo wysoko przez 4 osoby (57,1%), wysoko przez 1 osobę (14,3%) oraz średnio przez 2 osoby (28,6%). Zdaniem ekspertów ocena ryzyka została oceniona na bardzo wysokim poziomie przez 5 osób (71,4%), na wysokim przez 1 osobę (14,3%) oraz na średnim przez 1 osobę (14,3%).

Tabela 7.16. Możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego oraz obywateli (N = 7)

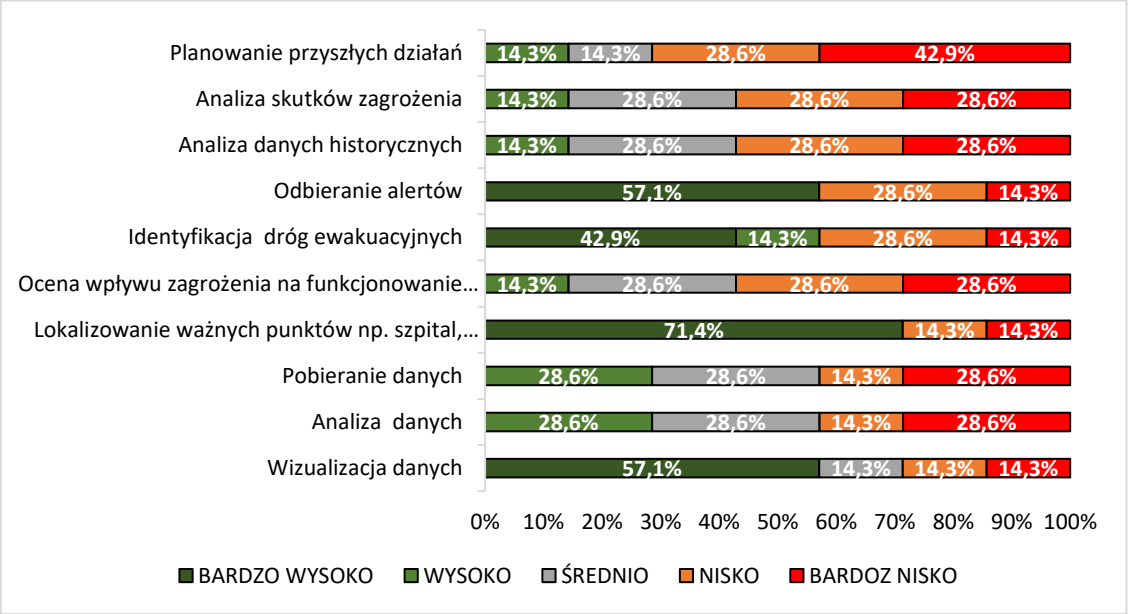
Odpowiedzi respondentów
• Systemy informacji geoprzestrzennej (GIS) są wykorzystywane w zarządzaniu kryzysowym do gromadzenia, przetwarzania i prezentacji danych geoprzestrzennych, które są niezbędne w procesie podejmowania decyzji w czasie rzeczywistym. Służą temu: o Analiza i przetwarzanie danych przestrzennych pozwalająca na zrozumienie charakterystyk terenu. Dzięki GIS, można zbadać informacje dotyczące warunków pogodowych, topografii, infrastruktury drogowej, itp. o Wspomaganie decyzji przy planowaniu tras i dostępności do rejonu np. katastrofy naturalnej czy wypadku drogowego. • Możliwość wykorzystania systemów GIS oceniam bardzo wysoko. Żaden opis nie zastąpi zobrazowania graficznego. Rozwiązania zobrazowania na mapach są dziś już tak powszechne, że wykorzystanie możliwości jakie daje ta powszechność są wręcz koniecznością. • System informacji geoprzestrzennej to bardzo dobra technologia, ale trzeba ją odpowiednio i doskonalić w miarę potrzeb i doświadczenia. • W systemach zarządzania kryzysowego do wspólnego obrazu sytuacji kryzysowej należy dostosować kategorie danych. • Systemy informacji geograficznej obejmują wszystkie zagadnienia związane z tworzeniem, gromadzeniem, przetwarzaniem i korzystaniem z informacji geograficznej Nazwa ta w Polsce często jest stosowana zamiennie z terminem „system informacji przestrzennej" (SIP), jednak warto znać różnicę pomiędzy tymi dwoma pojęciami. Słowo „geograficzny" odnosi się do obiektów zlokalizowanych w przestrzeni, zaś „przestrzenny" obejmuje zarówno obiekty znajdujące się w przestrzeni, jak również zjawiska i procesy w niej zachodzące. Podzielam pogląd doktoranta, iż systemy informacji geograficznej (GIS) mogą odgrywać istotną rolę na wszystkich szczeblach zarządzania kryzysowego, w procesie zwalczania klęsk żywiołowych oraz planowania działań zmierzających do likwidowania skutków zagrożeń. Zaproponowane w tabeli powyżej możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego uznaję zasadne • Zaproponowane w tabeli powyżej możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej obywateli uznaję ważne chociaż mogą być rzadziej wykorzystywane

Źródło opracowanie własne

Możliwości wykorzystania Systemów Informacji Geoprzestrzennej przez zespoły zarządzania kryzysowego ocenione zostały przez ekspertów bardzo wysoko, co pokazuje jak duży wpływ na zarządzanie kryzysowe ma analiza danych ich wizualizacja, a także planowane przyszłych działań na podstawie danych zbieranych w czasie rzeczywistym oraz danych historycznych odpowiednio zobrazowanych.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.16, w której przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii Systemów Informacji Geoprzestrzennej możliwych do wykorzystania przez zespoły zarządzania kryzysowego. Zaproponowane przez ekspertów kierunki rozwoju technologii Systemów Informacji Geoprzestrzennej oraz sposoby jej udoskonalenia pokrywają się funkcjonalnością opisaną w rozdziale VI.

b. Dla obywateli



Wykres 7.18. Możliwości wykorzystania Systemów Informacji Geoprzestrzennej (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

Możliwości wykorzystania Systemów Informacji Geoprzestrzennej przez obywateli w opinii ekspertów są podzielone. Zdaniem ekspertów planowanie przyszłych działań 1 osoba (14,3%), oceniła wskazaną funkcjonalność na wysokim poziome, 1 osoba na średnim poziomie, 2 osoby (28,6%) na niskim oraz 3 osoby (42,9%) na bardzo niskim. Analiza skutków zagrożeń, analiza danych historycznych oraz ocena wpływu

zagrożenia na funkcjonowanie państwa i obywateli w opinii ekspertów oceniona została wysoko przez 1 osobę (14,3%), średnio przez 2 osoby (28,6%), nisko przez 2 osoby (28,6%) oraz bardzo nisko przez 2 osoby (28,6%). Funkcjonalność taka jak odbieranie alertów oceniona została bardzo wysoko przez 4 ekspertów (57,1%), nisko przez 2 osoby (28,6%) oraz bardzo nisko przez 1 osobę (14,3%). W opinii ekspertów identyfikacja dróg ewakuacyjnych oceniona została bardzo wysoko przez 3 osoby (42,9%), wysoko przez 1 osobę (14,3%), nisko przez 2 osoby (28,6%) oraz bardzo nisko przez 1 osobę (14,3%).Najwyżej oceniona przez ekspertów została taka funkcja jak lokalizowanie ważnych punktów strategicznych np. szpital, komisariat policji itp. za pomocą zapytań *SQL*. I tak w opinii ekspertów 5 (71,4%), oceniło zaproponowane rozwiązanie bardzo wysoko, 1 nisko (14,3%) oraz 1 (14,3%) bardzo nisko. Ponadto funkcje takie jak pobieranie danych oraz analiza danych oceniona została wysoko przez 2 osoby (28,6%), średnio przez 2 osoby (28,6%), nisko przez 1 osobę (14,3%) oraz bardzo nisko przez 2 osoby (28,6%).Ocenie została poddana również funkcja wizualizacji danych, którą 4 ekspertów (57,1%) oceniło bardzo wysoko, 1 (14,3%) ekspert średnio, 1 (14,3%) nisko oraz 1 (14,3%) bardzo nisko. Pomimo podzielonych wśród ekspertów zdań na temat możliwości wykorzystania zaproponowanych rozwiązań można dostrzec w nich ogromny potencjał w kreowaniu świadomości sytuacyjnej obywateli na temat zagrożeń.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.17.

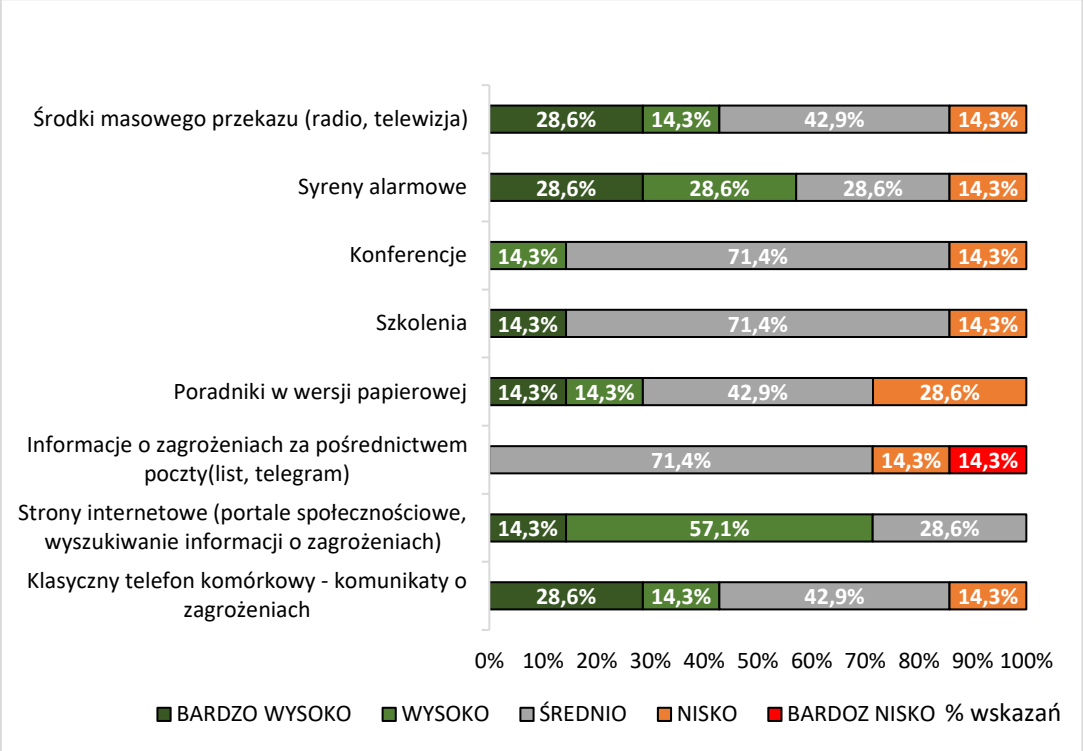
Tabela 7.17. Możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego (N = 7)

Odpowiedzi respondentów
• Możliwość wykorzystania systemów GIS dla obywateli oceniam bardzo wysoko. Żaden opis nie zastąpi zobrazowania graficznego. Rozwiązania zobrazowania na mapach są dziś już tak powszechne, że wykorzystanie możliwości jakie daje ta powszechność są wręcz koniecznością. Praktycznie 70-80% osób wykorzystuje codzienne rozwiązania od Google, mapy obszarowe np.: https://mapa.um.warszawa.pl co daje nie ograniczone możliwości ich wykorzystania. • Zaproponowane w tabeli powyżej możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej obywateli uznaję ważne chociaż mogą być rzadziej wykorzystywane • Z punktu widzenia obywatela, zastosowanie systemu klasy GIS postrzegać należy raczej jako element dostarczający określonych informacji czy prostych funkcji do wykorzystania przez obywatela a które to są organizowanie i zapewniane przez zarządzających. Stąd, w tym rozumieniu, większość funkcji choć wysoce przydatne z punktu widzenia zarządzających są z punktu widzenia obywatela nadmiarowe.

Źródło opracowanie własne

W tabeli 7.17 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii obywateli. Zaproponowane przez ekspertów kierunki rozwoju technologii Systemów Informacji Geoprzestrzennej oraz sposoby jej udoskonalenia pokrywają się funkcjonalnością opisaną w rozdziale VI.

- Jak ocenia Pani/Pan możliwości wykorzystania tradycyjnych technologii i współczesnych technologii IT/ICT w procesie kształtowania świadomości sytuacyjnej na temat zagrożeń?
- Tradycyjne technologie
    a. Dla zespołów zarządzania kryzysowego



Wykres 7.19. Możliwości wykorzystania tradycyjnych technologii przez zespoły zarządzania kryzysowego (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

W opinii ekspertów zdanie na temat możliwości wykorzystania tradycyjnych technologii jest podzielone. Wykorzystania takich rozwiązań jak środki masowego przekazu (radio, telewizja) oraz klasyczny telefon komórkowy – komunikaty o zagrożeniach ocenione zostały przez 2 ekspertów (28,6%) bardzo wysoko, 1 ekspert (14,3%) ocenił wysoko, 3 ekspertów (42,9%) oceniło średni oraz 1 (14,3%) nisko. Technologia taka jak syreny alarmowe ocenione zostały bardzo wysoko w opinii 2 ekspertów (28,6%), wysoko przez 2 (28,6%) ekspertów, średnio przez 2 ekspertów (28,6%) oraz nisko przez 1 eksperta (14,3%). Rozwiązanie takie jak konferencje w opinii eks-

pertów 1 osoba (14,3%) oceniła wysoko, 5 osób (71,4%) średnio oraz 1 nisko (14,3%). Podobnie ocenione zostały przez ekspertów szkolenia i tak 1 (14,3%) osoba oceniła zaproponowane rozwiązanie bardzo wysoko, 5 osób (71,4%) średnio oraz 1 osoba (14,3%) nisko. Wykorzystanie technologii takiej jak poradniki w wersji papierowej 1 osoba (14,3%) oceniła bardzo wysoko, 1 osoba (14,3%) wysoko, 3 osoby (42,9%) średnio oraz 2 osoby (28,6%) nisko. Ekspertów poproszono również o ocenę takiego rozwiązania jak informacje o zagrożeniach za pośrednictwem poczty (list, telegram) i tak w opinii ekspertów 5 osób (71,4%) oceniło zaproponowane rozwiązanie na średnim poziomie, 1 osoba (14,3%) na niskim oraz 1 (14,3%) na bardzo niskim. Eksperci ocenili również rozwiązanie takie jak strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach) i tak w opinii ekspertów 1 osoba (14,3%) oceniła potencjał zaproponowanej technologii bardzo wysoko, 4 osoby (57,1%) wysoko oraz 2 osoby (28,6%) średnio.

Na podstawie analizy odpowiedzi ekspertów można zauważyć, że technologie takie jak np. klasyczny telefon komórkowy, środki masowego przekazu oraz poradniki w wersji papierowej mogą okazać się przydatne dla zespołów zarządzania kryzysowego inne natomiast takie jak informacje za pośrednictwem poczty ocenione zostały bardzo nisko co wskazuje na ich nieprzydatność.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.18.

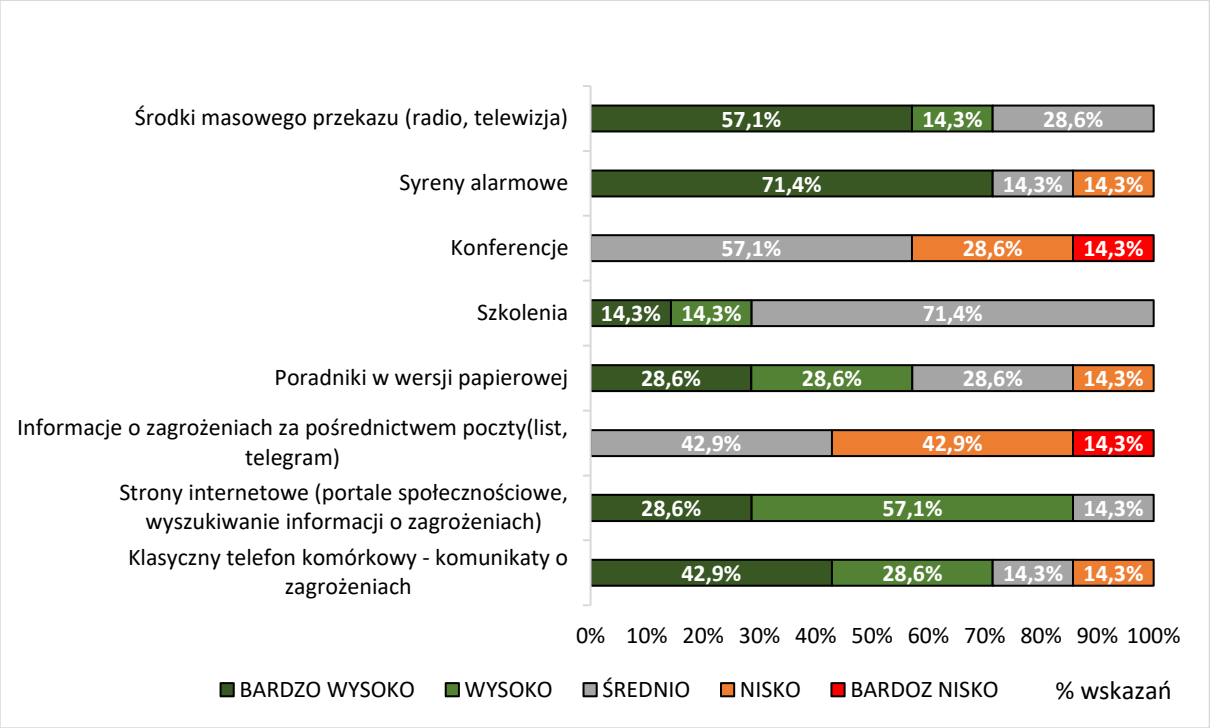
Tabela 7.18. Możliwości wykorzystania tradycyjnych technologii (N = 7)

Odpowiedzi respondentów
• Oceniam, że tradycyjne technologie długo jeszcze pozostaną najważniejszym obszarem wsparcia funkcjonowania zespołów zarządzania kryzysowego jak i obywateli w sytuacjach zagrożenia lub kryzysu. Ponownie podkreślam, ze istotne są dwa aspekty powszechność i dostępność. Jednak wykluczenie cyfrowe nie jest w Polsce tylko pojęciem, jest faktem. • Podzielam opinię Doktoranta, iż tradycyjne technologie mają wiele ograniczeń, to jednak mogą stanowić nadal przydatną możliwość wykorzystywaną przez część obywateli. Możliwości wykorzystania tradycyjnych technologii przedstawionych w tabelach powyżej w procesie kształtowania świadomości sytuacyjnej na temat • zagrożeń oceniam wyżej dla obywateli niż zespołów zarządzania kryzysowego. • Tradycyjne technologie IT nie znikną całkowicie. Będą raczej jeszcze bardzo długo współegzystować z tzw. technologiami nowoczesnymi. • Proces kształtowania świadomości sytuacyjnej na temat zagrożeń nie powinien odrzucać tradycyjnych technologii a umiejętnością zarządzających powinno być właściwe ich wykorzystanie. Uwzględnić należy oczywiście istniejące bariery i ograniczenia które z natury rzeczy powodują że niektóre z zaproponowanych rozwiązań uznać należy za mało (telefon komórkowy) czy wręcz nieprzydatne (tradycyjna korespondencja). Z punktu widzenia budowania w społeczeństwie powszechnej wiedzy, większość z proponowanych form jej kształtowania ocenić należy pozytywnie, nie mniej formuła konferencji raczej jest dedykowana zarządzającym niż obywatelom.

Źródło opracowanie własne

W tabeli 7.18 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii obywateli. Zaproponowane przez ekspertów kierunki rozwoju technologii oraz sposoby jej udoskonalenia pokrywają się funkcjonalnością opisaną w rozdziale VI.

b. Dla obywateli



Wykres 7.20. Możliwości wykorzystania tradycyjnych technologii przez zespoły zarządzania kryzysowego (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

W opinii ekspertów zdanie na temat możliwości wykorzystania tradycyjnych technologii przez obywateli jest podzielone. I tak rozwiązanie takie jak środki masowego przekazu (radio, telewizja) ocenione zostało bardzo wysoko przez 4 ekspertów (57,1%), wysoko przez1 osobę (14,3%) oraz średnio przez 2 osoby (28,6%). Spośród 7 ekspertów 5 (71,4%) uznało, że syreny alarmowe odgrywają kluczową rolę w procesie informowania obywateli o zagrożeniach, 1 ekspert (14,3%) ocenił tego typu rozwiązanie na średnim poziomie oraz 1 (14,3%) na niskim. Możliwość edukowania społeczeństwa poprzez konferencje 4 ekspertów (57,1%) oceniło na średnim poziomie, 2 (28,6%) na niskim oraz 1 (14,3%) na bardzo niskim. Szkolenia w opinii ekspertów ocenione zostały bardzo wysoko przez 1 osobę (14,3%), wysoko przez 1 osobę (14,3%) oraz średnio przez 5 osób (71,4%). Zaproponowane rozwiązanie takie jak poradniki w wersji papierowej 2 ekspertów (28,6%) oceniło bardzo wysoko 2

(28,6%) wysoko, 2 średnio (28,6%), a tylko 1 osoba (14,6%) nisko. Rozwiązanie takie jak informacje o zagrożeniach za pośrednictwem poczty (list, telegram) ocenione zostało najniżej. I tak 3 ekspertów (42,9%) oceniło tego typu rozwiązanie średnio, 3 (42,9%) nisko oraz 1 osoba (14,3%) bardzo nisko. Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach) w opinii ekspertów zostały ocenione bardzo wysoko przez 2 osoby (28,6%), wysoko przez 4 osoby (57,1%) oraz nisko przez 1 osobę (14,3%). Ponadto eksperci ocenili możliwości zastosowania takiego rozwiązania jak klasyczny telefon – komunikaty o zagrożeniach. I tak w opinii ekspertów 3 osoby (42,9%) oceniły tego typ rozwiązanie bardzo wysoko, 2 osoby (28,6%) wysoko, 1 osoba (14,3%) osoba średnio oraz 1 osoba (14,3%) nisko.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.19.

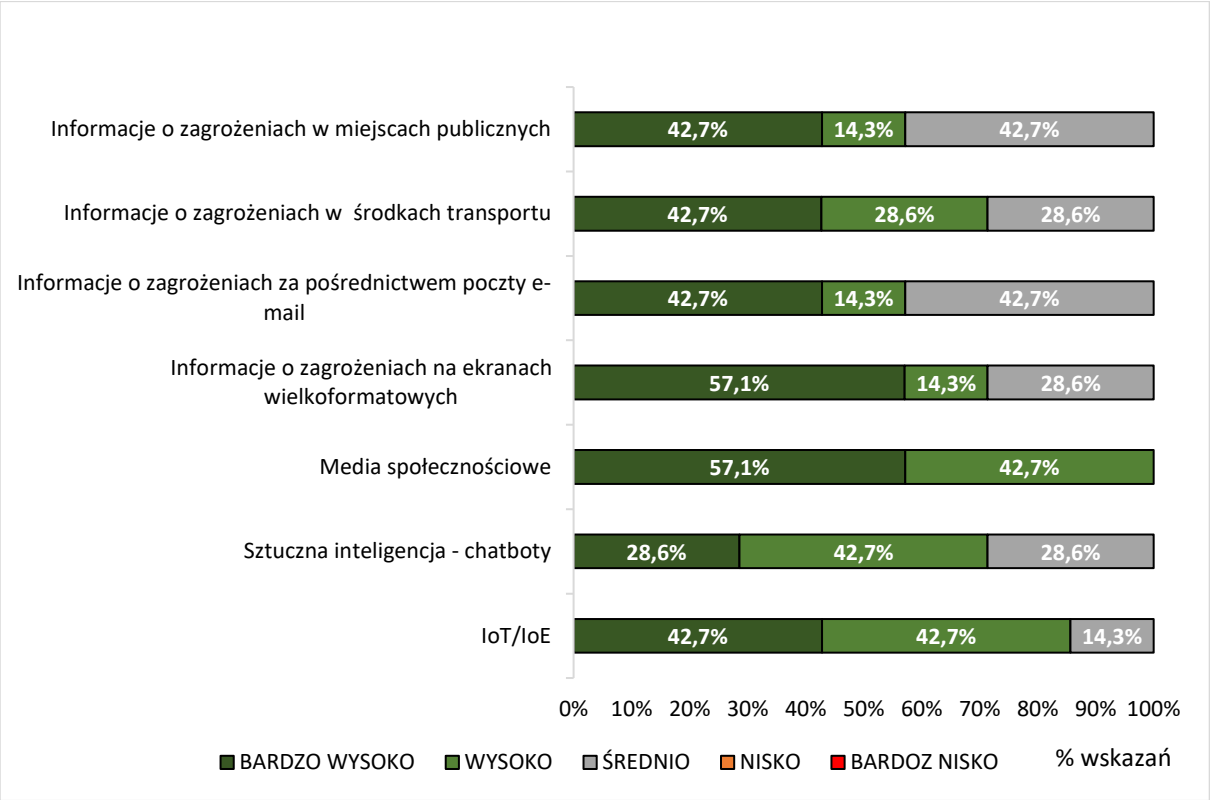
Tabela 7.19. Możliwości wykorzystania tradycyjnych technologii (N = 7)

Odpowiedzi respondentów
• Oceniam, że tradycyjne technologie długo jeszcze pozostaną najważniejszym obszarem wsparcia funkcjonowania zespołów zarządzania kryzysowego jak i obywateli w sytuacjach zagrożenia lub kryzysu. Ponownie podkreślam, ze istotne są dwa aspekty powszechność i dostępność. Jednak wykluczenie cyfrowe nie jest w Polsce tylko pojęciem, jest faktem.
• Podzielam opinię Doktoranta, iż tradycyjne technologie mają wiele ograniczeń, to jednak mogą stanowić nadal przydatną możliwość wykorzystywaną przez część obywateli. Możliwości wykorzystania tradycyjnych technologii przedstawionych w tabelach powyżej w procesie kształtowania świadomości sytuacyjnej na temat
• zagrożeń oceniam wyżej dla obywateli niż zespołów zarządzania kryzysowego.
• Tradycyjne technologie IT nie znikną całkowicie. Będą raczej jeszcze bardzo długo współegzystować z tzw. technologiami nowoczesnymi.
• Proces kształtowania świadomości sytuacyjnej na temat zagrożeń nie powinien odrzucać tradycyjnych technologii, a umiejętnością zarządzających powinno być właściwe ich wykorzystanie. Uwzględnić należy oczywiście istniejące bariery i ograniczenia które z natury rzeczy powodują że niektóre z zaproponowanych rozwiązań uznać należy za mało (telefon komórkowy) czy wręcz nieprzydatne (tradycyjna korespondencja). Z punktu widzenia budowania w społeczeństwie powszechnej wiedzy, większość z proponowanych form jej kształtowania ocenić należy pozytywnie, nie mniej formuła konferencji raczej jest dedykowana zarządzającym niż obywatelom.

Źródło opracowanie własne

W tabeli 7.19 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii obywateli Zaproponowane przez ekspertów kierunki rozwoju technologii oraz sposoby jej udoskonalenia pokrywają się funkcjonalnością opisaną w rozdziale VI.

- Współczesne technologie
    a. Zespoły zarządzania kryzysowego



Wykres 7.21. Możliwości wykorzystania współczesnych technologii przez zespoły zarządzania kryzysowego (odpowiedzi ekspertów) (N = 7)

Źródło opracowanie własne

W opinii ekspertów możliwości wykorzystania współczesnych technologii ocenione zostały bardzo wysoko co pokazuje jak ogromny potencjał mają one w zarządzaniu kryzysowym. Rozwiązania takie jak informacja o zagrożeniach w miejscach publicznych oraz informacje o zagrożeniach za pośrednictwem poczty e-mail w opinii ekspertów ocenione zostały bardzo wysoko przez 3 (42,7%) osoby, wysoko przez 1 (14,3%) osobę oraz średnio przez 3 (42,7%) osoby. Informacje o zagrożeniach w środkach transportu ocenione zostało przez 3 (42,7%) osoby bardzo wysoko, 2 (28,6%) osoby wysoko oraz 2 (28,6%) osoby średnio. Ponadto rozwiązanie takie jak informacje o zagrożeniach na ekranach wielkoformatowych ocenione zostało przez 4 (57,1%) osoby bardzo wysoko, 1 (14,3%) osoba oceniła wysoko oraz 2 osoby oceniły na średnim poziomie. Spośród zaproponowanych rozwiązań najwyżej ocenione został media społecznościowe i tak 4 (57,1%) osób oceniło tego typu rozwiązanie na bardzo wysokim poziomie, a 3 (42,7%) na wysokim. Eksperci ocenili również możliwości wykorzystania sztucznej inteligencji, a konkretnie chatbotów, które ocenione zostały bardzo wysoko przez 2 (28,6%) osoby, wysoko przez 3 (42,7%) osoby oraz średnio przez 2 (28,6%) osoby. Ponadto ocenie poddano możliwości wykorzystania

IoT i tak w opinii ekspertów 3 (42,7%) osoby oceniły tego typu rozwiązanie bardzo wysoko, 3 (42,7%) wysoko oraz 1 (14,3%) na średnim poziomie.

Przedstawione na wykresie wyniki wskazują jak istotne jest wdrożenie zaproponowanej technologii do zarządzania kryzysowego. Uszczegółowione dane zebrane od ekspertów przedstawiono za pomocą tabeli 7.20.

Tabela 7.20. Możliwości wykorzystania współczesnych technologii (N = 7)

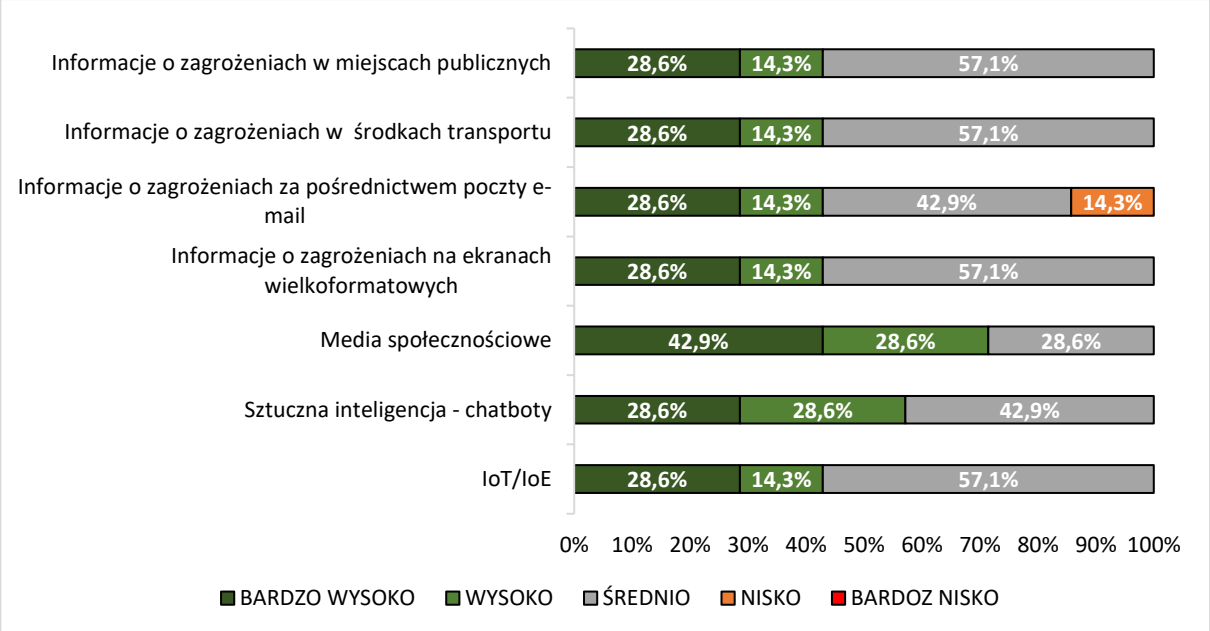
Odpowiedzi respondentów
• Oczywiście współczesne technologie IT/ICT są przyszłością wsparcia procesów zarządzania kryzysowego, jednak ich implementacja wymaga podniesienia świadomości technologicznej zespołów zarządzania kryzysowego, określonych sporych nakładów finansowych. • Możliwości wykorzystania współczesnych technologie IT/ICT przedstawionych w tabelach powyżej w procesie kształtowania świadomości sytuacyjnej na temat zagrożeń oceniam wyżej dla zespołów zarządzania kryzysowego niż dla obywateli. • Brak znajomości przypadków użycia takich technologii utrudnia ocenę. • Efektywność i skuteczność wykorzystania technologii IT/ICT w procesach zarządzania kryzysowego jest z punktu widzenia zarządzających jak i obywateli pożądanym kierunkiem obwarowanym jednak warunkiem dojrzałości cyfrowej państwa. Wszystkie z wymienionych propozycji są akceptowalne, nie mniej rozpatrując je w kontekście potencjalnych zasięgów niektóre z nich ocenić należy jako przydatne tylko w obrębie dużych aglomeracji.

Źródło opracowanie własne

W tabeli 7.20 przedstawiono opinię ekspertów na temat zaproponowanych funkcji technologii obywateli.

b. Obywatele

Wykres 7.22. Możliwości wykorzystania współczesnych technologii przez obywateli (odpowiedzi eksperów) (N = 7)



Źródło opracowanie własne

W opinii ekspertów zdanie na temat możliwości wykorzystania współczesnych technologii jest podzielone. I tak technologie takie jak informacje o zagrożeniach w miejscach, informacje o zagrożeniach w środkach transportu, informacje o zagrożeniach a ekranach wielkoformatowych oraz IoT ocenione zostały przez 2 (28,6%) ekspertów na bardzo wysokim poziomie, na wysokim poziomie przez 1 (14,3%) eksperta oraz na średnim przez 4 ekspertów. Podobnie ocenione zostało ocenione informowanie o zagrożeniach za pośrednictwem poczty -mail i tak 2 (28,6%) ekspertów oceniło tego typu rozwiązanie bardzo wysoko,1 (14,3%) osoba wysoko, 3 (42,6%) ekspertów średnio oraz 1 nisko (14,3%). Eksperci ocenili również możliwości wykorzystania mediówc. społecznościowych o tak 3 (42,9%) osoby oceniły tego typu rozwiązanie bardzo wysoko, 2 osoby (28,6%) oraz 2 (28,6%) osoby średnio. Ekspertów poproszono również o możliwości wykorzystania technologii sztucznej inteligencji chatbótów, które ocenione zostały bardzo wysoko przez 2 (28,6%) ekspertów, wysoko przez 1 (14,3%) eksperta oraz średnio przez 4 (57,1%)

Na podstawie przeprowadzonych badań można zauważyć że niektórzy eksperci upatrują potencjał we współczesnych technologiach oceniając je bardzo wysoko i jako przydatne dla obywateli, inni natomiast ocenili zaprezentowane technologie na średnim poziomie bądź niskim co wskazuje na to, że wśród ekspertów są osoby preferujące tradycyjne rozwiązanie lub są to osoby, które nie dostrzegają potencjału wskazanych rozwiązań.

Tabela 7.21. Możliwości wykorzystania współczesnych technologii (N = 7)

Odpowiedzi respondentów
• Oczywiście współczesne technologie IT/ICT są przyszłością wsparcia procesów zarządzania kryzysowego, jednak ich implementacja wymaga podniesienia świadomości technologicznej zespołów zarządzania kryzysowego, określonych sporych nakładów finansowych. • Możliwości wykorzystania współczesnych technologie IT/ICT przedstawionych w tabelach powyżej w procesie kształtowania świadomości sytuacyjnej na temat zagrożeń oceniam wyżej dla zespołów zarządzania kryzysowego niż dla obywateli. • Brak znajomości przypadków użycia takich technologii utrudnia ocenę. • Efektywność i skuteczność wykorzystania technologii IT/ICT w procesach zarządzania kryzysowego jest z punktu widzenia zarządzających jak i obywateli pożądanym kierunkiem obwarowanym jednak warunkiem dojrzałości cyfrowej państwa. Wszystkie z wymienionych propozycji są akceptowalne, nie mniej rozpatrując je w kontekście potencjalnych zasięgów niektóre z nich ocenić należy jako przydatne tylko w obrębie dużych aglomeracji.

Źródło opracowanie własne

W tabeli 7.21 przedstawiono opinię ekspertów na temat możliwości wykorzystania współczesnych technologii przez obywateli.

7.3. Wnioski końcowe z wywiadu eksperckiego

Na podstawie otrzymanych wyników można stwierdzić, że wskazane w rozdziale VI technologie stanowią przyszłość zarządzania kryzysowego, a ich wdrożenie w opinii ekspertów może istotnie przyczynić się do usprawnienia działań przed po i w trakcie kryzysu, a także zwiększyć świadomość sytuacyjną obywateli, członków zespołów zarządzania oraz służb ratowniczych. Eksperci bardzo wysoko ocenili możliwości wykorzystania tradycyjnych oraz współczesnych technologii IT/ICT (ZSIZ/BI/*OLTP*/OLAP/DM, IoT, *Big Data*/DM/AI, *VR/AR*, *CC*, *Blockchain*) potwierdzając słuszność rozwiązań zaproponowanych w rozdziale VI, a także wskazując możliwe kierunki rozwoju ich doskonalenia, co stanowiło uzupełnienie wywiadu eksperckiego. Pomimo wysokiej oceny zaproponowanych rozwiązań wśród ekspertów są osoby, które niektóre z funkcji współczesnych technologii IT/ICT oceniły na średnim bądź niskim poziomie. Tego typu ocena nie wynika z faktu, że zaproponowana funkcjonalność jest zbędna lecz innowacyjności przedstawionych rozwiązań, które do tej pory nie były wykorzystywane w zarządzaniu kryzysowym i stanowią w pewnym sensie wyzwanie w skutecznym wdrożeniu i wykorzystywaniu technologii, co wymaga przygotowania odpowiedniej infrastruktury oraz przeszkolenia osób wykorzystujących tego typu rozwiązania. Podobnie jak w przypadku współczesnych technologii również tradycyjne rozwiązania w opinii niektórych ekspertów ocenione zostały na średnim bądź niskim poziomie, co pokazuje, że skuteczne zarządzanie kryzysowe nie może zostać ograniczone do jednej technologii i musi być dostosowane do potrzeb różnych grup społecznych, aby możliwe było nie tylko dotarcie do jak największego grona odbiorców, ale również skorzystanie z alternatywnych rozwiązań na wypadek zawodności którejś z technologii.

Zaproponowane ekspertom rozwiązania w rozprawie stanowią w pewnym sensie odpowiedź na oczekiwania obywateli oraz członków zespołów zarządzania kryzysowego na wskazane w ankiecie potrzeby doskonalenia obecnego SZK tak, aby możliwe było dostosowanie ich do aktualnych potrzeb i trendów wyznaczonych przez współczesne i tradycyjne technologie.

Wyniki zebrane od ekspertów potwierdzają przydatność zaproponowanych rozwiązań, co podkreśla słuszność zaproponowanej koncepcji jak i całej rozprawy.

7.4. Podsumowanie rozdziału siódmego

Zaproponowana koncepcja doskonalenia systemu kreowania świadomości sytuacyjnej ludności przedstawiona w rozdziale VI została poddana ekspertyzie wskazanych w rozdziale VII podmiotów i miała na celu ocenę możliwości wykorzystania współczesnych oraz tradycyjnych rozwiązań możliwych do wykorzystania w SZK oraz w procesie informowania ludności o zagrożeniach w taki sposób, aby możliwe było dotarcie do jak największej grupy odbiorców. Opinia ekspertów potwierdziła przydatność zaproponowanych w koncepcji rozwiązań oraz potwierdziła możliwość implementacji zaproponowanej koncepcji. Jako największe zagrożenia w implementacji koncepcji eksperci wskazali koszty wdrożenia technologii ze względu na jej nieznajomość oraz trudności w ich wdrożeniu.

Pomimo bardzo wysokiej oceny zaproponowanych rozwiązań wśród ekspertów pojawiły się również krytyczne uwagi dotyczące, kosztów wdrożenia oraz utrudnionym procesie wdrożenia technologii w początkowej jej fazie, co wynikać może z nieznajomości wdrażanej technologii, a także zróżnicowanego budżetu na poszczególnych szczeblach (gminny powiatowy, wojewódzki i krajowy). Co istotne spośród zaproponowanych rozwiązań nie można wskazać konkretnego rozwiązania stanowiącego „złoty środek” na rozwiązanie wszystkich problemów. Niemniej jednak w opinii ekspertów zaproponowane w koncepcji rozwiązania są możliwe do wdrożenia i mogą przyczynić się do usprawnienia działań zespołów zarzadzania, służb ratowniczych oraz obywateli, a także zwiększyć ich świadomość sytuacyjną na temat zagrożeń.

ZAKOŃCZENIE

Przeprowadzone w rozprawie badania literaturowe oraz ankietowe miały na celu wskazanie luk w obecnym systemie zarzadzania kryzysowego oraz w procesie informowania ludności o zagrożeniach. Na ich podstawie wyznaczone zostały możliwe do wykorzystania technologie, których zdaniem członków zespołów zarządzania kryzysowego oraz obywateli mogą przyczynić się do usprawnienia aktualnych rozwiązań oraz zmienić sposób postrzegania zagrożeń i usprawnić proces przygotowania się na nie zwiększając poziom świadomości sytuacyjnej.

Badania i analizy stały się podstawą oceny możliwości wykorzystania nowoczesnych technologii do gromadzenia, wymiany oraz obiektywizacji informacji o zagrożeniach w sytuacjach kryzysowych oraz w procesie kreowania świadomości sytuacyjnej na temat zagrożeń.

W rozdziale I przedstawiona została dziedzina problemu oraz scharakteryzowane zostały istotne pojęcia z obszaru bezpieczeństwa i zarządzania kryzysowego.

W rozdziale II zaprezentowane zostały metody badawcze, które wykorzystane zostały do oceny aktualnych rozwiązań oraz do opracowania założeń i ograniczeń do koncepcji doskonalenia systemu kreowania świadomości sytuacyjnej ludności.

W rozdziale III wyeksponowano zostały takie aspekty jak rola Rządowego Centrum Bezpieczeństwa i jego funkcje, klęski żywiołowe i stan klęski żywiołowej oraz zarzadzanie kryzysowe. Hipoteza H.1. – Świadomość sytuacyjna ludności o zagrożeniach i ryzyku utraty bezpieczeństwa w warunkach materializacji zagrożeń i kryzysów kształtuje się na niskim poziomie. Hipoteza ta bezpośrednio odwołującą się do rozdziału III została w części badawczej częściowo sfalsyfikowana. Warto bowiem zwrócić uwagę na fakt, że w grupie respondentów były osoby, dla których rozpoznawanie zagrożeń na podstawie zmysłów, przygotowywanie się do zagrożeń, planowanie niezbędnych czynności na wypadek wystąpienia zagrożenia, zrozumiałość komunikatów RCB oraz świadomość zagrożeń stanowi duży problem. Jako jeden ze sposobów na rozwiązanie tego problemu w ankiecie zwrócono uwagę na poradniki związane sytuacjami kryzysowymi, które zostały ocenione wysoko, co pokazuje, że tego typu rozwiązanie jest warte rozważenia i należy umieścić je w koncepcji doskonalenia aktualnych rozwiązań.

W dalszej części rozprawy w rozdziale IV poruszone zostały takie aspekty jak istota i proces informowania ludności w sytuacjach kryzysowych, proces i istota wymiany informacji w sytuacjach kryzysowych oraz zapewnienie informacyjnej ciągłości

działania, modele zapewnienia świadomości sytuacyjnej oraz aktualne rozwiązania dotyczące informowania ludności w sytuacjach kryzysowych. Hipoteza H.2 „W funkcjonującym systemie informowania ludności o zagrożeniach poziom świadomości sytuacyjnej ludności nie jest determinowany złożonością tego systemu.” oraz hipoteza H.3 „Skuteczność i wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej a sprawnością systemu informowania w warunkach zagrożeń i kryzysów” stanowi rozszerzenie rozdziału III o rozwiązania, których celem jest poprawa świadomości sytuacyjnej poprzez wprowadzenie nowych rozwiązań do istniejącego systemu informowania ludności. W tym celu zostały sformułowane pytania skierowane zarówno do obywateli jak i do zespołów zarządzania kryzysowego. Spośród pytań zawartych w ankiecie do obywateli jako sposób na zwiększenie świadomości sytuacyjnej ludności w trakcie zagrożeń i kryzysów wskazano takie rozwiązania jak zwiększenie etatów odpowiedzialnych za zarządzanie kryzysowe, udostępnianie większej ilości informacji na temat zagrożeń, wykorzystanie symulatorów, które ułatwiłyby przygotowanie się na zagrożenia, rozszerzenie tradycyjnych środków informacji o współczesne technologie, przygotowanie poradników o zagrożeniach dla ludności, które zostały omówione w kontekście doskonalenia istniejących rozwiązań w rozdziale III. Ponadto w celu poprawy świadomości sytuacyjnej oraz zwiększenia wydajności systemu informowania ludności o zagrożeniach skierowane zostały pytania do zespołów zarządzania kryzysowego. Jako główne czynniki, które mogą przyczynić się do poprawy systemu kształtowania świadomości sytuacyjnej wskazano zacieśnienie współpracy między podmiotami zarządzania kryzysowego, stworzenie większej liczby etatów odpowiedzialnych za zarzadzanie kryzysowe, przeprowadzenie szkoleń oraz ćwiczeń, rozszerzenie tradycyjnych rozwiązań o współczesne technologie, a także rozpowszechnianie informacji o zagrożeniach w miejscach publicznych, efektywne udostępnianie szerszej informacji o zagrożeniach w mediach społecznościowych, co pokazuje, że istnieje potrzeba wykorzystania tego środka komunikacji. Z początkiem 2022 zostało wprowadzone rozwiązanie, które umożliwia rozpowszechnianie informacji w miejscach publicznych niemniej jednak wymaga to wprowadzenia odpowiednich modyfikacji, co zostało zaprezentowane w rozdziale VI.

W rozdziale V zidentyfikowano dostępne technologie dla poprawy stanu świadomości sytuacyjnej, scharakteryzowano możliwe do wykorzystania technologie,

przeanalizowano aktualny stan wyposażenia służb RP oraz potrzeby udoskonalenia zespołów ratunkowych oraz systemu zarządzania kryzysowego. Hipoteza H.4.„ Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów." oraz H.5 „Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja." swoje potwierdzenie znajduje w pytaniach ankietowych skierowanych zarówno do obywateli jak i zespołów zarządzania kryzysowego. Respondenci zwrócili uwagę na potrzeby wykorzystania współczesnych technologii w procesie informowania ludności o zagrożeniach oraz w działaniu systemów zarządzania kryzysowego wskazując na takie rozwiązania jak Internet, media społecznościowe, telefony komórkowe, drony. Niemniej jednak zwrócono również uwagę na potrzebę wykorzystania tradycyjnych rozwiązań takich jak telewizja, radio telefon stacjonarny, syreny alarmowe, które pomimo iż nie są tak często wykorzystywane jak współczesne technologie – stanowią ich użyteczne uzupełnienie. Zważywszy na zróżnicowany wiek respondentów tradycyjne rozwiązania mogą stanowić ważny czynnik w procesie informowania o zagrożeniach oraz w kreowaniu świadomości sytuacyjnej dla osób starszych. Należy uwzględnić fakt, że pomimo rozwoju współczesnych technologii wśród obywateli są osoby, które nie przystosowały się do ich wykorzystania i preferują tradycyjne środki komunikacji. W rozdziale VI omówione zostały zatem rozwiązania umożliwiające wykorzystanie zarówno współczesnych jak i tradycyjnych rozwiązań.

W rozdziale VI przedstawiono koncepcję wykorzystania aktualnie dostępnych technologii do usprawnienia procesu informowania ludności i kształtowania poziomu świadomości sytuacyjnej w aspekcie postrzegania, zrozumienia i prognozowania zagrożeń oraz możliwości przeciwdziałania. Przedstawione w tym rozdziale propozycje zmian zostały następnie poddane ocenie wybranej grupie ekspertów, które zostały zilustrowane i przeanalizowane w rozdziale VII.

W rozdziale VII przedstawiono wyniki badań przeprowadzonych wśród grupy ekspertów (metodą wywiadu) w zakresie oceny zaproponowanej koncepcji wykorzystania technologii teleinformatycznych do doskonalenia systemu kreowania świadomości sytuacyjnej ludności. Uzyskane wyniki pozwalają na uogólniona ocenę, że zasadne jest wykorzystanie zaproponowanych rozwiązań. Przeprowadzona analiza

literatury, badania ankietowe oraz wywiad ekspercki potwierdziły, że wdrażane rozwiązania należy dostosować do potrzeb każdego podmiotu zaangażowanego w zarządzanie kryzysowe w tym obywateli i osób zarządzających tak, aby każda osoba miała możliwość wykorzystania narzędzi, które najbardziej im odpowiadają.

Na podstawie wykonanych badań i analizie istniejących rozwiązań oraz modelowaniu rozwiązań docelowych można sformułować następujące wnioski:

I. Wnioski ogólne

1. System Zarządzania Kryzysowego powinien być dostosowany do potrzeb interesariuszy zaangażowanych w zarządzanie kryzysowe w tym obywateli. Dostosowanie się do tych potrzeb powinno opierać się na wykorzystaniu technologii teleinformatycznych tak, aby informacja była aktualna i efektywnie przetwarzana na wszystkich etapach zarządzania kryzysowego.
2. Ograniczenia zdolności systemu zarządzania kryzysowego do osiągania swoich celów wynikające z braku odpowiedniej infrastruktury teleinformatycznej niezbędnej do skutecznego zarządzania kryzysowego, nieznajomości technologii, przez personel oraz z braku skutecznych rozwiązań w procesie kształtowania świadomości sytuacyjnej obywateli i dość często nieadekwatne do zagrożeń działania na wszystkich etapach zarządzania kryzysowego, co zwiększa ryzyko materializacji zagrożenia.
3. Analiza danych historycznych oraz zagrożeń w trybie online, które miały miejsce w przeszłości, a także bieżące obserwacje związane z zarządzaniem kryzysowym nie jest możliwa bez wykorzystania technologii teleinformatycznych. Technologie te dostarczają różnorodne możliwości zmierzające do identyfikowania problemów związanych z przepływem informacji i podniesieniem świadomości sytuacyjnej do pożądanego poziomu.
4. Skuteczny system zarządzania kryzysowego to jedno z głównych zadań państwa i lokalnych grup społecznych. Do skutecznej realizacji tego celu niezbędne jest sukcesywne doskonalenie istniejących rozwiązań poprzez wykorzystanie tradycyjnych i współczesnych technologii stanowiących alternatywę bądź uzupełnienie dla obecnie wykorzystywanych.
5. Przeprowadzone badania literaturowe oraz ankietowe wykazały, że poziom wykorzystywania technologii teleinformatycznych jest niewystarczający w procesie informowania i kształtowania świadomości sytuacyjnej. Stąd możliwości

zapewnienia odpowiednio wysokiego poziomu świadomości informacyjnej oraz skutecznego przepływu informacji są dość ograniczone.

II. Wnioski teoretyczno – poznawcze

1. Zróżnicowane zagrożenia powstałe na skutek katastrof naturalnych, awarii technicznych bądź działalności człowieka wymagają przygotowania skutecznego Systemu Zarządzania Kryzysowego, którego celem jest wdrożenie rozwiązań umożliwiających niezawodne przygotowanie się na nie poprzez zwiększenie poziomu świadomości sytuacyjnej, poprawę poziomu bezpieczeństwa oraz zapewnienie ciągłości działania w momencie wystąpienia zagrożenia.
2. Działania zmierzające do zastosowania technologii teleinformatycznych pozwolą na wdrożenie rozwiązań umożliwiających gromadzenie, przechowywanie i zabezpieczenie dużej ilości danych w celu niezbędnej ich analizy.
3. Szybka identyfikacja zagrożeń, ich klasyfikacja, przetwarzanie oraz wizualizacja w formie dostosowanej do potrzeb obywateli możliwa jest jedynie przy wykorzystaniu współczesnych technologii. Tylko wtedy możliwe będzie skuteczne opracowanie odpowiednich raportów dla obywateli, które umożliwią im przygotowanie się na sytuacje kryzysowe.
4. Stałe monitorowanie zagrożeń, analiza danych historycznych oraz przetwarzanie dużej ilości danych umożliwia efektywniejsze zarządzanie kryzysowe poprzez analizę wszystkich dostępnych zasobów informacyjnych w czasie rzeczywistym, dzięki czemu możliwe jest lepsze przygotowanie się na nie i zapewnienie ciągłości działania państwa w momencie ich wystąpienia.
5. Brak jednolitych procedur, zasad działania, a także niewłaściwe wykorzystanie technologii w momencie wystąpienia zagrożenia ogranicza skuteczność i efektywność działań. Niezbędne jest zatem opracowanie i realizacja odpowiednich szkoleń w różnorodnych formach dla osób wykorzystujących wspomniane rozwiązania, a także stworzenie odpowiedniej infrastruktury niezbędnej do wykorzystania technologii.
6. Specyfika problemów badawczych pracy wywodzi się z obszaru nauk o bezpieczeństwie, co oznacza, że oprócz metod uniwersalnych, takich jak analiza systemowa, można zastosować także metody opisu jakościowego i analizy jakościowej badanej rzeczywistości. Koncepcja systemu powinna zapewnić kompletność i spójność podejścia do oceny i identyfikacji ryzyka wystąpienia zagrożeń. Przedstawione w pracy hipotezy dotyczące zasadności

wykorzystania współczesnych i tradycyjnych technologii w procesie informowania o zagrożeniach i kształtowania świadomości sytuacyjnej można zweryfikowano zarówno poprzez opinie osób zajmujących się bezpieczeństwem, zarządzaniem i informatyką, jak i poprzez samoocenę, analizę literatury i case study.

III. Wnioski dedykowane do praktyki zarządzania kryzysowego

1. System zarządzania kryzysowego powinien być stale doskonalony i analizowany zarówno pod kątem horyzontu czasowego, jak i ewolucji zagrożeń w poszczególnych fazach zarządzania kryzysowego. W związku z tym ważna jest ocena stanu zasobów, możliwości technicznych oraz funkcji i warunków, jakie musi spełniać. Ocena ta powinna skupiać się na identyfikacji rzeczywistych i użytecznych technologii służących do monitorowania, informowania, gromadzenia i przetwarzania dużych zbiorów danych oraz zapewniania ciągłości działania na wszystkich etapach zarządzania kryzysowego.
2. Skuteczne zarządzanie kryzysowe to wieloaspektowa identyfikacja zagrożeń, określenie ich zakresu i złożoności, identyfikacja infrastruktury krytycznej, miejsc zbiórek oraz punktów udzielania pierwszej pomocy oraz przypisanie zadań odpowiednim służbom, łagodzenie skutków zdarzenia, zapewnienie skutecznego przepływu informacji, a także ciągłe monitorowanie zagrożeń, informowanie społeczeństwa o zagrożeniu i określenie działań, jakie powinny być podjęte w danym miejscu i czasie.
3. O zapewnieniu ciągłości działania określonych podmiotów w warunkach zagrożeń i kryzysów decyduje niezawodność procesów informacyjno-decyzyjnych, które są wspierane przez obecnie stosowane rozwiązania rozszerzone o tradycyjne i współczesne technologie nieużywane dotychczas przy uwzględnieniu ograniczeń czasowych, finansowych i technicznych.
4. Opracowanie strategii działania w momencie wystąpienia zagrożenia oraz oszacowanie ryzyka jego wystąpienia uwarunkowane jest ograniczeniami zarówno finansowymi jak i czasowymi, które mogą utrudnić proces wdrożenia technologii na szczeblach gminnych, powiatowych i wojewódzkich.
5. Doskonalenie procesów decyzyjnych oraz skuteczne reagowanie na zagrożenia, a także przywracanie stanu eliminującego lub ograniczającego skutki materializacji tych zagrożeń po zaistniałej sytuacji kryzysowej przy istniejących

ograniczeniach wymaga wprowadzenia licznych zmian i udoskonaleń zmierzających do eliminacji luk w aktualnie funkcjonującym systemie poprzez:

a) wdrożenie i współdziałanie współczesnych i tradycyjnych technologii możliwych do zastosowania w zarządzaniu kryzysowym;
b) wzmocnienie użyteczności tych technologii poprzez opracowanie odpowiednich instrukcji ich obsługi oraz szkoleń, których celem jest precyzyjne wskazanie możliwości i potencjału zaproponowanych rozwiązań, a także zasady ich funkcjonowania;
c) zapewnienie systemowych zmian w procesie informowania ludności o zagrożeniach oraz w zakresie kreowania świadomości sytuacyjnej na ich temat;
d) systematyczne szkolenie w zakresie zwalczania i przygotowania się na zagrożenia oraz systematyczne aktualizowanie informacji o dostępnych siłach i środkach co mogą ułatwić nowoczesne technologie informacyjne.

6. Wykorzystanie współczesnych technologii jest uzależnione od dostępu do Internetu oraz sieci energetycznej. Brak odpowiedniej infrastruktury, alternatywnych rozwiązań oraz odpowiednio przeszkolonego personelu może ograniczyć użyteczność wspomnianych technologii lub zwiększać ich podatność na ataki oraz ryzyko utraty ciągłości działania na skutek niewłaściwego ich wykorzystania.
7. Do zwiększenia poziomu świadomości sytuacyjnej na temat zagrożeń niezbędne jest opracowanie strategii działania zmierzającej do dotarcia do jak największego grona odbiorców wykorzystując zarówno współczesne jak i tradycyjne technologie ze względu na zróżnicowanie wiekowe, miejsce zamieszkania i wykształcenie.
8. Komunikaty, instrukcje, szkolenia, poradniki oraz inne materiały przeznaczone dla obywateli powinny być proste, zrozumiałe i zawierać wyłącznie istotne informacje.
9. Zapewnienie ciągłości działania w momencie wystąpienia zagrożenia oraz wysokiego poziomu świadomości sytuacyjnej członków Zespołów Zarządzania Kryzysowego, służb ratowniczych oraz obywateli powinno się odbywać zgodnie z modelami kształtowania świadomości sytuacyjnej (standard M.R. Endsley, pętla OODA lub kolory Coopera), które umożliwiają holistyczne ujęcie procesu lepsze przygotowania się na zaistniałe zagrożenia oraz te, które mogą wystąpić w przyszłości.

Autor ma nadzieję, że propozycje rozwiązań koncepcyjnych stanowią istotny wkład do nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Potwierdzeniem tej konkluzji jest wielosektorowa analiza dostępnych rozwiązań wykorzystywanych przez Zespoły Zarządzania Kryzysowego w zakresie przygotowania się na zagrożenia oraz w procesie informowania ludności o zagrożeniach. Koncepcja doskonalenia systemu kreowania świadomości sytuacyjnej ludności jest wskazaniem sposobu eliminacji standardowych luk w istniejącym SZK poprzez wykorzystanie współczesnych i doskonalenia tradycyjnych rozwiązań w celu zapewnienia informacyjnej ciągłości działania, powiązanej z procesem informowania ludności o zagrożeniach oraz zwiększenia ich świadomości sytuacyjnej. W ten sposób zweryfikowano hipotezę główną mówiącą o tym, że system informowania ludności posiada istotne luki, co ujemnie wpływa na poziom świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów, które można eliminować poprzez wykorzysta-nie nowoczesnych rozwiązań teleinformatycznych (IT/ICT).

BIBLIOGRAFIA

I. Akty prawne:

1. Dekret z dnia 23 kwietnia 1953 r. o świadczeniach w celu zwalczania klęsk żywiołowych.
2. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
3. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 22 stycznia 2021 r. w sprawie ogłoszenia jednolitego tekstu ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2021 r. poz. 372).
4. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 31 sierpnia 2016 r. w sprawie ogłoszenia jednolitego tekstu ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej.
5. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 5 lipca 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Dz. U. 2019 poz. 1398).
6. Obwieszczenie Prezesa Rady Ministrów z dnia 24 marca 2015 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Prezesa Rady Ministrów w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa
7. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy (Dz. U. 2002 nr 217, poz. 1833).
8. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy (Dz. U. 2002 nr 217, poz. 1833).
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego
10. Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania (Dz. U. Nr 226 poz. 1810)
11. Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin.
12. Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach
13. Ustawa z 7 lipca 1994 r. Prawo budowlane (Dz.U. z 2010 r. nr 243, poz. 1623 z późn. zm.)
14. Ustawa z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r.
15. Ustawa z dnia 10 maja 2018 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. 2018 poz. 1118)
16. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne
17. Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 2138).
18. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2017 r. poz. 1897).
19. Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej
20. Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego.
21. Ustawa z dnia 24 sierpnia 1991 o Państwowej Straży Pożarnej

22. Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej
23. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590).
24. Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu i zwalczaniu zakażeń i chorób zakaźnych i ludzi (Dz.U. z 2021 r. poz. 2069).
25. Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane (Dz.U. z 2021 r. poz. 2351).
26. Ustawa z dnia 7 lipca 1994 r.- Prawo budowlane (Dz. U. z 2019 r. poz. 1186 z późn. zm.).

II. Pozycje zwarte:

1. Ahern J., Gun *Digest Buyer's Guide to Concealed-Carry Handgun,* [w:] Gun Digest Books, Stany Zjednoczone, 2010.
2. Alsalamah S., Nuzzolese E., *Promising Blockchain technology applications and use case designs for the identification of multinational victims of mass disasters*, [w:] Front *Blockchain* 2020.
3. Bajkiewicz – Grabowska E., Mikulski Z., *Hydrologia ogólna*, [w:] PWN, Warszawa 2007.
4. Bolstad C.A., Endsley M.R., *Tools for supporting team collaboration, Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society, Santa Monica, CA: HFES*.
5. Borowska-Mostafa D., *Encyklopedia PWN A-Z Oryginalna Azetka*, [w:] Wydawnictwo Naukowe PWN SA, Warszawa, 2012.
6. Chalmers D., The *Conscious Mind: In Search of a Fundamental Theory*, [w:] Oxford University Press", 1997.
7. Cuzzocrea A., Russo V., Saccà D., *A Robust Sampling-Based Framework for Privacy Preserving* OLAP, [w:] DaWaK, 2008.
8. Czekaj J., *Podstawy zarządzania informacją*, [w:] Uniwersytet Ekonomiczny w Krakowie, 2012.
9. Dąbrowski T.J., Komunikacja kryzysowa jako narzędzie kształtowania reputacji, [w:] "Marketing i Rynek" 2010
10. Endsley M. R., Jones D., *Designing for Situation Awareness(Second ed.).* [w:] Wydawnictwo CRC Press 2012.
11. Endsley M. R., *Theoretical underpinnings of situation awareness: A critical review*, M.R. Endsley & D.J. Garland (red.), Situation awareness analysis and measurement, Mahwah, NJ: LEA, 2000.
12. Endsley M. R., *Toward a theory of situation awareness in dynamic systems*, [w:] Human Factors, 1995.
13. Fehler W., *Zagrożenie – kluczowa kategoria teorii bezpieczeństwa*, [w:] Współczesne postrzeganie bezpieczeństwa, red. K. Jałoszyński, B. Wiśniewski, T. Wojtuszek, Wyższa Szkoła Administracji, Bielsko Biała 2007.
14. Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, [w:] *BEL Studio*, Warszawa, 2007.
15. Fryźlewicz Z., Nikończuk D., Windows Azure. Wprowadzenie do programowania w chmurze, [w:] Helion, Gliwice 2012
16. Górnikiewicz M., Szczurek T. Determinanty kształtowania bezpieczeństwa wewnętrznego [w:] Ślachcińska E. (red.), Prognozowanie międzynarodowych stosunków wojskowych na podstawie uwarunkowań społeczno-kulturowych, , 2017, Poznań.
17. Grocki R., *Vademecum zagrożeń*, [w:] *Bellona*, Warszawa 2003.

18. Grunig L.A., Grunig J.E., Dozier D.M., *Excellent public relations and effective organizations: A study of communication management in three countries*, [w:] Lawrence Erlbaum Associates, New York, 2002.
19. Hołówka J., Dziobkowski B., Panorama współczesnej filozofii, [w:] Wydawnictwo Państwowe Wydawnictwo Naukowe, Warszawa, 2016, s. 329.
20. Hon, W. K., Millard, C., Walden, I., *Who is Responsible for 'Personal Data' in Cloud Computing?* [w:] The Cloud of Unknowing, Part 2, 2011
21. Jagusiak B., *Bezpieczeństwo socjalne współczesnego państwa*, [w:] Difin, Warszawa 2015.
22. Jakubczak R., *Obrona narodowa w tworzeniu bezpieczeństwa III RP,* Dom Wydawniczy BELLONA, Warszawa 2003,
23. Jurek M., Staruch M., Potencjał wykorzystania technologii 5G i *Big Data* w kreowaniu świadomości sytuacyjnej w aspekcie ochrony danych osobowych, Ochrona danych osobowych. Perspektywa krajowa i międzynarodowa, red. K. Śmiałek, A. Kominek, Wydawnictwo Naukowe FNCE, Poznań 2021
24. K. Holla, J. Ristvej, M. Titko, *Crisis* Management [w:]Theory and Practice, IntechOpen United Kingdom, 2018.
25. Kennedy C., *Situational Awareness: The Urban Preppers Ultimate Guide to Situational Awareness and Survival Paperback*, [w:] CreateSpace Independent Publishing Platform, USA, 2016.
26. Kitler W., Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system, Akademia Obrony Narodowej, Warszawa 2011.
27. Kitler W., Skrabacz A., *Bezpieczeństwo ludności cywilnej. Pojęcie, organizacja i zadania w czasie pokoju, kryzysu i wojny*, [w:] Wydawnictwo Towarzystwo Wiedzy Obronnej, Warszawa 2010.
28. Kitler W., Skrabacz A., Ochrona ludności i obrona cywilna w świetle współczesnych uwarunkowań bezpieczeństwa narodowego, [w:] AON, Warszawa 2009.
29. Kitler W., *Zarządzanie kryzysowe jako element zarządzania bezpieczeństwem narodowym*, [w:] System reagowania kryzysowego, red. J. Gryz, W. Kitler, Wydawnictwo A. Marszałek, Toruń 2001.
30. Konieczny J., *Zarządzanie w sytuacjach kryzysowych, wypadkach i katastrofach*, [w:] Poznań-Warszawa GARMOND Oficyna Wydawnicza, 2001.
31. Korycki S., *System bezpieczeństwa Polski*, [w:] *AON,* Warszawa, 1994.
32. Kotarbiński T, Traktat o dobrej robocie, [w:] Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2019.
33. Kotarbiński T., Elementy teorii poznania, logiki formalnej i metodologii nauk, [w:] PAN, Wrocław 1990.
34. Kowalewski J. , Kowalewski M., *Polityka bezpieczeństwa informacji w praktyce,* [w:] Presscom Sp. z o.o.,Wrocław 2004.
35. Krutz R.L., Vines R.D., Cloud Security. A comphersive Guide to Secure *Cloud Computing*, Indi-anapholis, Whiley Publishing INC, 2010.
36. Krynojewski F.R., Mazur S., Podstawy wiedzy o zarządzaniu, [w:] F.R. Krynojewski, S. Mazur, G. Mikrut, P. Tchorzewski, Zarządzanie kryzysowe, obrona cywilna kraju, ochrona informacji niejawnych, Akademia
37. Liddell H. G., Scott R., Jones H. S., *A Greek–English Lexicon*,, [w:] *Oxford University Press*, Wielka Brytania, 1940.
38. Liderman K., *Bezpieczeństwo informacyjne*, [w:] PWN, Warszawa 2012.
39. Łobocki M., *Metody badań pedagogicznych*, [w:] PWN, Warszawa 1984.

40. Logeswaran L., Bandara H. M. N. D., and. Bhathiya H. S*., Performance, Resource, and Cost Aware Resource Provisioning in the*, in 2016 IEEE 9th International Conference on *Cloud Computing* (CLOUD), 2016, s. 913–916.
41. Longo F., Nicoletti L., Padovano A., *Emergency preparedness in industrial plants: a forward-looking solution based on industry 4.0 enabling technologies*, [w:] Comput. Ind. 105, 2019.
42. Macierzyński W., *Rola mediów w komunikacji kryzysowej*, red. M. Jabłonowski, L. Smolak, [w:] Zarządzanie kryzysowe w Polsce, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2007
43. Marczak J*., Bezpieczeństwo narodowe – pojęcie, charakter, uwarunkowania*, [w;] red. R. Jakubczak, J. Flis, Bezpieczeństwo narodowe Polski w XXI wieku: wyzwania i strategie, Bellona, Warszawa 2006.
44. Marczak J*., Bezpieczeństwo narodowe – pojęcie, charakter, uwarunkowania* ,[w:] R. Jakubczak, J. Flis *(*red.), *Bezpieczeństwo narodowe Polski w XXI wieku: wyzwania i strategie, Bellona*, Warszawa 2006
45. Mateos A., Rosenberg J., Chmura obliczeniowa. Rozwiązania dla biznesu. [w:] Helion, Gliwice 2011.
46. McLuhan M., *Zrozumieć media. Przedłużenia człowieka*, przedm. L.H. Lapham, przeł. N. Szczucka, [w:] Wydawnictwo WNT, Warszawa 2004
47. Michailiuk B., *Praca naukowo badawcza Korelacja systemu ochrony ludności z systemem zarzadzania*., [w:] D. Majchrzak, B. Michailiuk, J. Denysiuk, Warszawa, 2016.
48. Michalski T., *Zagrożenia we współczesnym świecie jako temat edukacji geograficznej*, [w:] Szkolne i Pedagogiczne, 2008.
49. Nadarzewski M., *Procesy i zjawiska zachodzące w bezpieczeństwie Polski*, [w:] Ochrona infrastruktury krytycznej, WSPol red*.* A. Tyburska, Szczytno, 2010.
50. Oleński J., *Ekonomika informacji*: *Metody,* [w:] PWE, Warszawa 2003.
51. Otałęga Z., *Encyklopedia biologiczna tom X,* Wydawnictwo Agencja Publicystyczno-Wydawnicza Opres, Kraków 2000.
52. Otwinowski W., *Podstawy Zarządzania Kryzysowego I Systemu Obronnego,* [w:] Wydawnictwo Wyższej Szkoły Handlu i Usług Poznań 2015
53. P. Potejko, *Bezpieczeństwo informacyjne,* [w:] Bezpieczeństwo państwa, Warszawa 2009.
54. Pacek B., Hoffmann R., *Działania sił zbrojnych w cyberprzestrzeni,* [w:] AON, Warszawa 2013.
55. Pawłowski J., Zdrodowski B., Kuliczkowski M., *Słownik terminów z zakresu bezpieczeństwa narodowego,* [w:] Akademia Obrony Narodowej, Warszawa 2008.
56. Pawłowski J., *Zarys teorii sytemu bezpieczeństwa państwa*, [w:] Akademia Obrony Narodowej, Warszawa 2013.
57. Perlman A., Sacks R., Barak R., Hazard recognition and risk perception in construction, [w:] Saf. Sci. 64, 2014.
58. Phillip M., Kerrow C., Jo Abrantes. "*Robots in Urban Search and Rescue Operations",* [w:] Proceedings Aukland ACRA 2002.
59. Piwowarski J., *Polska droga od filozofii bezpieczeństwa do nauk o bezpieczeństwie i kultury bezpieczeństwa*, red. M. Kubiak, [w:] Konteksty bezpieczeństwa personalnego i strukturalnego – jedność w różnorodności, 2021.

60. Piwowarski J., Zachuta A., *Pojęcie bezpieczeństwa w naukach społeczno-prawnych*, [w:] Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2013.
61. Poseł-Częścik E., *Kryteria bezpieczeństwa państwa,* [w:] Wydawnictwo Kryteria bezpieczeństwa międzynarodowego państwa, PISM*,* Warszawa 2003.
62. Qyarantelli E.L., *What is a Disaster? Perscpective on the Qestion*, Routledge; 1st edition, London 1998.
63. Rokitowska J., *Vademecum Bezpieczeństwa*, red. O. Wasiuta, R. Klepka, R. Kopeć, [w:] LIBRON– Filip Lohner, 2018, Kraków.
64. Rozwadowska B., Public relations w sytuacjach kryzysowych, Wrocław 2002.
65. S. Tomasz, *Badania przyczyn pożarów.* [w:] Elamed, Katowice 2008.
66. Salmon P. M., Stantion N. A., Walker G. H., Jenkins D. P., *Distributed Situation Awareness Theory, Measurement and Application to Teamwork , [*w:] Ashigate, Wielka Brytania 2009.
67. Seitel F.P., *Public Relations w praktyce,* [w:] Felberg SJA, Warszawa 2003.
68. Skoczylas J. J., *Prawo ratownicze, wyd. 2*, [w:] LexisNexis, Warszawa 2011.
69. Skomry *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, [w:] Presscom, Wrocław 2010.
70. Smolak L., *Zarządzanie kryzysowe w Polsce*, [w:] Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk 2007.
71. Sobolewski G., Model *zarządzania przepływem informacji w sytuacjach kryzysowych*, [w:] *Akademia Obrony Narodowej*, Warszawa 2013.
72. Sobolewski G., Zagrożenia kryzysowe,[w:] AON, Warszawa 2011
73. Sobolewski G., Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego, [w:], Wybrane zagadnienia zarządzania kryzysowego, red. G. Sobolewski, D. Majchrzak, Warszawa 2012.
74. Stańczyk J., Kres „zimnej wojny". Bezpieczeństwo europejskie w procesie zmiany międzynarodowego układu sił (na przełomie lat osiemdziesiątych. i dziewięćdziesiątych XX w.), Wydawnictwo Adam Marszałek, Toruń 2004.
75. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, [w]: R. Jakubczak i inni, Podstawy bezpieczeństwa narodowego Polski w erze globalizacji, Warszawa 2008.
76. Stańczyk K., Geopolityczne aspekty bezpieczeństwa, [w:] Wydawnictwo Akademickie AMW, Gdynia, 2019.
77. Staruch M., praca inż. pt. „Analiza porównawcza wybranych maszyn wirtualnych" napisana pod kierunkiem, dr inż. R. Hoffmana, WAT, Warszawa, 2014.
78. Staruch M., praca mgr. pt.*, „Cyberterroryzm jako współczesne zagrożenie informacyjnego bezpieczeństwa kraju"* napisana pod kierunkiem, dr inż. R. Hoffmana, WAT, Warszawa, 2018.
79. Stoner J. A. F., Freedman R. E., Gilbert D. G. Jr., *Kierowanie*, [w:] Wydawnictwo Państwowe Wydawnictwo Ekonomiczne, Warszawa 1998.
80. Świniarski J., *O naturze bezpieczeństwa,* [w:] Agencja Wydawnicza ULMAX, Warszawa 1999.
81. Szczurek T., *Problemy podejmowania decyzji w sytuacjach kryzysowych,* [w:] Świadczenie na rzecz obrony realizowane w sytuacjach kryzysowych AON, Warszawa 2006.
82. Szwarc K., Zaskórski P., *Ciągłość działania systemów zapewniania bezpieczeństwa*, [w:] Współczesne wyzwania bezpieczeństwa Polski, WAT*,* red. B. Jagusiak, Warszawa 2015.

83. Szymańska A., *Efektywna komunikacja w zarządzaniu kryzysami i problemami*, red. Tworzydło D., Soliński T., [w:] Public relations – wyzwania współczesności, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Rzeszów 2004.
84. Tokarski J., *Słownik wyrazów obcych*, [w:] PWN, Warszawa 1980
85. Wołoszyn E., *Meteorologia i klimatologia w zarysie*, [w:] Wydawnictwo Politechniki Gdańskiej, 2009.
86. Woźniak J., Staruch M., Jurek M., Wereda W., Zaskórski P., *Jak uczyć (się) zdalnie?*, [w:] Wydawnictwo CeDeWu, Warszawa 2020.
87. Wróblewski R. *Wprowadzenie do strategii wojskowej*, [w:] AON, Warszawa, 1998.
88. Wychowania Fizycznego, Katowice 2003
89. Zaskórski P, Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania, WAT, Warszawa, 2011.
90. Zaskórski P. , Asymetria informacyjna w zarządzaniu procesami, [w:] Wojskowa Akademia Techniczna, Warszawa 2012.
91. Zaskórski P., Zaskórski W, Woźniak J., *Świadomość sytuacyjna, a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, [w:] *CeDeWu,* Warszawa 2021.
92. Żebrowski A., Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej, Kraków 2012.
93. Ziarko J., Walas-Trębacz J., *Podstawy zarządzania kryzysowego.* Część 1. Zarządzanie kryzysowe w administracji publicznej, [w:] Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010.

III. Artykuły:

1. Abgarowicz G., Abgarowicz I., *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, Uniwersytet Szczeciński Zeszyty Naukowe Nr 882, Szczecin 2015.
2. Adamkiewicz M., Wokół rozważań nad bezpieczeństwem egzystencjalnym, czyli interpretacje śmierci w nauce, [w:] Studia Bezpieczeństwa Narodowego, 2013, nr 4.
3. Banduka N., Veza I., Bilic B., *An integrated lean approach to Process Failure Mode and Effect Analysis w: A case study from automotive industry, Advances In Production Engineering & Management*, 2016.
4. Baniak K., *Analiza zagrożeń telekomunikacyjnych sektora publicznego, Bezpieczeństwo w telekomunikacji i teleinformatyce*, Biblioteka „Bezpieczeństwa Narodowego", kwartalnika wydawanego przez Biuro Bezpieczeństwa Narodowego, tom 3, 2007.
   https://www.bbn.gov.pl/download/1/1000/analizazagrozen.pdf
5. Barney J., *Firm resources and sustained competitive advantage*, "Journal of Management" , Vol. 2, 1991.
6. Bartosiewicz S. *IT and telematic systems in Polish logistics centres,* Przedsiębiorczość i Zarządzanie w: SAN, Tom XIV, Zeszyt 7, 2013.
7. Bolstad C.A Endsley ., M.R., *Tools for supporting team collaboration,* Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society, Santa Monica, CA: HFES.
8. Boyd J., The essence of winning and losing. June 28, 1995; https://fasttransients.files.wordpress.com/2010/03/essence_of_winning_losing.pdf.
9. Buckler S. A., *The Spiritual Nature of Innovation*. Research Technology Management, 1997, Vol 40/2.

10. Burnett J. J., *A strategic approach to managing crises, Public Relations Review*, 1998, Vol. 24, No 4.
11. Chen N. and Chen A. *The role of data mining techniques in emergency management*, In Proceedings of the 11th International Conference on Enterprise Information Systems - Volume 2: ICEIS, .2009
12. Communicating in a Crisis: Risk Communication Guidelines for Public Officials. Rockville, MD, Substance Abuse and Mental Health Services Administration, 2019 (https://store.samhsa.gov/sites/default/files/d7/priv/pep19-01-01-005.pdf)
13. Czapliński W., *Bezpieczeństwo, spokój i porządek publiczny – próba konstrukcji teoretycznej*, „Gazeta Administracji i Policji Państwowej" 1929, nr 19.
14. Dahns F., *A Practical Guide to Public Information during a Crisis (Budapest Guidelines III)*, NATO Civil Preparedness Civil Protection Group.
15. Domalewska D., *Wielowymiarowość komunikacji w kontekście bezpieczeństwa*. Komunikacja w sytuacjach kryzysowych i komunikacja strategiczna, Warszawa 2020
16. Domiguez C., Vidulich M., Vogel M.E., McMilan G., *Situation awerenesss: Papers and annotated bibliography, Human System Center*,1994.
17. Dong B. Y., Zhang Z. Q., Xu L J, *Research status and development trend of intelligent emergency rescue equipment* Journal of Mechanical Engineering, 2020 (11).
18. Gaździcki J., *Technologie i infrastruktury informacji przestrzennej w zastosowaniu do zarządzania kryzysowego,* Warszawa: Roczniki Geomatyki, tom IV, zeszyt 1.,2006.
19. Goldsteen R., Schorr J.K.,. *The long-term impact of a man-made disaster: An examination of a small town in the aftermath of the Three Mile Island Nuclear Reactor Accident, Disasters*, Department of Sociology Stetson University DeLand, Florida, U.S.A, 1982, Vol. 6, No. 1.
20. González-Herrero A., Pratt C.B., *An integrated symmetrical model for crisis-communication management, "*Journal of Public Relations Research*"*, 1996, Vol.8, No.2.
21. Grace K., Salvatier J., Dafoe A., Zhang B., Evans O., When Will AI Exceed Human Performance? Evidence from AI Experts, https://*AR*xiv.org/pdf/1705.08807.pdf
22. Greer P.M., McKerrow, P.J., *Robots in Urban Search and Rescue Operations",* Proceedings , Aukland ACRA 2002.
23. Gruntfest E., Weber M., *Internet and emergency management:* Prospects for the future 1998.
24. Gruntfest, E., Weber, M., *Internet and emergency management*, Prospects for the future 1998.
25. Heldman, A.B., Schindelar, J., & Weaver, J., *Social media engagement and public health communication: Implications for public health organizations being truly "social*." Public Health Reviews, 35(1).
26. Hennig B., *Cartesian Conscientia,* British Journal for the History of Philosophy, 2007, vol. 15, No.3.
27. Hosny A., Parmar C., Quackenbush J., Schwartz LH., Aerts Hj., *Artificial intelligence in radiology*. Nat Rev Cancer. 2018.
28. Hutton G., Fosdick M., *The Globalization of Social Media*, Journal of Advertising Research 2011, Vol. 51.

29. Kołodziejczyk K., *Personalny wymiar bezpieczeństwa*, [w:] Periodyk Naukowy Akademii Polonijnej, 2010, Nr 1.
30. Kompała D., *istota zagrożeń,* Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 3, 2014.
31. Kompała D., *istota zagrożeń,* Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 3.
32. Kowalczyk T., *Przeobrażenia struktury przestrzennej osadnictwa i zmiany hydrotechniczne w dolinie Wisły wywołane powodzią zimową 1982 roku w województwie płockim*, „Notatki Płockie" 1983, nr 1/114, s
33. Langseth J., Vivatrat N., Why Proactive Business Intelligence is a Hallmark of the Real-Time Enterprise: Outward Bound," Intelligent Enterprise, (5)18, 2003.
34. Lawhorn R., *Tarantino-Style Approach to Secure Cloud Computing*, Sec Techno, 2010.
35. Lukáš L, Hrůza P, Kný M., *Information Management in Security Components*, Prague: Ministry of Defence of the Czech Republic; 2008.
36. M. Szyłkowska, *Cyfrowa globalizacja determinantem współczesnego bezpieczeństwa*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Legnica 2015, nr 16.
37. Manyika J., Chui M., Bughin J., Brown R., Dobbs R., Roxburgh Ch., *Big Data*: The next frontier for innovation, competition, and productivity, McKinsey Global Institute 2021.
38. Marek H., Współczesne zagrożenia naturalne Polski w świadomości społeczeństwa, na przykładzie reprezentatywnej grupy mieszkańców miasta Rybnika i powiatu rybnickiego (woj. śląskie), s. 37, dostęp w Internecie na *www.seminarium.21/edu.pl/*ks/5/0004%20MAREK.pdf. (data dostępu 10.07.2021)
39. Mell P., Grance. T., Special Publication 800-145 (Draft): The NIST Definition of *Cloud Computing* (Draft) – Recommendations of the National Institute of Standards and Technology. [On-line]. National Institute of Standards and Technology. Dostęp na stronie: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
40. Michałowski S., *Bezpieczeństwo ekonomiczne w stosunkach Wschód – Zachód*, Sprawy międzynarodowe, Warszawa ,1990, Vol. 36, nr.4.
41. Moneta A., *Zeszyty Naukowe Ruchu Studenckiego*, Wydawnictwo Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. T. Kościuszki Nr 1, 2016.
42. Nowacki G., *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, nr 44, część 1, 2015.
43. Ogórek M., Zaskórski P., *Internet Rzeczy W Integracji Procesów Zarządzania Kryzysowego*, Zeszyty Naukowe Politechniki Poznańskiej, Organizacja i Zarządzanie nr 76, Poznań 2018.
44. Pawlak M., Świadomość sytuacyjna a czynniki kulturowe. https://www.academia.edu/11791913/
45. Peng L, Xu W H, Su Y C, *New infrastructure" and smart emergency*, China Emergency Management Science, 2020.
46. Perrin A., & Anderson, M., *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. Fact Tank: News in the Numbers. Washington, DC: Pew Research Center* (dostęp 22.07.2022 https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostlyunchanged-since-2018).

47. Perrin A., Anderson M., Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. Fact Tank: News in the Numbers. Washington, DC: Pew Research Center (dostęp 22.07.2022 https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostlyunchanged-since-2018)
48. Pokorski G., Zaskórski P., *Systemy informacji geoprzestrzennej w zarządzaniu procesami biznesowym,* Nowoczesne Systemy Zarządzania, Zeszyt 13, nr 2, Wojskowa Akademia Techniczna, 2018.
49. *Public Leadership Under Pressure*. Cambridge, UK: Cambridge University Press; 2016, *A Practical Guide to Public Information during a Crisis* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170612_170612-Budapest_Guidelines_en.pdf (dostęp w internecine 21.08.2021)
50. Rahmi, R., Joho, H., Shirai, T*., An Analysis of Natural Disaster-Related Information-Seeking Behavior Using Temporal Stages*. Journal of the Association for Information Science and Technology 70(7), 2018.
51. Samuel AL., *Some studies in machine learning using the game of checkers*. IBM J Res Dev. 1959.
52. Santucci G., "*From Internet of Data to Internet of Things*," in International Conference on Future Trends of the Internet, 2009.
53. Sapriel C. *Effective crisis management: tools and best practice for the new millennium*, Journal of Communication Management*,* 2003,vol. 7, No.4.
54. Senthilvel G. - Exploring the concepts of Artificial Intelligence dostęp na stronie (https://www.codeproject.com/*AR*ticles/1182210/*AR*tificial-Intelligence)
55. Shah, B. and Choset H. (2003), "*Survey on Urban Search and Rescue Robotics",* CMU, Pittsburgh, 2003.
56. Shrivastava P., *Crisis theory / practice: towards a sustainable future, Industrial & Environmental Crisis Quarterly,* USA, Sage Publications, 1993, Vol 7 no. 1.
57. Smits S.J., Ezzat N., *Thinking the unthinkable' – leadership's role in creating behavioral readiness for crisis management,* Competitiveness Review,2003, Vol 13, No.1.
58. Szczepańska J., *Świadomość sytuacyjna – Vademecum kierowcy* „ Drogownictwo" , Warszawa, 2010, nr 10.
59. Turing A. , *Maszyny myślące a inteligencja*, [w:] Maszyny matematyczne i myślenie, tłum. D. Gajkowicz, Warszawa 1972.
60. T*VR*díková M. Implementation and Innovation of Information Systems in Companies. 1st ed. Prague: Grada; 2010.
61. Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. *The risk perception paradox: Implictions for governance and communication of natural hazards*, Risk Analysis, 33(6), 2013.
62. Walczak W., *Zarządzanie kryzysowe – rola i zadania organów administracji państwowej,* „Przedsiębiorczość i Zarzadzanie" nr 8 z 11.08.2009 r., s.108.
63. Wang RY., *Journal of Management Information Systems,* 1996, Vol. 12, No. 4.
64. Warzecha K., *Technologie informacyjno-komunikacyjne wykorzystywane przez młodzież - szanse i zagrożenia,* Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*,* Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2018 nr 13.
65. Yue X., Wang H., Jin D., Li M. ,Jiang W., *Healthcare data gateways: found healthcare intelligence on Blockchain with novel privacy risk contro,*. J Med Syst 2016; 40(10).

66. Zaborowski J., *Administracyjno-prawne ujęcie pojęć bezpieczeństwo publiczne*
i porządek publiczny, niektóre uwagi w świetle unormowań prawnych, Zeszyty Naukowe Akademii Spraw Wewnętrznych, Warszawa 1985, nr 41.
67. Zaskórski P., *Integracja Zasobów I Usług Informacyjnych w Organizacji Biznesowej*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, nr 7, Warszawa, 2012.
68. Zaskórski P., Jurek M., Internet Rzeczy w Integracji procesów logistycznych w Systemach Zarządzania *Kryzysowego*, Gospodarka Materiałowa i Logistyka nr 5, 2018.
69. Zaskorski P., Wozniak J., Implications of Industry 4.0 for Security in Contemporary Organizations – Perspective of Information Strategies, European Research Studies Journal, Volume XXV, Issue 1, 2022.
70. Zawiła-Niedźwiecki J., *Analogie zarządzania kryzysowego z zarządzaniem ryzykiem operacyjnym przedsiębiorstwa*, Logistyka, nr 5.
71. Zeng, L., Xu, L., Shi, Z., Wang, M., & Wu, W. Techniques, process, and enterprise solutions of business intelligence. In IEEE International Conference on Systems, Man and Cy-bernetics (Vol. 6), 2006.

IV. Źródła internetowe:

1. gminadebno.pl/katastrofy-budowlane.html
2. http://adamkorcz.dl.interia.pl/,
3. http://aims.fao.org/information-and-communication-technologies-ict
4. http://bigdatariding.blogspot.com/2013/10/cloud-computing-types-of-cloud.html
5. http://rcb.gov.pl/wp-content/uploads/RCB-Zagro%C5%BCenia-okresowe-w-Polsce-aktualizacja.pdf
6. http://web.archive.org/web/20110
7. http://www.cisco.com/web/about/ac79/innov/IoE.html
8. http://www.cmagriffin.com/situational-awareness-level/
9. http://www.nwlink.com/~donclark/leadership/ooda.html
10. https://asystentbhp.pl/przyczyny-awarii-sieci-gazowych/
11. https://bezpieczna.um.warszawa.pl/zarzadzanie-kryzysowe
12. https://blogs.worldbank.org/dev4peace/exploiting-full-potential-new-technologies-data-collection-monitoring-and-conflict-prevention
13. https://businessinsider.com.pl/poradnik-finansowy/Blockchain-na-czym-polega/fdctpsb
14. https://ctif.org/news/panic-and-human-behavior-fire-emergency-situations
15. https://doit.software/blog/big-data-technologies
https://www.javatpoint.com/big-data-characteristics
16. https://ec.europa.eu/digital-single-market/en
17. https://epodreczniki.pl/a/ostrzeganie-i-alarmowanie/D9S0KGBEH
18. https://epodreczniki.pl/a/zadania-obrony-cywilnej-i-ochrona-ludnosci/Dkf7nISSZ
19. https://epodreczniki.pl/a/zagrozenia-w-czasie-pokoju/D1EuS4od1
20. https://imtech.imt.fr/en/2022/09/15/virtual-reality-to-improve-crisis-management-and-cybersecurity/
21. https://intellipaat.com/blog/tutorial/Blockchain-tutorial/how-does-Blockchain-work/
22. https://inzynierbudownictwa.pl/awarie-w-systemie-dystrybucji-wody-cz-i/
23. https://learn.g2.com/history-of-computers

24. https://learn.microsoft.com/en-us/azure/ARchitecture/data-guide/relational-data/data-warehousing
25. https://learn.microsoft.com/en-us/azure/ARchitecture/data-guide/relational-data/online-transaction-processing
26. https://learn.microsoft.com/en-us/*SQL*/relational-databases/in-memory-OLTP/survey-of-initial-areas-in-in-memory-OLTP?view=*SQL*-server-ver16
27. https://news.stanford.edu/news/2011/october/john-mccarthy-obit-102511.html
28. https://nomadeec.com/
29. https://onlim.com/en/using-chatbots-for-crisis-management-and-beyond-part-1/
30. https://predictivesolutions.pl/przeglad-klasycznych-modeli-rzetelnosci
31. https://pulpysoft.com/types-of-cloud-computing/
32. https://rcb.gov.pl/alert-rcb-w-nowej-odslonie/
33. https://regiony.tvp.pl/57671107/od-nowego-roku-alert-rcb-rowniez-na-publicznych-nosnikach
34. https://resilia.pl/blog/iso-22301-ciaglosc-dzialania-czym-jest-jakie-daje-korzysci/
35. https://samorzad.gov.pl/web/gmina-buczkowice/zarzadzanie-kryzysowe-zagrozenia
36. https://screennetwork.pl/alert-rcb-ekrany-reklamowe/
37. https://sjp.pwn.pl/sjp/zagro%C5%BCenie;2542384
38. https://soinso.uj.edu.pl/klasyfikacja-zagrozen
39. https://solutions.arcgis.com/emergency-management/situational-awareness-overview
40. https://solutions.arcgis.com/emergency-management/situational-awareness-overview/
41. https://spinlab.vu.nl/wp-content/uploads/2016/09/Review-of-emerging-technologies-for-crisis-management.pdf)
42. https://tele2IoT.com/ARticle/the-role-of-IoT-in-disaster-management-emergency-planning/
43. https://terytorialsi.wp.mil.pl/faq/struktura-i-zadania
44. https://u.group/thinking/sight-foresight-helping-first-responders-visualize-the-future-in-ar-with-spatial-data/
45. https://www.allerin.com/blog/big-data-in-disaster-management
46. https://www.allerin.com/blog/IoT-can-help-in-disaster-management-heres-how
47. https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html
48. https://www.benchmark.pl/aktualnosci/avast-konczy-wsparcie-dla-windows-xp-i-vista.html
49. https://www.bmc.com/blogs/bcp-business-continuity-planning/
50. https://www.britannica.com/technology/ARtificial-intelligence/Alan-Turing-and-the-beginning-of-AI
51. https://www.businesstechweekly.com/operational-efficiency/business-continuity/business-continuity-crisis-management/#What-is-Business-Continuity
52. https://www.connectpos.com/major-cloud-computing-advantages/
53. https://www.coolfiresolutions.com/blog/5-situational-awareness-technologies/
54. https://www.coolfiresolutions.com/blog/what-is-the-internet-of-things/
55. https://www.czk.pl/zk/index01.php

56. https://www.disaster-survival-resources.com/drought.html
57. https://www.duw.pl/czk/informatory-i-poradniki/poradniki/7106,Przygotowanie-na-wypadek-naglego-zdarzenia.html
58. https://www.facebook.com/crisisresponse/?source=crisis_bookmark
59. https://www.gislounge.com/
60. https://www.goodworklabs.com/big-data-for-disaster-management
61. https://www.gov.pl/attachment/4153fe60-a576-487f-96dd-2e863512e1d2
62. https://www.gov.pl/web/cyfryzacja/wazne-zmiany-w-prawie-telekomunikacyjnym1
63. https://www.gov.pl/web/kmpsp-jeleniagora/burze-zagrozenia-atmosferyczne
64. https://www.gov.pl/web/mswia/regionalny-system-ostrzegania
65. https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi
66. https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego
67. https://www.gov.pl/web/rcb/obieg-informacji-i-rola-rcb-w-systemie-zarzadzania-
68. https://www.helsebiblIoTeket.no/kvalitetsforbedring/metoder-og-verktoy/strategisk-analyse-swot-analyse
69. https://www.ibm.com/docs/pl/spss-statistics/SaaS?topic=analysis-factor-descriptives
70. https://www.internetofeverything.com/
71. https://www.investopedia.com/ask/answers/041415/what-are-some-common-functions-business-intelligence-technologies.asp
72. https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/zarzadzanie-strategiczne/analiza-swot/
73. https://www.javatpoint.com/big-data-characteristics
74. https://www.link4.pl/biuro-prasowe/aktualnosci-link4/alerty-pogodowe-od-link4-teraz-takze-dla-kierowcow
75. https://www.ltb.pl/digital-marketing-w-polsce-w-2020-roku/
76. https://www.motorolasolutions.com/en_us/about/company-overview/history/explore-motorola-heritage/cell-phone-development.html
77. https://www.mytechmag.com/IoT-in-disaster-management/
78. https://www.nik.gov.pl/aktualnosci/polska-nie-ma-skutecznego-systemu-ochrony-ludnosci.html
79. https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud
80. https://www.oknonet.pl/akcesoria/software_oprogramowanie_branzowe/news,26621,w,rfid-jako-wsparcie-dla-systemow-bezpieczenstwa.html
81. https://www.orange.pl/poradnik/siec-komorkowa/od-1g-do-5g-czyli-historia-technologii-mobilnej/
82. https://www.ore.edu.pl/2019/08/iii-edycja-kursu-alert-rcb/
83. https://www.prezydent.pl/download/gfx/prezydent/pl/defaultopisy/2467/4/1/demokracja.pdf
84. https://www.rfidjournal.com/that-internet-of-things-thing
85. https://www.scientificcooperation.com/products/PerSim-AugmentedRealityMedicalSimulation
86. https://www.simavi.ro/en/node/61
87. https://www.skybrary.aero/index.php/Situational_Awareness_(OGHFA_BN)
88. https://www.statista.com/statistics/982664/poland-most-popular-messaging-apps/
89. https://www.tandfonline.com/doi/full/10.1080/23276665.2020.1784769
90. https://www.techtarget.com/searchenterpriseai/definition/driverless-car

91. https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html
92. https://www.teldat.com.pl/oferta/produkty/systemy/96-c3is.html
93. https://www.teraz-srodowisko.pl/aktualnosci/wiekszosc-awarii-sieci-wodociagowych-ma-miejsce-przy-przylaczach-4827.html
94. https://www.thevintagenews.com/2018/01/06/wireless-phone/
95. https://www.ue.wroc.pl/pracownicy/455/obrona_cywilna.html
96. https://www.ushahidi.com/
97. https://www.zdnet.com/ARticle/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/
98. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/cloud-based-artificial-intelligence.html
99. https://zpe.gov.pl/a/ostrzeganie-i-alarmowanie/DwCxBQzIo

V. Inne źródła:

1. Badanie „Aktualne problemy i wydarzenia” (326) przeprowadzono metodą wywiadów bezpośrednich (face-to-face) wspomaganych komputerowo (CAPI) w dniach 29 czerwca – 6 lipca 2017 roku na liczącej 977 osób reprezentatywnej próbie losowej dorosłych mieszkańców Polski.
2. Baryłka A., Baryłka J., Okresowe kontrole jako ważny etap diagnostyki technicznej obiektów budowlanych, Referat na V Krajowej Konferencji Naukowo-Technicznej, ARCHBUD 2012 „Problemy współczesnej architektury i budownictwa”, Zakopane 2012.
3. Baryłka J.: Katastrofy budowlane -określenia i analiza zdarzeń. Referat na XII Konferencji Naukowo-Technicznej nt. Warsztat pracy rzeczoznawcy budowlanego. Kielce-Cedzyna, 16-18.05.2012 r.
4. Berliński L., *Wykłady i ćwiczenia z Zarządzania Strategicznego Politechnika Łódzka*, wydz. *Organizacji i Zarządzania*, *studia podyplomowe dla inżynierów*, sem. III i IV, 1998/1999 – dostęp na stronie (https://cire.pl/pliki/16/t_imiela_literatura_1.pdf).
5. Bezpieczeństwo ekologiczne Rzeczypospolitej Polskiej, http://adamkorcz.dl.interia.pl/.
6. Biuro Bezpieczeństwa i Zarządzania Kryzysowego: Awaria Techniczna. budowlanych. Referat na V Krajowej Konferencji Naukowo-Technicznej ARCHBUD 2012 „Problemy współczesnej architektury i budownictwa”, Zakopane, 3 – 6.09.2012 r
7. Plan Zarządzania Kryzysowego Powiatu Płockiego, Starostwo powiatowe w Płocku, Biuro spraw obronnych i zarzadzania kryzysowego, 2015.
8. Projekt Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej, Warszawa 2015, dostęp ma stronie https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf
9. Przygotowanie I Realizacja Policyjnego Zabezpieczenia Turnieju Finałowego Mistrzostw Europy W Piłce Nożnej Uefa Euro 2012 - https://kpk.policja.gov.pl/download/18/17418/Raport_UEFA_EURO_2012.pdf
10. Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Warszawa 2010
11. Sprawozdanie z realizacji przedsięwzięć EURO 2012 oraz z wykonanych działań dotyczących realizacji przygotowań Polski do finałowego turnieju Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 (styczeń–grudzień 2012 r.) - Dostęp na stronie:

https://bip.msit.gov.pl/download/2/3062/Sprawozdanie_EURO_2012-styczen_2013_r.pdf (data dostępu 23.01.2023)
12. Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2014, Warszawa 2014
13. The National Institute of Standards and Technology: www.nit.gov/itl/-cloud/index.cfm
14. Wypadki drogowe w Polsce w 2013 roku, raport Komendy Głównej Policji, Biuro prewencji i ruchu drogowego, Wydział Ruchu Drogowego, Warszawa 2014.
15. Zaktualizowana metodyka Wstępnej oceny ryzyka powodziowego, Warszawa 2018 r. dostęp na stronie: https://www.wody.gov.pl/WORP/zal_1_metodyka_04122018.pdf
16. Wymiana dobrych praktyk oraz analiza porównawcza aktów prawnych dla pracowników administracyjnych JST odpowiedzialnych za funkcjonowanie jednostek OSP pogranicza polsko-słowackiego (dostęp na stronie https://wsb.edu.pl/files/pages/3276/materialy_10_11_pl.pdf)

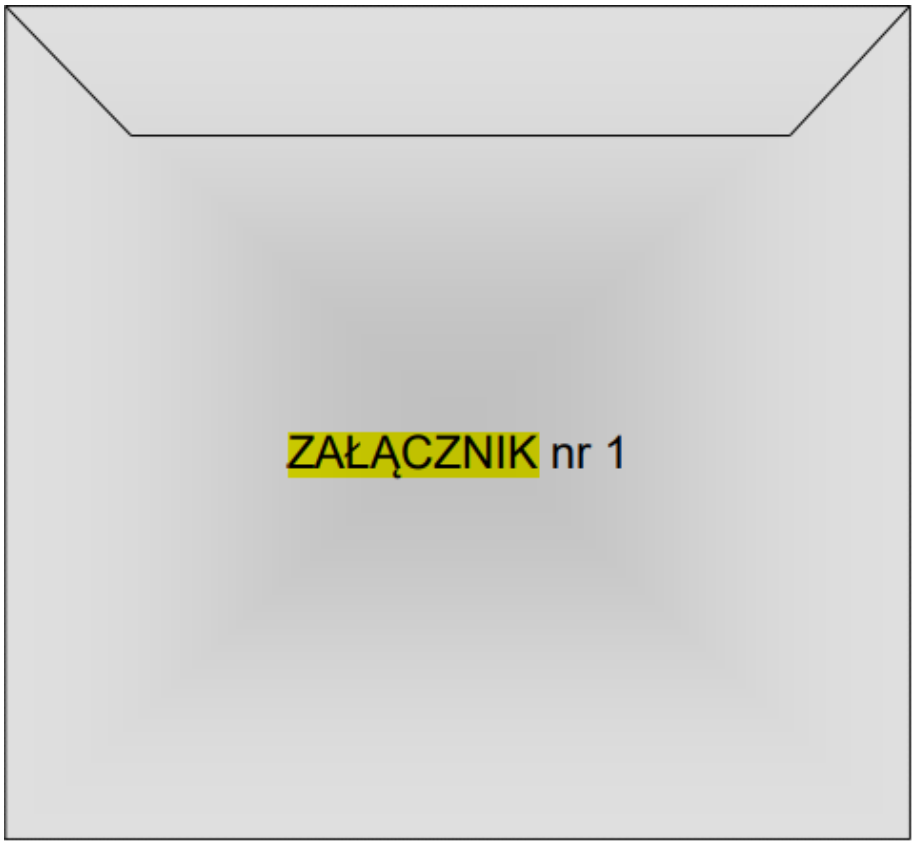
WYKAZ RYSUNKÓW

WYKAZ TABEL

WYKAZ WYKRESÓW

ZAŁĄCZNIKI

Załącznik nr1 – Płyta CD



Załącznik nr 2 - Ankieta skierowana do obywateli

Pytanie 1.

Proszę w skali 5 stopniowej ocenić stopień realizacji danego działania przez Pana/Panią:
(1 oznacza – bardzo niski stopień zgody, 2 – niski, 3- umiarkowany, 4- wysoki, 5 – bardzo wysoki stopień)

LP.		Ocena (1-5)
1.	Jestem w stanie rozpoznać zagrożenie na podstawie zmysłów (wzrok, słuch, węch)	
2.	Jestem w stanie rozpoznać zagrożenie takie jak powódź	
3.	Jestem świadomy podstawowych zagrożeń, jakie występują na terenie województwa, w którym mieszkam	
4.	Jestem w stanie na podstawie alertów RCB zaplanować odpowiednie kroki działania na wypadek wystąpienia zagrożenia	
5.	Jestem w stanie przewidzieć skutki wystąpienia zagrożenia	
6.	Jestem w stanie ocenić stopień zagrożenia na podstawie obserwacji	
7.	Jestem świadomy ryzyka jakie niesie ze sobą niestosowanie się do alertów RCB	
8.	Jestem świadomy tego, że odpowiednia reakcja na zagrożenie może uchronić mnie przed jego skutkami	
9.	Jestem świadomy tego, że podjęcie odpowiednich kroków w odpowiednim czasie może zniwelować skutki zagrożenia	
10.	Moja wiedza na temat zagrożeń kształtuje się na wysokim poziomie	
11.	Komunikaty wysyłane przez RCB są dla mnie zrozumiałe	
12.	Uważam, że dzięki poradnikom na temat zagrożeń jestem w stanie lepiej się do nich przygotować	
13.	Jestem w stanie zaplanować wszystkie niezbędne czynności jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi obce	
14.	Jestem w stanie zaplanować wszystkie niezbędne czynności jakie należy wykonać w przypadku wystąpienia zagrożenia, które jest mi znane	
15.	Jestem w stanie przygotować się do zagrożenia bez potrzeby otrzymywania komunikatów o nich	

Pytanie 2.

Proszę w skali 5-stopniowej ocenić stopień realizacji danego działania przez administrację publiczną: (1 oznacza – bardzo niski stopień zgody, 2 – niski, 3- umiarkowany, 4- wysoki, 5 – bardzo wysoki stopień)

		Ocena (1-5)
1.	Stworzyć większą liczbę etatów odpowiedzialnych za zarządzanie kryzysowe	
2.	Przeprowadzać coroczne szkolenia, ćwiczenia dla zespołów zarządzania kryzysowego	
3.	Przeprowadzać więcej zajęć w szkołach o tematyce zarządzania kryzysowego	
4.	Uświadamiać ludność w zakresie zagrożeń oraz ochrony przed nimi	
5.	Organizować konferencje i seminaria informacyjne	
6.	Zacieśnić współpracę między podmiotami zarządzania kryzysowego	
7.	Zmienić formę aktualnego sposobu informowania ludności o zagrożeniach	
8.	Zmodernizować aktualne alerty wysyłane przez Rządowe Centrum Bezpieczeństwa	
9.	Zwiększyć nacisk na poprawię świadomości ludności o zagrożeniach	
10.	Przygotować poradniki o zagrożeniach dla ludności	
11.	Wykorzystać nowoczesne technologie w celu zwiększenia poziomu bezpieczeństwa	
12.	Rozszerzyć tradycyjne środki informowania o zagrożeniach o współczesne technologie	
13.	Wykorzystać symulatory do modelowania scenariuszy zagrożeń	
14.	Udostępniać więcej informacji o zagrożeniach w mediach społecznościowych	
15.	Stworzyć audycje radiowo-telewizyjne o zagrożeniach w Polsce w celu zwiększenia świadomości o nich	
16.	Rozpowszechniać informacje o zagrożeniach w środkach transportu publicznego i prywatnego	
17.	Rozpowszechniać informację o zagrożeniach w miejscach publicznych	

Pytanie 3.

Proszę w skali 5-stopniowej ocenić stopień realizacji danego działania przez administrację publiczną: (1 oznacza – bardzo niski stopień zgody, 2 – niski, 3- umiarkowany, 4- wysoki, 5 – bardzo wysoki stopień)

		Ocena (1-5)
1.	Informowanie ludności o zagrożeniach odgrywa kluczową rolę w procesie kreowania świadomości o zaistniałych zagrożeniach	
2.	Niezwłoczne informowanie ludności w momencie ryzyka wystąpienia sytuacji kryzysowych może przyczynić się do zniwelowania jego skutków	
3.	Poinformowanie ludności o sposobie postępowania w trakcie wystąpienia zagrożenia może przyczynić się do optymalnego działania służb ratowniczych	
4.	Organizowanie spotkań mających na celu uświadomienie ludności o zagrożeniach może przyczynić się do zwiększenia świadomości o nich	
5.	Wdrożenie do systemu informowania ludności możliwości przesyłania informacji o zagrożeniach na współczesne urządzenia (smartfon, smartwatch komputery tablety itp.) w formie graficznej może przyczynić się do zwiększenia poziomu świadomości ludności	
6.	Zmiana formy komunikatów przesyłanych przez RCB na tekstowo-graficzne może przyczynić się do poprawy poziomu świadomości ludności	
7.	Wysyłanie przez RCB komunikatów o zagrożeniach oraz procedur postępowania w trakcie jego wystąpienia może przyczynić się do zmniejszenia jego skutków	
8.	Wykorzystanie mediów społecznościowych w procesie informowania ludności o zagrożeniach może zwiększyć poziom świadomości o nich	
9.	Wykorzystanie nowoczesnych technologii w środkach transportu publicznego może przyczynić się do zwiększenia poziomu świadomości o nich	
10.	Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do zmniejszenia czasu reakcji na wypadek wystąpienia zagrożenia	
11.	Wykorzystanie sztucznej inteligencji w aplikacjach związanych z informowaniem ludności o zagrożeniach może przyczynić się do uproszczenia procesu postępowania w trakcie zagrożenia	
12.	Wprowadzenie dla ludności szkoleń e-learningowych na temat zagrożeń może przyczynić się do poprawy ich świadomości o nich	
13.	Dostosowanie systemu informowania ludności do aktualnych rozwiązań techniczno- technologicznych może przyczynić się do poprawy świadomości o zagrożeniach	
14.	Zwiększenie poziomu świadomości ludności o zagrożeniach jest niezbędne do poprawy świadomości o nich	
15.	Utworzenie grup reagowania kryzysowego spośród mieszkańców może przyczynić się do poprawy świadomości o zagrożeniach	

Pytanie 4.

Jakie funkcje nowoczesnych technologii teleinformatycznych (ICT) Pana/Pani zdaniem mogą być najważniejsze w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów?

(proszę wybrać MAX 5 odpowiedzi) **Proszę również ocenić poziom użyteczności tych funkcji dla administracji w zakresie informowania ludności o zagrożeniach**

(1 oznacza – bardzo niski stopień, 2 – niski, 3 – umiarkowany, 4 – wysoki, 5 – bardzo wysoki stopień)

Lp.	**Wybór funkcji (MAX 5)**	**Stopień użyteczności (ocena 1-5)**
1.	Lokalizacja	
2.	Monitorowanie	
3.	Informowanie o zagrożeniach	
4.	Przesyłanie wiadomości o zagrożeniach	
5.	Odbieranie wiadomości o zagrożeniach	
6.	Dokumentowanie zagrożeń w formie elektronicznej	
7.	Zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania	
8.	Symulowanie zagrożeń	
9.	Tworzenie modeli statycznych modeli przyszłych zagrożeń na podstawie danych historycznych	
10.	Porównywanie zagrożeń	
11.	Prognozowanie przyszłych zagrożeń	
12.	Analizowanie obecnej sytuacji	
13.	Dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych	
14.	Przesyłanie podglądu na żywo z miejsca wystąpienia zagrożenia za pomocą urządzeń naziemnych	
15.	Wykorzystanie portali społecznościowych w celu zwiększenia poziomu świadomości o zagrożeniach	

Pytanie 5.
Jakie funkcje tradycyjnych form komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów?
(proszę wybrać MAX 5 odpowiedzi) **Proszę również ocenić poziom użyteczności tych funkcji dla administracji w zakresie informowania ludności o zagrożeniach**
(1 oznacza – bardzo niski stopień, 2 – niski, 3 – umiarkowany, 4 – wysoki, 5 – bardzo wysoki stopień)

Lp.	Wybór funkcji (MAX 5)	Stopień użyteczności (ocena 1-5)
1.	Wykorzystanie środków masowego przekazu w celu informowania o zagrożeniach	
2.	Wykorzystanie poradników w formie papierowej w celu zwiększenia poziomu informowania o zagrożeniach	
3.	Wykorzystanie tradycyjnych środków przekazu w celu informowania o zagrożeniach (telefon, list, telegram itp.)	
4.	Tworzenie papierowych map zagrożeń	
5.	Analiza map historycznych w celu identyfikacji zagrożenia	
6.	Analiza danych historycznych	
7.	Wykorzystanie radiofonii i telewizji w celu informowania o zagrożeniach	
8.	Wykorzystanie SMS w celu informowania o zagrożeniach	
9.	Wykorzystanie fizycznych (analogowych) urządzeń pomiarowych w celu oceny stanu zagrożenia	
10.	Dokumentowanie zagrożeń w formie papierowej	
11.	Wyszukiwanie informacji o zagrożeniach w Internecie	
12.	Ręczna analiza danych	
13.	Wyszukiwanie informacji o zagrożeniach w archiwach	
14.	Dostarczanie niezbędnych zasobów za pomocą pojazdów zmechanizowanych	
15.	Wykorzystanie megafonów w celu informowania o zagrożeniach (policja)	

Pytanie 6.
Jak ocenia Pan/Pani potencjalny wpływ poszczególnych technologii ICT na kształtowanie świadomości sytuacyjnej ludności w sytuacjach kryzysów i zagrożeń?
Proszę w skali 5- stopniowej ocenić poniższe technologie:
(1 oznacza – bardzo słaby wpływ, 2 – słaby, 3 – umiarkowany, 4 – silny, 5 – bardzo silny wpływ)

	Ocena (1-5)
Telefon komórkowy	
Telewizja	
Internet	
Telefon stacjonarny	
Smartwatch	
Media społecznościowe	
Komunikatory	
Radio	
Dron	
Tablet	
Megafon	
Syreny alarmowe	
E-mail	
Forum internetowe	
Inne ……	

\

Metryczka:
1. **PŁEĆ:** M; K
2. **WIEK:** do 25 lat; 26-35 lat; 36-50 lat; 51-65 lat; powyżej 65 lat
3. **WYKSZTAŁCENIE:** podstawowe, gimnazjalne, zasadnicze zawodowe, średnie, wyższe
4 **MIEJSCE ZAMIESZKANIA:** wieś, miasto liczące do 20 tys. mieszkańców, miasto liczące 21–50 tys. mieszkańców, miasto liczące powyżej 50 tys. Mieszkańców

Załącznik nr 3 - Ankieta skierowana do ZZK

Pytanie 1.

Które działania są Pana/Pani zdaniem najważniejsze w kontekście funkcjonowania systemu informowania ludności o zagrożeniach w momencie zaistnienia sytuacji kryzysowych? (proszę wybrać MAX 5 odpowiedzi)

		Wybór
1.	*Stworzyć większą liczbę etatów odpowiedzialnych za zarządzanie kryzysowe*	
2.	*Przeprowadzać coroczne szkolenia, ćwiczenia dla zespołów zarządzania kryzysowego*	
3.	*Przeprowadzać więcej zajęć w szkołach o tematyce zarządzania kryzysowego*	
4.	*Uświadamiać ludność w zakresie zagrożeń oraz ochrony przed nimi*	
5.	*Organizować konferencje i seminaria informacyjne*	
6.	*Zacieśnić współpracę między* podmiotami *zarządzania kryzysowego*	
7.	*Zmienić formę aktualnego sposobu informowania ludności o zagrożeniach*	
8.	*Zmodernizować aktualne alerty wysyłane przez Rządowe Centrum Bezpieczeństwa*	
9.	*Zwiększyć nacisk na poprawię świadomości ludności o zagrożeniach*	
10.	*Przygotować poradniki o zagrożeniach dla ludności*	
11.	*Wykorzystać nowoczesne technologie w celu zwiększenia poziomu bezpieczeństwa*	
12.	*Rozszerzyć tradycyjne środki informowania o zagrożeniach o współczesne technologie*	
13.	*Wykorzystać symulatory do modelowania scenariuszy zagrożeń*	
14.	*Udostępniać więcej informacji o zagrożeniach w mediach społecznościowych*	
15.	*Stworzyć audycje radiowo-telewizyjne o zagrożeniach w Polsce w celu zwiększenia świadomości o nich*	
16.	*Rozpowszechniać informacje o zagrożeniach w środkach transportu publicznego i prywatnego*	
17.	*Rozpowszechniać informację o zagrożeniach w miejscach publicznych*	

Pytanie 2.

Które działania są Pana/Pani zdaniem najważniejsze w kontekście funkcjonowania systemu informowania ludności na wypadek zaistnienia sytuacji kryzysowych/zagrożeń? (proszę wybrać MAX 5 odpowiedzi)

		Wybór
1.	Zapewnienie ciągłości działania systemu informowania ludności	
2.	Niezwłoczne informowanie ludności w momencie zaistnienia sytuacji kryzysowych	
3.	Utrzymanie stałego poziomu wydajności systemu informowania ludności	
4.	Organizowanie ćwiczeń w terenie	
5.	Zwiększenie wydajności systemu informowania ludności o zagrożeniach przy wykorzystaniu współczesnych technologii ICT	
6.	Zwiększenie wydajności komunikatów RCB poprzez wykorzystanie współczesnych technologii ICT	
7.	Udostępnianie informacji mających na celu zrozumienie istoty zagrożenia	
8.	Przekazywanie informacji ludności na temat postępowania w trakcie zagrożenia	
9.	Przygotowanie informacje ułatwiających postępowanie w celu przygotowania się do zagrożenia	
10.	Rozbudowa systemu informowania o formy graficzne	
11.	Wykorzystanie współczesnych technologii w systemach informowania ludności	
12.	Podnoszenie kwalifikacji zawodowych	
13.	Modernizacja obecnego systemu informowania ludności o zagrożeniach	
14.	Zwiększenie poziomu świadomości ludności o zagrożeniach	
15.	Organizowanie szkoleń dla grup społecznych w celu uświadamiania ich o zagrożeniach	

Pytanie 3.

Jakie funkcje nowoczesnych technologii teleinformatycznych (ICT) Pana/Pani zdaniem mogą być najważniejsze w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów? (proszę wybrać MAX 5 odpowiedzi)

		Wybór
1.	Lokalizacja	
2.	Monitorowanie	
3.	Informowanie o zagrożeniach	
4.	Przesyłanie wiadomości o zagrożeniach	
5.	Odbieranie wiadomości o zagrożeniach	
6.	Dokumentowanie zagrożeń w formie elektronicznej	
7.	Zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania	
8.	Symulowanie zagrożeń	
9.	Tworzenie modeli statycznych modeli przyszłych zagrożeń na podstawie danych historycznych	
10.	Porównywanie zagrożeń	
11.	Prognozowanie przyszłych zagrożeń	
12.	Analizowanie obecnej sytuacji	
13.	Dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych	
14.	Przesyłanie podglądu na żywo z miejsca wystąpienia zagrożenia za pomocą urządzeń naziemnych	
15.	Wykorzystanie portali społecznościowych w celu zwiększenia poziomu świadomości o zagrożeniach	

Pytanie 4.

Jakie funkcje tradycyjnych form komunikowania Pana/Pani zdaniem mogą być najważniejsze w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów? (proszę wybrać MAX 5 odpowiedzi)

		Wybór
1.	Telefon komórkowy	
2.	Telewizja	
3.	Internet	
4.	Telefon stacjonarny	
5.	Smartwatch	
6.	Media społecznościowe	
7.	Komunikatory	
8.	Radio	
9.	Dron	
10.	Tablet	
11.	Megafon	
12.	Syreny alarmowe	
13.	E-mail	
14.	Forum internetowe	

Pytanie 5.

Jak ocenia Pan/Pani poniższe stwierdzenia? (1 oznacza – zdecydowanie się nie zgadzam, 2 – raczej się nie zgadzam, 3 – umiarkowanie się zgadzam, 4 – raczej się zgadzam, 5 – zdecydowanie się zgadzam)

		Ocena (1-5)
1.	Nowoczesne technologie ICT mogą być ważnym dopełnieniem dla tradycyjnych rozwiązań stosowanych w zakresie kształtowania świadomości sytuacyjnej ludności	
2.	Wykorzystanie nowoczesnych technologii ICT w systemach informowania ludności może istotnie poprawiać poziom świadomości sytuacyjnej ludności.	
3.	Współczesne technologie ICT nie są w stanie w pełni zastąpić tradycyjnych środków komunikowania w kreowaniu świadomości sytuacyjnej ludności	
4.	Nowoczesne technologie są w stanie zapewnić odpowiedni poziom ciągłości działania w procesie kreowania świadomości sytuacyjnej.	
5.	Nowoczesne technologie mogą wywierać dodatni wpływ na kształtowanie się poziomu świadomości sytuacyjnej	
6.	Wykorzystanie nowoczesnych technologii w szkoleniach służb ratowniczych może poprawić ich poziom świadomości o zagrożeniach	
7.	Wykorzystanie nowoczesnych technologii ICT do monitorowania i zobrazowania zagrożeń może przyczynić się do zwiększenia świadomości sytuacyjnej zespołów zarządzania kryzysowego.	
8.	W celu zapewnienia ciągłości działania akcji ratunkowej niezbędne jest wykorzystanie nowoczesnych technologii	

Metryczka:

1. **PŁEĆ:** M; K
2. **WIEK:** do 25 lat; 26-35 lat; 36-50 lat; 51-65 lat; powyżej 65 lat
3. **WYKSZTAŁCENIE – poziom**: podstawowe; średnie; wyższe
4. **WYKSZTAŁCENIE – kierunek:** nauki ścisłe/techniczne; nauki społeczne; inne-jakie?
5. **STAŻ PRACY W JEDNOSTCE ORGANIZACYJNEJ:** do 5 lat; 5-15 lat; 15-25 lat; powyżej 25 lat
6. **ZAJMOWANE STANOWISKO:** kierownicze; techniczne; analityk; administracja; inne-jakie?
7. **KOMÓRKA ORGANIZACYJNA/sekcja/wydział (*opcjonalnie*):**

……

Załącznik 4 - Szczegółowe wyniki badań

Hipoteza [H.1] Świadomość sytuacyjna ludności w warunkach zagrożeń i kryzysów kształtuje się na niskim poziomie

Tabela 3.7. Statystyki rzetelności

Alfa Cronbacha	Liczba pozycji
0,939	15

Źródło: opracowanie własne

Tabela 3.8. Testy Kaisera-Mayera-Olkina i Bartletta – tworzenie wskaźnika kompozytowego

Miara KMO adekwatności doboru próby.		0,926
Test sferyczności Bartletta	Przybliżone chi-kwadrat	1012,881
	df	105
	Istotność	0,000

Źródło: opracowanie własne

Tabela 3.9. Całkowita wyjaśniona wariancja

Składowa	Początkowe wartości własne			Sumy kwadratów ładunków po wyodrębnieniu		
	Ogółem	% wariancji	% skumulowany	Ogółem	% wariancji	% skumulowany
1	8,140	54,263	54,263	8,140	54,263	54,263
Metoda wyodrębniania czynników – głównych składowych.						

Źródło: opracowanie własne

Hipoteza [H.2] Złożoność systemu informowania ludności o zagrożeniach w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występu-je ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej ludności, a złożonością informowania ludności o zagrożeniach w warunkach zagrożeń i kryzysów

Tabela 4.8. Całkowita wyjaśniona wariancja

Składowa	Początkowe wartości własne			Sumy kwadratów ładunków po wyodrębnieniu		
	Ogółem	% wariancji	% skumulowany	Ogółem	% wariancji	% skumulowany
1	10.134	59.611	59.611	10.134	59.611	59.611
Metoda wyodrębniania czynników – głównych składowych.						

Źródło: opracowanie własne

Tabela 4.9. Statystyki rzetelności

Alfa Cronbacha	Liczba pozycji
0,957	17

Źródło: opracowanie własne

Tabela 4.10. Testy Kaisera-Mayera-Olkina i Bartletta – tworzenie wskaźnika kompozytowego

Miara KMO adekwatności doboru próby.		0,942
Test sferyczności Bartletta	Przybliżone chi-kwadrat	1401,704
	df	136
	Istotność	0,000

Źródło: opracowanie własne

Tabela 4.11. Korelacja rho Spearmana pomiędzy wskaźnikami kompozytowymi ZSIL i PŚSL

			ZSIL	PŚSL
rho Spearmana	ZSIL	Współczynnik korelacji	1,000	0,614**
		Istotność (dwustronna)	.	0,000
		N	112	112
	PŚSL	Współczynnik korelacji	0,614**	1,000
		Istotność (dwustronna)	0,000	.
		N	112	112
**. Korelacja istotna na poziomie 0.01 (dwustronnie).				

Źródło: opracowanie własne

Hipoteza [H.3] Wydajność systemu informowania ludności w momencie zaistnienia sytuacji kryzysowych jest zbyt niska oraz występuje ujemna korelacja pomiędzy poziomem świadomości sytuacyjnej a wydajnością systemu informowania ludności w warunkach zagrożeń i kryzysów

Tabela 4.12. Całkowita wyjaśniona wariancja

	Początkowe wartości własne			Sumy kwadratów ładunków po wyodrębnieniu		
Składowa	Ogółem	% wariancji	% skumulowany	Ogółem	% wariancji	% skumulowany
1	8.094	53.963	53.963	8.094	53.963	53.963
Metoda wyodrębniania czynników – głównych składowych.						

Źródło: opracowanie własne

Tabela 4.13. Statystyki rzetelności

Alfa Cronbacha	Liczba pozycji
0,939	15

Źródło: opracowanie własne

Tabela 4.14. Testy Kaisera-Mayera-Olkina i Bartletta – tworzenie wskaźnika kompozytowego

Miara KMO adekwatności doboru próby.		0,906
Test sferyczności Bartletta	Przybliżone chi-kwadrat	1011,866
	df	105
	Istotność	0,000

Źródło: opracowanie własne

Tabela 4.15. Korelacja rho Spearmana pomiędzy wskaźnikami kompozytowymi ZSIL i PŚSL

			WSIL	PŚSL
rho Spearmana	WSIL	Współczynnik korelacji	1,000	0,621**
		Istotność (dwustronna)	.	0,000
		N	112	112
	PŚSL	Współczynnik korelacji	0,621**	1,000
		Istotność (dwustronna)	0,000	.
		N	112	112
**. Korelacja istotna na poziomie 0.01 (dwustronnie).				

Źródło: opracowanie własne

Hipoteza [H.4] Nowoczesne technologie teleinformatyczne (ICT) są w pełni przydatne i mogą stanowić alternatywny dla tradycyjnych środków, wydajny sposób komunikowania w kształtowaniu pożądanego poziomu świadomości sytuacyjnej ludności w warunkach zagrożeń i kryzysów.

Tabela 4.16. Korelacja rho-Spearmana (pomiędzy średnią użytecznością ICT w procesie informowania ludności oraz PŚSL

		PŚSL	
Lokalizacja	Współczynnik korelacji	0,501**	1,000
	Istotność (dwustronna)	.000	.
	N	50	50
Monitorowanie	Współczynnik korelacji	0,405**	0,619**
	Istotność (dwustronna)	0,002	0,001
	N	54	25
Informowanie o zagrożeniach	Współczynnik korelacji	0,320*	0,640**
	Istotność (dwustronna)	0,013	0,000
	N	60	27
Przesyłanie wiadomości o zagrożeniach	Współczynnik korelacji	0,327*	0,501**
	Istotność (dwustronna)	0,012	0,007
	N	58	28
Odbieranie wiadomości o zagrożeniach	Współczynnik korelacji	0,213	0,315
	Istotność (dwustronna)	0,182	0,253
	N	41	15
Dokumentowanie zagrożeń w formie elektronicznej	Współczynnik korelacji	0,333	-0,008
	Istotność (dwustronna)	0,164	0,986
	N	19	8
Zobrazowanie zagrożeń za pomocą specjalistycznego oprogramowania	Współczynnik korelacji	0,196	0,730
	Istotność (dwustronna)	0,383	0,099
	N	22	6
Symulowanie zagrożeń	Współczynnik korelacji	0,203	0,456
	Istotność (dwustronna)	0,236	0,158
	N	36	11
Tworzenie modeli statycznych modeli przyszłych zagrożeń na podstawie danych historycznych	Współczynnik korelacji	0,000	-0,500
	Istotność (dwustronna)	1,000	0,667
	N	7	3
Porównywanie zagrożeń	Współczynnik korelacji	-0,049	-0,211
	Istotność (dwustronna)	0,833	0,688
	N	21	6
Prognozowanie przyszłych zagrożeń	Współczynnik korelacji	0,248	0,568*
	Istotność (dwustronna)	0,179	0,027
	N	31	15
Analizowanie obecnej sytuacji	Współczynnik korelacji	0,384*	0,177
	Istotność (dwustronna)	0,025	0,562
	N	34	13
Dostarczanie niezbędnych zasobów za pomocą urządzeń naziemnych	Współczynnik korelacji	0,477	-1.000**
	Istotność (dwustronna)	0,232	.
	N	8	2
Przesyłanie podglądu na żywo z miejsca wystąpienia zagrożenia za pomocą urządzeń naziemnych	Współczynnik korelacji	0,139	0,162
	Istotność (dwustronna)	0,609	0,729
	N	16	7
Wykorzystanie portali społecznościowych w celu zwiększenia poziomu świadomości o zagrożeniach	Współczynnik korelacji	0,279	0,342
	Istotność (dwustronna)	0,247	0,408
	N	19	8
Korelacja istotna na poziomie 0.01 (dwustronnie). **			
Korelacja istotna na poziomie 0.05 (dwustronnie). *			

Źródło: opracowanie własne

W tabeli 4.16 przedstawiona została Korelacja rho-Spearmana (pomiędzy średnią użytecznością ICT w procesie informowania ludności oraz PŚSL. Kolorem zielonym zaznaczono korelację istotną na (dwustronnie) na poziomie 0.05, kolorem niebieskim zaznaczono korelacje istotną (dwustronnie) na poziomie 0.01.

Tabela 4.17. Korelacja rho-Spearmana (pomiędzy średnią użytecznością ICT w informowaniu ludności oraz PŚSL

		PŚSL	
Telefon komórkowy	Współczynnik korelacji	0,435**	1,000
	Istotność (dwustronna)	0,000	.
Telewizja	Współczynnik korelacji	0,346**	0,469**
	Istotność (dwustronna)	0,000	.000
Internet	Współczynnik korelacji	0,440**	0,544**
	Istotność (dwustronna)	0,000	0,000
Telefon stacjonarny	Współczynnik korelacji	-0,166	-0,137
	Istotność (dwustronna)	0,080	0,150
Smartwatch	Współczynnik korelacji	0,123	0,078
	Istotność (dwustronna)	0,197	0,411
Media społecznościowe	Współczynnik korelacji	0,252**	0,308**
	Istotność (dwustronna)	0,007	0,001
Komunikatory	Współczynnik korelacji	0,335**	0,306**
	Istotność (dwustronna)	0,000	v001
Radio	Współczynnik korelacji	0,309**	0,271**
	Istotność (dwustronna)	0,001	0,004
Dron	Współczynnik korelacji	0,189*	0,034
	Istotność (dwustronna)	0,046	0,724
Tablet	Współczynnik korelacji	0,260**	0,176
	Istotność (dwustronna)	0,006	.064
Megafon	Współczynnik korelacji	0,234*	0,248**
	Istotność (dwustronna)	0,013	0,008
Syreny alarmowe	Współczynnik korelacji	0,457**	0,464**
	Istotność (dwustronna)	0,000	0,000
E-mail	Współczynnik korelacji	0,153	0,099
	Istotność (dwustronna)	0,106	0,297
Forum internetowe	Współczynnik korelacji	0,140	0,124
	Istotność (dwustronna)	0,141	0,192
Inne	Współczynnik korelacji	0,053	0,073
	Istotność (dwustronna)	0,579	0,447
Korelacja istotna na poziomie 0.01 (dwustronnie). **			
Korelacja istotna na poziomie 0.05 (dwustronnie). *			

Źródło: opracowanie własne

W tabeli 4.17 przedstawiona została Korelacja rho-Spearmana (pomiędzy średnią użytecznością ICT w procesie informowania ludności oraz PŚSL. Kolorem zielonym zaznaczono korelację istotną na (dwustronnie) na poziomie 0.05, kolorem niebieskim zaznaczono korelacje istotną (dwustronnie) na poziomie 0.01.

Hipoteza [H.5] Pomiędzy wykorzystaniem nowoczesnych technologii teleinformatycznych (ICT) w systemach informowania ludności, a poziomem świadomości sytuacyjnej ludności występuje silna dodatnia korelacja

Tabela 4.18. Statystyki rzetelności

Alfa Cronbacha	Liczba pozycji
0,854	14

Źródło: opracowanie własne

Tabela 4.19. Testy Kaisera-Mayera-Olkina i Bartletta – tworzenie wskaźnika kompozytowego

Testy Kaisera-Mayera-Olkina i Bartletta		
Miara KMO adekwatności doboru próby.		0,819
Test sferyczności Bartletta	Przybliżone chi-kwadrat	598,195
	df	91
	Istotność	0,000

Źródło: opracowanie własne

Załącznik nr 5 - Analiza SWOT/TOWS – tabele

SWOT/TOWS - INTERNET RZECZY (IoT)

Tabela 5.26. Czy mocne strony IoT mogą wykorzystać szanse?

Mocne strony / Szanse	Zwiększenie poziomu świadomości sytuacyjnej na temat zagrożeń	Przyśpieszenie czasu reakcji na zagrożenia	Możliwość monitorowania zagrożeń z dowolnego miejsca bez potrzeby narażania ludzi na zagrożenia	Usprawnienie procesu reagowania na zagrożenia	Usprawnienie działań służb ratowniczych	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Monitorowanie zagrożeń i aktualnego stanu	1	1	1	1	1	1	5	30	5
Udostępnianie informacji	1	1	1	1	1	1	5	30	5
Pobieranie danych	1	1	1	1	1	1	5	30	5
Wykrywanie zagrożeń i otrzymywanie alertów	1	1	1	1	1	1	5	30	5
Monitoring niezbędnych zasobów	0	1	1	1	1	1	5	25	4
Identyfikacja zagrożeń	1	1	1	1	1	1	5	30	5
Poszukiwanie poszkodowanych	0	0	1	0	1	1	5	15	2
Sprawdzanie statusu siec np. energetycznej	0	0	1	1	1	1	5	20	3
Sprawdzanie parametrów życiowych	0	0	0	0	1	1	5	10	1
Wysyłanie alertów	0	1	1	1	1	1	5	25	4
Odbieranie alertów	1	1	1	1	1	1	5	30	5
Wysyłanie komunikatów	0	1	1	1	1	1	5	25	4
Odbieranie komunikatów	1	1	1	1	1	1	5	30	5
Możliwość oszacowania prędkości rozprzestrzeniania się zagrożenia	1	1	0	1	1	1	5	25	4
Zmniejszenie emisji dwutlenku węgla, a tym samym pomoc w ochronie środowiska	0	0	0	0	0	0	5	0	1
Łatwość użycia	1	1	1	1	1	1	5	30	5
WAGA	5	5	5	5	5	5	**Suma interakcji**		770
Iloczyn wag i interakcji	45	60	65	65	75	75	**77**		
RANGA	2	3	4	4	5	5	Suma iloczynów		

Źródło opracowanie własne

Tabela 5.27. Czy mocne strony IoT przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	Utrata funkcjonalności na skutek awarii sieci elektrycznej	Utrata funkcjonalności na skutek awarii sieci komputerowej (Internet)	Podatność na cyberataki	Fałszywe powiadomienia (na skutek czynników pogodowych)	Luki w oprogramowaniu układowym	Koszt urządzeń	WAGA	Iloczyn wag i interakcji	Ranga
Monitorowanie zagrożeń i aktualnego stanu	0	0	0	0	0	1	5	5	4
Udostępnianie informacji	0	0	0	0	0	1	5	5	4
Pobieranie danych	0	0	0	0	0	1	5	5	4
Wykrywanie zagrożeń i otrzymywanie alertów	0	0	0	0	1	1	5	10	5
Monitoring niezbędnych zasobów	0	0	0	0	0	1	5	5	4
Identyfikacja zagrożeń	0	0	0	0	0	1	5	5	4
Poszukiwanie poszkodowanych	0	0	0	0	0	0	5	0	3
Sprawdzanie statusu siec np. energetycznej	1	1	0	0	0	0	5	10	4
Sprawdzanie parametrów życiowych	0	0	0	0	0	0	5	0	3
Wysyłanie alertów	0	0	0	0	0	0	5	0	3
Odbieranie alertów	0	0	0	0	0	0	5	0	3
Wysyłanie komunikatów	0	0	0	0	0	0	5	0	3
Odbieranie komunikatów	0	0	0	0	0	0	5	0	3
Możliwość oszacowania prędkości rozprzestrzeniania się zagrożenia	0	0	0	0	0	0	5	0	3
Zmniejszenie emisji dwutlenku węgla, a tym samym pomoc w ochronie środowiska	0	0	0	0	0	0	5	0	3
Łatwość użycia	0	0	0	0	0	0	5	0	3
WAGA	5	5	3	4	4	3	**Suma interakcji 9**		77
Iloczyn wag i interakcji	5	5	0	0	4	18			
RANGA	4	4	2	2	3	5	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.28. Czy słaba strona IoT ogranicza wykorzystanie szansy?

Słabe strony / szanse	Zwiększenie poziomu świadomości sytuacyjnej na temat zagrożeń	Przyśpieszenie czasu reakcji na zagrożenia	Możliwość monitorowania zagrożeń z dowolnego miejsca bez potrzeby narażania ludzi na zagrożenia	Usprawnienie procesu reagowania na zagrożenia	Usprawnienie działań służb ratowniczych	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Nieznajomość technologii	0	0	0	0	0	0	3	0	1
Ograniczenia czasowe	0	0	1	1	1	1	5	20	5
Koszt wdrożenia	0	1	1	1	1	1	3	15	4
Brak przeszkolonego personelu	0	0	0	0	0	1	3	3	2
Zależność od instalacji elektrycznej	0	0	0	0	0	0	5	0	1
Zależność od sieci komputerowej (Internet)	0	0	0	0	0	1	5	5	3
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	0	0	0	0	0	0	5	0	2
Bezpieczeństwo urządzeń	1	1	1	0	1	1	4	20	5
WAGA	5	5	5	5	5	5	**Suma interakcji 16**		143
Iloczyn wag i interakcji	5	10	15	10	15	25			
RANGA	2	3	4	3	4	5	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.29. Czy słaba strona IoT może mieć wpływ zagrożenia?

Słabe strony / Zagrożenia	Utrata funkcjonalności na skutek awarii sieci elektrycznej	Utrata funkcjonalności na skutek awarii sieci komputerowej (Internet)	Podatność na cyberataki	Fałszywe powiadomienia (na skutek czynników pogodowych)	Luki w oprogramowaniu układowym	Koszt urządzeń	WAGA	Iloczyn wag i interakcji	Ranga
Nieznajomość technologii	0	0	1	1	0	0	3	6	1
Ograniczenia czasowe	0	0	0	0	0	0	5	0	1
Koszt wdrożenia	0	0	1	0	0	1	3	6	1
Brak przeszkolonego personelu	1	1	1	1	0	0	3	12	4
Zależność od instalacji elektrycznej	1	1	0	0	0	0	5	10	3
Zależność od sieci komputerowej (Internet)	1	1	1	0	0	0	5	15	5
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	0	0	1	0	0	1	5	10	3
Bezpieczeństwo urządzeń	0	0	1	0	0	1	4	8	2
WAGA	5	5	3	4	4	3	**Suma interakcji 17**		132
Iloczyn wag i interakcji	15	15	18	8	0	9			
RANGA	4	4	5	2	1	3	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.30. Czy szanse IoT wpływają na mocne strony?

Szanse / Mocne strony	Monitorowanie zagrożeń i aktualnego stanu	Udostępnianie informacji	Pobieranie danych	Wykrywanie zagrożeń i otrzymywanie alertów	Monitoring niezbędnych zasobów	Identyfikacja zagrożeń	Poszukiwanie poszkodowanych	Sprawdzanie statusu siec np. energetycznej	Sprawdzanie parametrów życiowych	Wysyłanie alertów	Odbieranie alertów	Wysyłanie komunikatów	Odbieranie komunikatów	Możliwość oszacowania prędkości rozprzestrzeniania się zagrożenia	Zmniejszenie emisji dwutlenku węgla, a tym samym pomoc w ochronie środowiska	Łatwość użycia	WAGA	Iloczyn wag i interakcji	Ranga
Zwiększenie poziomu świadomości sytuacyjnej na temat zagrożeń	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
Przyśpieszenie czasu reakcji na zagrożenia	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
Możliwość monitorowania zagrożeń z dowolnego miejsca bez potrzeby narażania ludzi na zagrożenia	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
Usprawnienie procesu reagowania na zagrożenia	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
Usprawnienie działań służb ratowniczych	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	5	80	5
WAGA	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	**Suma interakcji 96**		960
Iloczyn wag i interakcji	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30			
RANGA	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.31. Czy zagrożenia IoT wpływają na mocne strony?

Zagrożenia / Mocne strony	Monitorowanie zagrożeń i aktualnego stanu	Udostępnianie informacji	Pobieranie danych	Wykrywanie zagrożeń i otrzymywanie alertów	Monitoring niezbędnych zasobów	Identyfikacja zagrożeń	Poszukiwanie poszkodowanych	Sprawdzanie statusu siec np. energetycznej	Sprawdzanie parametrów życiowych	Wysyłanie alertów	Odbieranie alertów	Wysyłanie komunikatów	Odbieranie komunikatów	Możliwość oszacowania prędkości rozprzestrzeniania się zagrożenia	Zmniejszenie emisji dwutlenku węgla, a tym samym pomoc w ochronie środowiska	Łatwość użycia	WAGA	Iloczyn wag i interakcji	Ranga
Utrata funkcjonalności na skutek awarii sieci elektrycznej	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	5
Utrata funkcjonalności na skutek awarii sieci komputerowej (Internet)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	5
Podatność na cyberataki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	5
Fałszywe powiadomienia (na skutek czynników pogodowych)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	5
Luki w oprogramowaniu układowym	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	5
Koszt urządzeń	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	5
WAGA	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	**Suma interakcji 0**		0
Iloczyn wag i interakcji	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
RANGA	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.32. Czy szanse IoT wpływają na słabe strony?

Szanse / Słabe strony	Nieznajomość technologii	Ograniczenia czasowe	Koszt wdrożenia	Brak przeszkolonego personelu	Zależność od instalacji elektrycznej	Zależność od sieci komputerowej (Internet)	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	Bezpieczeństwo urządzeń	WAGA	Iloczyn wag i interakcji	Ranga
Zwiększenie poziomu świadomości sytuacyjnej na temat zagrożeń	0	1	0	1	0	0	0	0	5	10	3
Przyśpieszenie czasu reakcji na zagrożenia	1	1	0	1	0	0	0	0	5	15	4
Możliwość monitorowania zagrożeń z dowolnego miejsca bez potrzeby narażania ludzi na zagrożenia	1	0	0	1	0	0	0	0	5	10	3
Usprawnienie procesu reagowania na zagrożenia	1	0	0	1	0	0	0	0	5	10	3
Usprawnienie działań służb ratowniczych	1	0	0	1	0	0	0	0	5	10	3
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	0	1	1	1	1	1	0	5	30	5
WAGA	3	5	3	3	5	5	5	4	**Suma interakcji 17**		146
Iloczyn wag i interakcji	15	10	3	18	5	5	5	0			
RANGA	4	3	1	5	2	2	2	1	Suma iloczynów		

Źródło opracowanie własne.

Tabela 5.33. Czy zagrożenia IoT wpływają na słabe strony?

Zagrożenia / Słabe strony	Nieznajomość technologii	Ograniczenia czasowe	Koszt wdrożenia	Brak przeszkolonego personelu	Zależność od instalacji elektrycznej	Zależność od sieci komputerowej (Internet)	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	Bezpieczeństwo urządzeń	WAGA	Iloczyn wag i interakcji	Ranga
Utrata funkcjonalności na skutek awarii sieci elektrycznej	1	0	0	1	1	1	0	1	5	25	5
Utrata funkcjonalności na skutek awarii sieci komputerowej (Internet)	1	0	0	1	1	1	0	1	5	25	5
Podatność na cyberataki	1	0	0	1	0	1	0	1	3	12	4
Fałszywe powiadomienia (na skutek czynników pogodowych)	1	0	0	1	0	0	0	1	4	12	4
Luki w oprogramowaniu układowym	0	0	0	0	0	0	0	1	4	4	2
Koszt urządzeń	1	0	1	1	0	0	0	0	3	9	3
WAGA	3	5	3	3	5	5	5	4	**Suma interakcji 21**		165
Iloczyn wag i interakcji	15	0	3	15	10	15	0	20			
RANGA	4	1	2	4	3	4	1	5	Suma iloczynów		

Źródło: opracowanie własne

SWOT/TOWS - SZTUCZNA INTELIGENCJA

Tabela 5.34. Czy mocne strony sztucznej mogą wykorzystać szanse?

Mocne strony	Szanse	Usprawnienie działania służb ratowniczych	Możliwość przygotowania się na zagrożenia	Symulacje przyszłych zagrożeń	Usprawnienie procesu komunikacji (chatboty - źródło informacji o zagrożeniach)	Prowadzenie ćwiczeń i scenariuszy zagrożeń	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Robotyka akcje - akcje poszukiwawczo ratownicze		1	1	1	1	1	1	5	30	5
Wymiana informacji		1	1	1	1	1	1	5	30	5
Pobieranie danych		1	1	1	1	1	1	5	30	5
Symulowanie zagrożeń		1	1	1	1	1	1	5	30	5
Analiza zagrożeń na podstawie zebranych danych		1	1	1	1	1	1	5	30	5
Identyfikacja zagrożeń		1	1	1	1	1	1	5	30	5
Tworzenie chatbotów		1	1	1	1	1	1	5	30	5
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)		1	1	1	1	1	1	5	30	5
Komunikacja z dowolnego miejsca		1	0	1	1	1	1	5	25	4
Przetwarzanie danych		1	0	0	0	1	1	5	15	3
Generowanie scenariuszy zagrożeń		0	1	1	1	1	1	5	25	4
WAGA		5	5	5	5	5	5	**Suma interakcji 61**		61
Iloczyn wag i interakcji		50	45	50	50	55	55			
RANGA		4	3	4	4	5	5	Suma iloczynów		0

Źródło: opracowanie własne

Tabela 5.35. Czy mocne strony sztucznej inteligencji przeważają nad zagrożeniami?

Mocne strony	Zagrożenia	Utrata funkcjonalności niektórych urządzeń na skutek awarii sieci komputerowej (Internet)	Podatność na cyberataki	Luki w oprogramowaniu układowym	Bezpieczeństwo danych	WAGA	Iloczyn wag i interakcji	Ranga
Robotyka akcje - akcje poszukiwawczo ratownicze		0	1	1	0	5	10	5
Wymiana informacji		0	1	0	1	5	10	5
Pobieranie danych		0	1	0	1	5	10	5
Symulowanie zagrożeń		1	0	1	0	5	10	5
Analiza zagrożeń na podstawie zebranych danych		0	1	0	1	5	10	5
Identyfikacja zagrożeń		0	0	0	0	5	0	3
Tworzenie chatbotów		0	0	0	0	5	0	3
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)		0	1	0	1	5	10	5
Komunikacja z dowolnego miejsca		0	1	0	1	5	10	5
Oszacowanie możliwości wystąpienia zagrożenia		0	0	0	1	5	5	4
Przetwarzanie danych		0	1	0	1	5	10	5
Generowanie scenariuszy zagrożeń		1	0	0	0	5	5	4
WAGA		5	3	4	3	**Suma interakcji 18**		
Iloczyn wag i interakcji		10	21	8	21			
RANGA		4	5	3	5	Suma iloczynów		150

Źródło: opracowanie własne

Tabela 5.36. Czy słabe strony sztucznej inteligencji ograniczą wykorzystanie szansy?

Słabe strony / szanse	Usprawnienie działania służb ratowniczych	Możliwość przygotowania się na zagrożenia	Symulacje przyszłych zagrożeń	Usprawnienie procesu komunikacji (chatboty - źródło informacji o zagrożeniach)	Prowadzenie ćwiczeń i scenariuszy zagrożeń	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Nieznajomość technologii	1	1	1	1	1	1	3	18	3
Ograniczenia czasowe	1	1	1	1	1	1	5	30	5
Koszt wdrożenia	0	0	0	1	0	0	3	3	1
Brak przeszkolonego personelu	1	1	1	1	1	1	3	18	3
Zależność niektórych urządzeń od Internetu	0	0	0	0	0	1	5	5	2
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	0	0	1	1	1	1	5	20	4
WAGA	5	5	5	5	5	5	**Suma interakcji 24**		
Iloczyn wag i interakcji	15	15	20	25	20	25			
RANGA	3	3	4	5	4	5	Suma iloczynów		214

Źródło: opracowanie własne.

Tabela 5.37. Czy słabe strony sztucznej inteligencji mogą mieć wpływ na zagrożenia?

Słabe strony / Zagrożenia	Utrata funkcjonalności niektórych urządzeń na skutek awarii sieci komputerowej (Internet)	Podatność na cyberataki	Luki w oprogramowaniu układowym	Bezpieczeństwo danych	WAGA	Iloczyn wag i interakcji	Ranga
Nieznajomość technologii	1	1	1	1	3	12	5
Ograniczenia czasowe	0	0	0	0	5	0	2
Koszt wdrożenia	0	0	0	0	3	0	2
Brak przeszkolonego personelu	1	1	0	1	3	9	3
Zależność niektórych urządzeń od internetu	1	1	0	0	5	10	4
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	0	0	0	1	5	5	3
WAGA	5	3	4	3	**Suma interakcji 10**		
Iloczyn wag i interakcji	15	9	4	9			
RANGA	5	4	3	4	Suma iloczynów		73

Źródło: opracowanie własne

Tabela 5.38. Czy szanse wykorzystania sztucznej inteligencji wpływają na mocne strony?

Szanse	Mocne strony	Robotyka akcje - akcje poszukiwawczo ratownicze	Wymiana informacji	Pobieranie danych	Symulowanie zagrożeń	Analiza zagrożeń na podstawie zebranych danych	Identyfikacja zagrożeń	Tworzenie chatbotów	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	Komunikacja z dowolnego miejsca	Oszacowanie możliwości wystąpienia zagrożenia	Przetwarzanie danych	Generowanie scenariuszy zagrożeń	WAGA	Iloczyn wag i interakcji	Ranga
Usprawnienie działania służb ratowniczych		1	1	1	1	1	1	0	1	1	1	1	1	5	55	4
Możliwość przygotowania się na zagrożenia		1	1	1	1	1	1	1	1	1	1	1	1	5	60	5
Symulacje przyszłych zagrożeń		1	1	1	1	1	1	0	1	1	1	1	1	5	55	4
Usprawnienie procesu komunikacji (chatboty - źródło informacji o zagrożeniach)		1	1	1	1	1	1	1	1	1	1	1	1	5	60	5
Prowadzenie ćwiczeń i scenariuszy zagrożeń		1	1	1	1	1	1	1	1	1	1	1	1	5	60	5
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)		1	1	1	1	1	1	1	1	1	1	1	1	5	60	5
WAGA		5	5	5	5	5	5	5	5	5	5	5	5	**suma interakcji 70**		700
Iloczyn wag i interakcji		30	30	30	30	30	30	20	30	30	30	30	30			
RANGA		5	5	5	5	5	5	5	5	5	5	5	5	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.39. Czy zagrożenia sztucznej inteligencji wpływają na mocne strony?

Zagrożenia	Mocne strony	Robotyka akcje - akcje poszukiwawczo ratownicze	Wymiana informacji	Pobieranie danych	Symulowanie zagrożeń	Analiza zagrożeń na podstawie zebranych danych	Identyfikacja zagrożeń	Tworzenie chatbotów	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	Komunikacja z dowolnego miejsca	Oszacowanie możliwości wystąpienia zagrożenia	Przetwarzanie danych	Generowanie scenariuszy zagrożeń	WAGA	Iloczyn wag i interakcji	Ranga
Utrata funkcjonalności niektórych urządzeń na skutek awarii sieci komputerowej (Internet)		0	0	0	0	0	0	0	0	0	0	0	0	5	0	5
Podatność na cyberataki		0	0	0	0	0	0	0	0	0	0	0	0	3	0	5
Luki w oprogramowaniu układowym		0	0	0	0	0	0	0	0	0	0	0	0	4	0	5
Bezpieczeństwo danych		0	0	0	0	0	0	0	0	0	0	0	0	3	0	5
WAGA		5	5	5	5	5	5	5	5	5	5	5	5	**suma interakcji 0**		
Iloczyn wag i interakcji		0	0	0	0	0	0	0	0	0	0	0	0			
RANGA		5	5	5	5	5	5	5	5	5	5	5	5	Suma iloczynów		0

Źródło: Opracowanie własne

Tabela 5.40. Czy szanse wykorzystania sztucznej inteligencji wpływają na słabe strony?

Szanse / Słabe strony	Nieznajomość technologii	Ograniczenia czasowe	Koszt wdrożenia	Brak przeszkolonego personelu	Zależność niektórych urządzeń od internetu	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	WAGA	Iloczyn wag i interakcji	Ranga
Usprawnienie działania służb ratowniczych	1	1	0	1	0	0	5	15	4
Możliwość przygotowania się na zagrożenia	1	0	0	1	0	1	5	15	4
Symulacje przyszłych zagrożeń	1	1	0	1	0	1	5	20	5
Usprawnienie procesu komunikacji (chatboty - źródło informacji o zagrożeniach)	1	1	0	1	1	0	5	20	5
Prowadzenie ćwiczeń i scenariuszy zagrożeń	1	1	0	1	0	0	5	15	4
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	0	0	1	1	1	5	20	5
WAGA	3	5	3	3	5	5	**suma interakcji**		191
Iloczyn wag i interakcji	18	20	0	18	15	15	**21**		
RANGA	4	5	3	4	3	3	Suma iloczynów		

Źródło: opracowanie własne

Tabela 5.41. Czy zagrożenia sztucznej inteligencji wpływają na słabe strony?

Zagrożenia / Słabe strony	Nieznajomość technologii	Ograniczenia czasowe	Koszt wdrożenia	Brak przeszkolonego personelu	Zależność niektórych urządzeń od internetu	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	WAGA	Iloczyn wag i interakcji	Ranga
Utrata funkcjonalności niektórych urządzeń na skutek awarii sieci komputerowej (Internet)	1	0	0	1	1	1	5	20	5
Podatność na cyberataki	1	0	0	1	1	1	3	12	4
Luki w oprogramowaniu układowym	0	0	0	0	0	0	4	0	2
Bezpieczeństwo danych	1	0	0	1	0	1	3	9	3
WAGA	3	5	3	3	5	5	**suma interakcji**		
Iloczyn wag i interakcji	9	0	0	9	10	15	**11**		
RANGA	3	2	2	3	4	5	Suma iloczynów		84

Źródło: opracowanie własne

SWOT/TOWS - VIRTUAL REALITY I AUGMENTED REALITY

Tabela 5.42. Czy mocne strony VR/AR mogą wykorzystać szanse?

Mocne strony / Szanse	Usprawnienie działania służb ratowniczych	Możliwość przygotowania się na zagrożenia	Symulacje przyszłych zagrożeń	Usprawnienie procesu komunikacji	Prowadzenie ćwiczeń i scenariuszy zagrożeń - bez narażania życia i zdrowia	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Symulowanie realistycznych zagrożeń	1	1	1	1	1	1	5	30	5
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	1	1	1	1	1	1	5	30	5
Tworzenie realistycznych szkoleń dla służb ratowniczych	1	1	1	1	1	1	5	30	5
Wyświetlanie nazw ulic, śledzenie służb ratowniczych,	1	1	1	1	1	1	5	30	5
Komunikacja głosowa	1	1	1	1	1	1	5	30	5
Nanoszenie obrazów 3D na rzeczywiste środowisko	1	1	1	1	1	1	5	30	5
WAGA	5	5	5	5	5	5	**suma interakcji 36**		
Iloczyn wag i interakcji	30	30	30	30	30	30			
RANGA	5	5	5	5	5	5	suma iloczynów	360	

Źródło: opracowanie własne

Tabela 5.43. Czy mocne strony VR/AR przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	Zaburzenia błędnika, choroba lokomocyjna	Podatność na cyberataki i śledzenie	Uzależnienie od technologii	WAGA	Iloczyn wag i interakcji	Ranga
Symulowanie realistycznych zagrożeń	1	0	1	5	10	5
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	1	0	1	5	10	5
Tworzenie realistycznych szkoleń dla służb ratowniczych	1	0	1	5	10	5
Wyświetlanie nazw ulic, śledzenie służb ratowniczych,	0	1	0	5	5	4
Komunikacja głosowa	0	1	0	5	5	4
Nanoszenie obrazów 3D na rzeczywiste środowisko	0	1	0	5	5	4
WAGA	5	4	3	suma interakcji 9		
Iloczyn wag i interakcji	15	12	9			
RANGA	5	4	3	suma iloczynów		81

Źródło: opracowanie własne

Tabela 5.44. Czy słabe strony VR/AR ograniczą wykorzystanie szans?

słabe strony / szanse	Usprawnienie działania służb ratowniczych	Możliwość przygotowania się na zagrożenia	Symulacje przyszłych zagrożeń	Usprawnienie procesu komunikacji	Prowadzenie ćwiczeń i scenariuszy zagrożeń - bez narażania życia i zdrowia	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Koszt wdrożenia	0	0	0	0	0	0	3	0	3
Brak przeszkolonego personelu	1	1	1	1	1	1	3	18	4
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	1	1	1	1	1	1	5	30	5
Brak kontaktu z otoczeniem (*VR*)	0	0	0	0	0	0	1	0	2
WAGA	5	5	5	5	5	5	**suma interakcji 12**		
Iloczyn wag i interakcji	10	10	10	10	10	10			
RANGA	5	5	5	5	5	5	suma iloczynów	108	

Źródło: opracowanie własne

Tabela 5.45. Czy słabe strony VR/AR może mieć wpływ zagrożenia?

słabe strony / zagrożenia	Zaburzenia błędnika, choroba lokomocyjna	Podatność na cyberataki i śledzenie	Uzależnienie od technologii	WAGA	Iloczyn wag i interakcji	Ranga
Koszt wdrożenia	0	0	0	3	0	3
Brak przeszkolonego personelu	0	1	0	3	3	4
Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	0	1	0	5	5	5
Brak kontaktu z otoczeniem (*VR*)	0	0	0	1	0	3
WAGA	5	4	3	**suma interakcji 2**		
Iloczyn wag i interakcji	0	8	0			
RANGA	4	5	4	suma iloczynów		16

Źródło: opracowanie własne

Tabela 5.46. Czy szanse VR/AR wpływają na mocne strony?

Szanse / Mocne strony	Symulowanie realistycznych zagrożeń	Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	Tworzenie realistycznych szkoleń dla służb ratowniczych	Wyświetlanie nazw ulic, śledzenie służb ratowniczych,	Komunikacja głosowa	Nanoszenie obrazów 3D na rzeczywiste środowisko	WAGA	Iloczyn wag i interakcji	Ranga
Usprawnienie działania służb ratowniczych	1	1	1	1	1	1	5	30	5
Możliwość przygotowania się na zagrożenia	1	1	1	1	1	1	5	30	5
Symulacje przyszłych zagrożeń	1	1	1	1	1	1	5	30	5
Usprawnienie procesu komunikacji	1	1	1	1	1	1	5	30	5
Prowadzenie ćwiczeń i scenariuszy zagrożeń - bez narażania życia i zdrowia	1	1	1	1	1	1	5	30	5
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	1	1	1	1	1	5	30	5
WAGA	5	5	5	5	5	5	**suma interakcji 36**		360
Iloczyn wag i interakcji	30	30	30	30	30	30			
RANGA	5	5	5	5	5	5	suma iloczynów		

Źródło: opracowanie własne

Tabela 5.47. Czy zagrożenia VR/AR wpływają na mocne strony?

Zagrożenia / Mocne strony	Symulowanie realistycznych zagrożeń	Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	Tworzenie realistycznych szkoleń dla służb ratowniczych	Wyświetlanie nazw ulic, śledzenie służb ratowniczych,	Komunikacja głosowa	Nanoszenie obrazów 3D na rzeczywiste środowisko	WAGA	Iloczyn wag i interakcji	Ranga
Zaburzenia błędnika, choroba lokomocyjna	0	0	0	0	0	0	5	0	5
Podatność na cyberataki i śledzenie	0	0	0	0	0	0	4	0	5
Uzależnienie od technologii	0	0	0	0	0	0	3	0	5
WAGA	5	5	5	5	5	5	**suma interakcji** 0		
Iloczyn wag i interakcji	0	0	0	0	0	0			
RANGA	5	5	5	5	5	5	suma iloczynów		0

Źródło: opracowanie własne

Tabela 5.48. Czy szanse VR/AR wpływa na słabe strony?

Szanse / Słabe strony	Koszt wdrożenia	Brak przeszkolonego personelu	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	Brak kontaktu z otoczeniem (*VR*)	WAGA	Iloczyn wag i interakcji	Ranga
Usprawnienie działania służb ratowniczych	1	1	1	0	5	15	5
Możliwość przygotowania się na zagrożenia	0	1	1	0	5	10	4
Symulacje przyszłych zagrożeń	0	1	1	0	5	10	4
Usprawnienie procesu komunikacji	1	1	1	0	5	15	5
Prowadzenie ćwiczeń i scenariuszy zagrożeń - bez narażania życia i zdrowia	0	1	1	0	5	10	4
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	1	1	0	5	15	5
WAGA	3	3	5	1	**suma interakcji 15**		
Iloczyn wag i interakcji	9	18	30	0			
RANGA	3	4	5	3	suma iloczynów		132

Źródło: opracowanie własne

Tabela 5.49. Czy zagrożenia VR/AR wpływają na słabe strony?

Zagrożenia / Słabe strony	Koszt wdrożenia	Brak przeszkolonego personelu	Brak odpowiedniej infrastruktury do przetwarzania i gromadzenia danych	Brak kontaktu z otoczeniem (*VR*)	WAGA	Iloczyn wag i interakcji	Ranga
Zaburzenia błędnika, choroba lokomocyjna	0	0	0	1	5	5	4
Podatność na cyberataki i śledzenie	0	1	1	0	4	8	5
Uzależnienie od technologii	0	0	0	1	3	3	3
WAGA	5	5	5	5	**suma interakcji 4**		
Iloczyn wag i interakcji	0	5	5	10			
RANGA	3	4	4	5	suma iloczynów		36

Źródło: opracowanie własne

SWOT/TOWS - *CLOUD COMPUTING*

Tabela 5.50. Czy mocne strony Cloud Computing mogą wykorzystać szanse?

Mocne strony / Szanse	Duża ilość przechowywanych danych i dostępność zasobów	nieograniczona skalowalność	najnowsze technologie oraz oprogramowanie	Usprawnienie procesu komunikacji	zwiększenie efektywności działań	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
Niski koszt wdrożenia	1	0	1	1	1	1	4	20	3
Dostęp do zasobów za pośrednictwem Internetu	1	0	1	1	1	1	5	25	4
Komunikacja z dowolnego miejsca	1	0	1	1	1	1	5	25	4
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	1	1	1	1	1	1	5	30	5
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	1	1	1	1	1	1	5	30	5
Tworzenie kopii zapasowych	1	1	1	1	1	1	5	30	5
Oszczędność energii	1	0	0	0	1	1	5	15	2
Łatwe odzyskiwanie danych po awariach	1	0	0	0	1	0	5	10	1
Skalowalność i elastyczność	1	1	1	1	1	0	5	25	4
Opłata jedynie za wykorzystane zasoby	1	1	1	1	1	1	5	30	5
WAGA	5	5	4	5	5	5	**suma interakcji 49**		
Iloczyn wag i interakcji	50	25	32	40	50	40			
RANGA	5	2	3	4	5	4	suma iloczynów		477

Źródło: opracowanie własne

Tabela 5.51. Czy mocne strony Cloud Computing przeważają nad zagrozeniami?

Mocne strony / Zagrożenia	bezpieczeństwo danych	zależność od technologii	Uzależnienie od zewnętrznego dostawcy	ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych)	mała liczba dostawców	WAGA	Iloczyn wag i interakcji	Ranga
Niski koszt wdrożenia	0	0	0	0	0	4	0	4
Dostęp do zasobów za pośrednictwem Internetu	1	1	1	1	1	5	25	5
Komunikacja z dowolnego miejsca	1	1	1	1	1	5	25	5
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	1	1	1	1	1	5	25	5
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	1	1	1	1	1	5	25	5
Tworzenie kopii zapasowych	1	1	1	1	1	5	25	5
WAGA	5	4	3	4	3	**suma interakcji 25**		
Iloczyn wag i interakcji	25	20	15	20	15			
RANGA	5	4	2	4	2	suma iloczynów		185

Źródło: opracowanie własne.

Tabela 5.52. Czy słabe strony Cloud Computing ograniczą wykorzystanie szansy?

słabe strony / szanse	Duża ilość przechowywanych danych i dostępność zasobów	nieograniczona skalowalność	najnowsze technologie oraz oprogramowanie	Usprawnienie procesu komunikacji	zwiększenie efektywności działań	Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	WAGA	Iloczyn wag i interakcji	Ranga
awarie techniczne	1	0	0	1	1	1	3	12	1
wymagany dostęp do internetu	1	0	1	1	1	1	5	25	4
brak przeszkolonego personelu	1	0	0	1	1	1	3	12	1
zróżnicowany poziom bezpieczeństwa	1	0	1	0	0	1	3	9	1
zależność od dostawców usług	1	1	1	1	1	1	5	30	5
trudna integracja z aktualnymi rozwiązaniami	1	0	1	1	0	1	4	16	2
ograniczenia transferu danych	1	0	0	1	1	1	3	12	5
brak możliwości wyboru fizycznej lokalizacji danych	1	0	0	0	0	0	5	5	1
dostęp do wydajnego internetu	1	0	0	1	1	1	5	20	3
WAGA	5	5	4	5	5	5	**suma interakcji 35**		
Iloczyn wag i interakcji	45	5	16	35	30	40			
RANGA	5	1	1	3	2	4	suma iloczynów		441

Źródło: opracowanie własne.

Tabela 5.53. Czy słabe strony Cloud Computing mogą mieć wpływ zagrożenia?

słabe strony / zagrożenia	bezpieczeństwo danych	zależność od technologii	Uzależnienie od zewnętrznego dostawcy	ukryte koszty (archiwizacja danych, rozwiązywania problemów, odzyskiwania danych)	mała liczba dostawców	WAGA	Iloczyn wag i interakcji	Ranga
awarie techniczne	1	1	1	0	0	3	9	2
wymagany dostęp do internetu	1	1	1	1	1	5	25	5
brak przeszkolonego personelu	1	0	1	1	0	3	9	2
zróżnicowany poziom bezpieczeństwa	1	1	1	1	1	3	15	3
zależność od dostawców usług	1	1	1	1	1	5	25	5
trudna integracja z aktualnymi rozwiązaniami	1	1	1	1	0	4	16	4
ograniczenia transferu danych	0	1	1	1	0	3	9	5
brak możliwości wyboru fizycznej lokalizacji danych	1	0	1	0	1	5	15	3
dostęp do wydajnego internetu	0	1	1	1	0	5	15	3
WAGA	5	4	3	2	2	suma interakcji 34		
Iloczyn wag i interakcji	35	28	27	14	8			
RANGA	5	3	4	2	1	suma iloczynów		250

Źródło: opracowanie własne

Tabela 5.54. Czy szanse Cloud Computing wpływają na mocne strony?

Szanse / Mocne strony	Niski koszt wdrożenia	Dostęp do zasobów za pośrednictwem Internetu	Komunikacja z dowolnego miejsca	Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	Tworzenie kopii zapasowych	Oszczędność energii	Łatwe odzyskiwanie danych po awariach	skalowalność i elastyczność	opłata jedynie za wykorzystane zasoby	WAGA	Iloczyn wag i interakcji	Ranga
Duża ilość przechowywanych danych i dostępność zasobów	1	1	1	1	1	1	1	1	1	1	5	50	5
nieograniczona skalowalność	0	0	0	0	1	1	1	1	1	0	5	25	2
najnowsze technologie oraz oprogramowanie	1	1	1	1	1	1	1	1	1	1	4	40	3
Usprawnienie procesu komunikacji	0	1	1	1	1	1	1	1	1	1	5	45	4
zwiększenie efektywności działań	0	1	1	1	1	1	1	1	1	1	5	45	4
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)	1	1	1	1	1	1	1	1	1	1	5	50	5
WAGA	4	5	5	5	5	5	5	5	5	5	**suma interakcji** 53		
Iloczyn wag i interakcji	12	25	25	25	30	30	30	30	30	25			
RANGA	3	4	4	4	5	5	5	5	5	4	suma iloczynów		517

Źródło: opracowanie własne

Tabela 5.55. Czy zagrożenia Cloud Computing wpływają na mocne strony?

Zagrożenia / Mocne strony	Niski koszt wdrożenia	Dostęp do zasobów za pośrednictwem Internetu	Komunikacja z dowolnego miejsca	Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	Tworzenie kopii zapasowych	Oszczędność energii	Łatwe odzyskiwanie danych po awariach	skalowalność i elastyczność	opłata jedynie za wykorzystane zasoby	WAGA	Iloczyn wag i interakcji	Ranga
bezpieczeństwo danych	0	1	1	1	1	0	1	0	0	1	5	30	5
zależność od technologii	0	1	1	1	1	1	0	1	0	1	4	28	4
Uzależnienie od zewnętrznego dostawcy	0	1	1	1	1	1	0	1	1	1	3	24	3
WAGA	4	5	5	5	5	5	5	5	5	5	suma interakcji 21		
Iloczyn wag i interakcji	0	15	15	15	15	10	5	10	5	15			
RANGA	2	5	5	5	5	4	3	4	3	5	suma iloczynów		187

Źródło: opracowanie własne

Tabela 5.56. Czy szanse wykorzystania Cloud Computing wpływają na słabe strony?

Szanse	Słabe strony	awarie techniczne	wymagany dostęp do internetu	brak przeszkolonego personelu	zróżnicowany poziom bezpieczeństwa	zależność od dostawców usług	truda integracja z aktualnymi rozwiąza-niami	ograniczenia transferu danych	brak możliwości wyboru fizycznej loka-lizacji danych	WAGA	Iloczyn wag i interakcji	Ranga
Duża ilość przechowy-wanych danych i dostęp-ność zasobów		0	1	1	0	1	0	1	0	5	20	4
nieograniczona skalo-walność		0	1	1	0	1	1	0	0	5	20	4
najnowsze technologie oraz oprogramowanie		0	1	1	0	1	1	0	0	4	16	3
Usprawnienie procesu komunikacji		1	1	1	0	1	0	0	0	5	20	4
zwiększenie efektywności działań		1	1	1	0	1	1	0	0	5	25	5
Możliwość integracji z urządzeniami mobilnymi (telefon, tablet, komputer smartwatch)		1	1	1	0	1	0	0	0	5	20	4
WAGA		3	5	3	3	5	4	3	5	**suma interakcji 25**		
Iloczyn wag i interakcji		9	30	18	0	30	12	3	0			
RANGA		2	5	4	1	5	3	1	1	suma iloczynów		223

Źródło: opracowanie własne

Tabela 5.57. Czy zagrożenia Cloud Computing wpływają na słabe strony?

Zagrożenia	Słabe strony	awarie techniczne	wymagany dostęp do internetu	brak przeszkolonego personelu	zróżnicowany poziom bezpieczeń-stwa	zależność od dostawców usług	trudna integracja z aktualnymi rozwiązaniami	ograniczenia transferu danych	brak możliwości wyboru fizycznej lokalizacji danych	WAGA	Iloczyn wag i interakcji	Ranga
bezpieczeństwo danych		1	1	1	1	1	1	1	1	5	40	5
zależność od technologii		1	1	1	1	1	1	1	1	4	32	5
Uzależnienie od zewnętrzne-go dostawcy		1	1	1	1	1	1	1	1	3	24	3
ukryte koszty (archiwizacja danych, rozwiązywania pro-blemów, odzyskiwania da-nych)		1	1	1	1	1	1	1	1	2	16	2
mała liczba dostawców		0	0	0	1	1	1	1	1	2	10	1
WAGA		3	5	3	3	5	4	3	5	**suma interakcji 37**		
Iloczyn wag i interakcji		12	20	12	15	25	20	15	25			
RANGA		3	5	3	4	4	5	4	4	suma iloczynów		266

Źródło: opracowanie własne.

SWOT/TOWS - *BLOCKCHAIN*

Tabela 5.58. Czy mocne strony Blockchain mogą wykorzystać szanse?

Mocne strony	Szanse	usprawnienie zarządzania kryzysowego	zwiększenie świadomości sytuacyjnej na temat zagrożeń	najnowsze technologie oraz oprogramo-wanie	Zabezpieczenie danych	zwiększenie efektywności działań	WAGA	Iloczyn wag i interakcji	Ranga
Łatwość dostępu		1	1	1	1	1	4	20	4
Kontrola zasobów		1	1	1	1	1	5	25	5
Stanowi własność użytkownika		1	1	1	1	1	5	25	5
Szyfrowanie danych		1	1	1	1	1	5	25	5
Transakcje bez osób trzecich		1	1	1	1	1	5	25	5
Weryfikacja tożsamości		1	1	1	1	1	5	25	5
WAGA		5	5	4	5	5	**suma interakcji 30**		
Iloczyn wag i interakcji		30	30	24	30	30			
RANGA		5	5	4	5	5	suma iloczynów		289

Źródło: opracowanie własne

Tabela 5.59. Czy mocne strony Blockchain przeważają zagrożenia?

Mocne strony	Zagrożenia	utrata dostępu przy braku klucza prywatnego	brak dostępu do internetu czyni technologię bezużyteczną	podatność na ataki i kradzież da-nych	WAGA	Iloczyn wag i interakcji	Ranga
Łatwość dostępu		1	1	1	4	12	4
Kontrola zasobów		1	1	1	5	15	5
Stanowi własność użytkownika		1	1	1	5	15	5
Szyfrowanie danych		1	1	1	5	15	5
Transakcje bez osób trzecich		1	1	1	5	15	5
Weryfikacja tożsamości		1	1	1	5	15	5
WAGA		5	4	3	**suma interakcji 18**		
Iloczyn wag i interakcji		30	24	18			
RANGA		5	4	3	suma iloczynów		159

Źródło: opracowanie własne

Tabela 5.60. Czy słabe strony Blockchain ograniczą wykorzystanie szansy?

słabe strony / szanse	usprawnienie zarządzania kryzysowego	zwiększenie świadomości sytuacyjnej na temat zagrożeń	najnowsze technologie oraz oprogramowanie	Zabezpieczenie danych	zwiększenie efektywności działań	WAGA	Iloczyn wag i interakcji	Ranga
Brak wykwalifikowanych osób	1	1	1	1	1	3	15	3
Wysokie zużycie energii	1	0	1	1	1	5	20	5
Dostęp wyłącznie za pośrednictwem internetu	1	0	1	1	1	3	12	2
wymaga wysokowydajnościowego sprzętu	1	0	1	1	0	3	9	1
zależność od internetu	1	0	1	1	1	5	20	5
trudna integracja z innymi systemami	1	0	1	1	1	4	16	4
WAGA	5	5	4	5	5	**suma interakcji 24**		
Iloczyn wag i interakcji	30	5	24	30	25			
RANGA	5	2	3	5	4	suma iloczynów		206

Źródło: opracowanie własne

Tabela 5.61. Czy słabe strony Blockchain mogą mieć wpływ na zagrożenia?

słabe strony / zagrożenia	utrata dostępu przy braku klucza prywatnego	brak dostępu do internetu czyni technologię bezużyteczną	podatność na ataki i kradzież danych	WAGA	Iloczyn wag i interakcji	Ranga
Brak wykwalifikowanych osób	1	0	1	3	6	4
Wysokie zużycie energii	0	0	1	5	5	3
Dostęp wyłącznie za pośrednictwem internetu	1	0	1	3	6	4
wymaga wysokowydajnościowego sprzętu	0	0	1	3	3	2
zależność od Internetu	1	1	1	5	15	5
trudna integracja z innymi systemami	0	0	0	4	0	1
WAGA	5	4	3	**suma interakcji 9**		
Iloczyn wag i interakcji	15	4	15			
RANGA	5	4	5	suma iloczynów		69

Źródło: opracowanie własne

Tabela 5.62. Czy szanse Blockchain wpływają na mocne strony?

Szanse / Mocne strony	Łatwość dostępu	Kontrola zasobów	Stanowi własność użytkownika	Szyfrowanie danych	Transakcje bez osób trzecich	Weryfikacja tożsamości	WAGA	Iloczyn wag i interakcji	Ranga
usprawnienie zarządzania kryzysowego	1	1	1	1	1	1	5	45	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń	0	0	0	0	1	1	5	20	2
najnowsze technologie oraz oprogramowa-nie	1	1	1	1	1	1	4	36	3
Zabezpieczenie danych	0	1	1	1	1	1	5	40	4
zwiększenie efektywności działań	0	1	1	1	1	1	5	40	4
WAGA	4	5	5	5	5	5	**suma interakcji 24**		
Iloczyn wag i interakcji	8	20	20	20	25	25			
RANGA	3	4	4	4	5	5	suma iloczynów		299

Źródło: opracowanie własne

Tabela 5.63. Czy zagrożenia Blockchain wpływają na mocne strony?

Zagrożenia / Mocne strony	Łatwość dostępu	Kontrola zasobów	Stanowi własność użytkownika	Szyfrowanie danych	Transakcje bez osób trzecich	Weryfikacja tożsamości	WAGA	Iloczyn wag i interakcji	Ranga
utrata dostępu przy braku klucza prywatnego	0	1	1	1	1	0	5	20	5
brak dostępu do internetu czyni technologię bezużyteczną	0	1	1	1	1	1	4	20	5
podatność na ataki i kradzież danych	0	1	1	1	1	1	3	15	4
WAGA	4	5	5	5	5	5	**suma interakcji 14**		
Iloczyn wag i interakcji	0	15	15	15	15	10			
RANGA	3	5	5	5	5	4	suma iloczynów		125

Źródło: opracowanie własne

Tabela 5.64. Czy szanse Blockchain wpływają na słabe strony?

Szanse	Słabe strony	Brak wykwalifikowanych osób	Wysokie zużycie energii	Dostęp wyłącznie za pośrednictwem internetu	wymaga wysokowydajnościowego sprzętu	zależność od internetu	trudna integracja z innymi systemami	WAGA	Iloczyn wag i interakcji	Ranga
usprawnienie zarządzania kryzysowego		1	1	1	1	1	1	5	30	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń		1	1	1	0	1	1	5	25	4
najnowsze technologie oraz oprogramowanie		1	1	1	1	1	1	4	24	3
Zabezpieczenie danych		1	1	1	1	1	1	5	30	5
zwiększenie efektywności działań		1	1	1	1	1	1	5	30	5
WAGA		3	5	3	3	5	4	**suma interakcji 29**		
Iloczyn wag i interakcji		15	25	15	12	25	20			
RANGA		3	5	3	2	5	4	suma iloczynów		251

Źródło: opracowanie własne.

Tabela 5.65. Czy zagrożenia Blockchain wpływają na słabe strony?

Zagrożenia	Słabe strony	Brak wykwalifikowanych osób	Wysokie zużycie energii	Dostęp wyłącznie za pośrednictwem internetu	wymaga wysokowydajnościowego sprzętu	zależność od internetu	trudna integracja z innymi systemami	WAGA	Iloczyn wag i interakcji	Ranga
utrata dostępu przy braku klucza prywatnego		1	1	1	1	1	1	5	35	5
brak dostępu do internetu czyni technologię bezużyteczną		1	1	1	1	1	1	4	28	4
podatność na ataki i kradzież danych		1	1	1	1	1	1	3	21	3
WAGA		3	5	3	3	5	4	**suma interakcji 18**		
Iloczyn wag i interakcji		9	15	9	9	15	12			
RANGA		3	5	3	3	5	4	suma iloczynów		153

Źródło: opracowanie własne

SWOT/TOWS - SYSTEMY INFORMACJI GEOPRZESTRZENNEJ (GIS)

Tabela 5.66. Czy mocne strony GIS mogą wykorzystać szansę?

Mocne strony / Szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość wizualizacji zagrożeń	możliwość opracowywania scenariuszy przyszłych zagrożeń	zwiększenie efektywności działań	usprawnienie działania służb ratowniczych	WAGA	Iloczyn wag i interakcji	Ranga
szybkie i proste przeglądanie dużych zbiorów danych	1	1	1	1	1	1	5	30	5
pobieranie danych	1	1	1	1	1	1	5	30	5
analiza, monitorowanie, raportowanie danych w systemie	1	1	1	1	1	1	5	30	5
lokalizacja ważnych punktów z perspektywy ZK	1	1	1	1	1	1	5	30	5
tworzenie planu odbudowy	1	1	1	1	1	1	5	30	5
analiza danych	1	1	1	1	1	1	5	30	5
opracowywanie scenariuszy planów ZK	1	1	1	1	1	1	5	30	5
opracowywanie przyszłych działań dla ZK	1	1	1	1	1	1	5	30	5
WAGA	5	5	4	5	5	4	**suma interakcji 48**		
Iloczyn wag i interakcji	40	40	32	40	40	32			
RANGA	5	5	4	5	5	4	suma iloczynów		464

Źródło: opracowanie własne

Tabela 5.67. Czy mocne strony GIS przeważają nad zagrożenia?

Mocne strony / Zagrożenia	awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych	awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych	błędna wizualizacja danych	poleganie wyłącznie na technologii może wygenerować zagrożenia dla życia lub zdrowia	WAGA	Iloczyn wag i interakcji	Ranga
szybkie i proste przeglądanie dużych zbiorów danych	1	1	0	0	5	10	4
pobieranie danych	1	1	0	0	5	10	4
analiza, monitorowanie, raportowanie danych w systemie	1	1	1	1	5	20	5
lokalizacja ważnych punktów z perspektywy ZK	1	1	1	1	5	20	5
tworzenie planu odbudowy	1	1	1	1	5	20	5
analiza danych	1	1	1	1	5	20	5
WAGA	5	3	3	3	suma interakcji 20		
Iloczyn wag i interakcji	30	18	12	12			
RANGA	5	4	3	3	suma iloczynów		172

Źródło: opracowanie własne

Tabela 5.68. Czy słabe strony GIS ograniczą wykorzystanie szansy?

słabe strony	szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość wizualizacji zagrożeń	możliwość opracowywania scenariuszy przyszłych zagrożeń	zwiększenie efektywności działań	usprawnienie działania służb ratowniczych	WAGA	Iloczyn wag i interakcji	Ranga
duże koszty wdrożenia		1	1	1	1	0	1	4	20	5
brak znajomości technologii		1	0	1	1	0	1	4	16	4
potrzeba przeszkolenia pracowników		1	0	1	1	0	1	3	12	3
ograniczenia czasowe		1	0	1	1	0	0	4	12	3
brak dostępu do danych		1	0	1	1	0	1	3	12	3
WAGA		5	5	4	5	5	4	**suma interakcji 20**		
Iloczyn wag i interakcji		25	5	20	25	0	16			
RANGA		5	2	4	5	1	3	suma iloczynów	163	

Źródło: opracowanie własne.

Tabela 5.69. Czy słabe strony GIS mogą mieć wpływ na zagrożenia?

słabe strony	zagrożenia	awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych	awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych	błędna wizualizacja danych	poleganie wyłącznie na technologii może wygenerować zagrożenia dla życia lub zdrowia	WAGA	Iloczyn wag i interakcji	Ranga
duże koszty wdrożenia		0	0	0	0	4	0	2
brak znajomości technologii		0	0	1	0	4	4	4
potrzeba przeszkolenia pracowników		0	0	1	0	3	3	3
ograniczenia czasowe		0	0	1	0	4	4	4
brak dostępu do danych		1	1	1	0	3	9	5
WAGA		5	3	3	3	**suma interakcji 6**		
Iloczyn wag i interakcji		5	3	12	0			
RANGA		4	3	5	2	suma iloczynów		40

Źródło: opracowanie własne

Tabela 5.70. Czy szanse GIS wpływają na mocne strony?

Szanse / Mocne strony	szybkie i proste przeglądanie dużych zbiorów danych	pobieranie danych	analiza, monitorowanie, raportowanie danych w systemie	lokalizacja ważnych punktów z perspektywy ZK	tworzenie planu odbudowy	analiza danych	opracowywanie scenariuszy planów ZK	opracowywanie przyszłych działań dla ZK	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji	1	1	1	1	1	1	1	1	5	55	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń	1	1	1	1	1	1	1	1	5	50	4
możliwość wizualizacji zagrożeń	1	1	1	1	1	1	1	1	4	44	2
możliwość opracowywania scenariuszy przyszłych zagrożeń	1	1	1	1	1	1	1	1	5	55	5
zwiększenie efektywności działań	1	1	1	1	1	1	1	1	5	40	2
usprawnienie działania służb ratowniczych	1	1	1	1	1	1	1	1	4	44	3
WAGA	5	5	5	5	5	5	5	5	suma interakcji 48		
Iloczyn wag i interakcji	30	30	30	30	30	30	30	30			
RANGA	5	5	5	5	5	5	5	5	suma iloczynów	528	

Źródło: opracowanie własne

Tabela 5.71. Czy zagrożenia GIS wpływają na mocne strony?

Zagrożenia / Mocne strony	szybkie i proste przeglądanie dużych zbiorów danych	pobieranie danych	analiza, monitorowanie, raportowanie danych w systemie	lokalizacja ważnych punktów z perspektywy ZK	tworzenie planu odbudowy	analiza danych	opracowywanie scenariuszy planów ZK	opracowywanie przyszłych działań dla ZK	WAGA	Iloczyn wag i interakcji	Ranga
awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych	1	1	1	1	1	1	1	0	5	40	5
awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych	1	1	1	1	1	1	1	1	3	30	4
błędna wizualizacja danych	0	0	1	1	1	1	1	1	3	18	3
poleganie wyłącznie na technologii może wygenerować zagrożenia dla życia lub zdrowia	0	0	0	0	0	0	0	0	3	9	2
WAGA	5	5	5	5	5	5	5	5	**suma interakcji 21**		
Iloczyn wag i interakcji	10	10	15	15	15	15	15	10			
RANGA	4	4	5	5	5	5	5	4	suma iloczynów	202	

Źródło: opracowanie własne.

Tabela 5.72. Czy szanse GIS wpływa na słabe strony?

Szanse	Słabe strony	duże koszty wdrożenia	brak znajomości technologii	potrzeba przeszkolenia pracowników	ograniczenia czasowe	brak dostępu do danych	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji		0	1	1	1	1	5	20	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń		0	1	1	1	1	5	20	5
możliwość wizualizacji zagrożeń		0	1	1	1	1	4	16	4
możliwość opracowywania scenariuszy przyszłych zagrożeń		0	1	1	1	1	5	20	5
zwiększenie efektywności działań		0	1	1	1	1	5	20	5
usprawnienie działania służb ratowniczych		0	1	1	1	1	4	16	4
WAGA		4	4	3	4	3	**suma interakcji 24**		
Iloczyn wag i interakcji		0	24	18	24	18			
RANGA		3	5	4	5	4	suma iloczynów		196

Źródło: opracowanie własne

Tabela 5.73. Czy zagrożenia GIS wpływają na słabe strony?

Zagrożenia	Słabe strony	duże koszty wdrożenia	brak znajomości technologii	potrzeba przeszkolenia pracowników	ograniczenia czasowe	brak dostępu do danych	WAGA	Iloczyn wag i interakcji	Ranga
awaria infrastruktury energetycznej może unieruchomić oprogramowanie do wizualizacji danych		1	0	0	0	1	5	10	4
awaria infrastruktury teleinformatycznej może unieruchomić oprogramowanie do wizualizacji danych		1	0	0	0	1	3	6	3
błędna wizualizacja danych		0	1	1	1	1	3	12	5
poleganie wyłącznie na technologii może wygenerować zagrożenia dla życia lub zdrowia		0	1	1	1	1	3	12	5
WAGA		4	4	3	4	3	**suma interakcji 12**		
Iloczyn wag i interakcji		8	8	6	8	12			
RANGA		4	4	3	4	5	suma iloczynów		82

Źródło: opracowanie własne

SWOT/TOWS - OLAP

Tabela 5.74. Czy mocne strony OLAP mogą wykorzystać szansę?

Mocne strony / Szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość klasyfikacji zagrożeń	cyfryzacja	możliwość gromadzenia dużej ilości danych	szybki dostęp do danych z dowolnego miejsca	WAGA	Iloczyn wag i interakcji	Ranga
eksploracja danych	1	1	1	1	1	1	5	30	5
wspomaganie decyzji i raportowanie	1	1	1	1	1	1	5	30	5
szybka analiza wielowymiarowych informacji	1	1	1	1	1	1	5	30	5
elastyczność	1	1	1	1	1	1	5	30	5
łatwość dostępu do danych	1	1	1	1	1	1	5	30	5
Konsolidacja	1	1	1	1	1	1	5	30	5
łatwa analiza i obliczenia na danych	1	1	1	1	1	1	5	30	5
szybkie zapytania analityczne	1	1	1	1	1	1	5	30	5
WAGA	5	5	4	5	5	4	**suma interakcji**		
Iloczyn wag i interakcji	40	40	32	40	40	32	**48**		
RANGA	5	5	4	5	5	4	suma iloczynów		464

Źródło: opracowanie własne

Tabela 5.75. Czy mocne strony OLAP przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	podatność na ataki	awaria infrastruktury teleinformatycznej może unieruchomić technologię	błąd ludzki	awaria infrastruktury energetycznej może unieruchomić technologię	WAGA	Iloczyn wag i interakcji	Ranga
eksploracja danych	1	1	0	0	5	10	4
wspomaganie decyzji i raportowanie	1	1	0	0	5	10	4
szybka analiza wielowymiarowych informacji	1	1	1	0	5	15	5
elastyczność	1	1	1	0	5	15	5
łatwość dostępu do danych	1	1	1	0	5	15	5
Konsolidacja	1	1	1	0	5	15	5
WAGA	5	3	1	5	**suma interakcji**		
Iloczyn wag i interakcji	30	18	4	0	**16**		
RANGA	5	4	3	2	suma iloczynów		132

Źródło: opracowanie własne

Tabela 5.76. Czy słabe strony OLAP ogranicza wykorzystanie szansy?

słabe strony	szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość klasyfikacji zagrożeń	cyfryzacja	możliwość gromadzenia dużej ilości danych	szybki dostęp do danych z dowolnego miejsca	WAGA	Iloczyn wag i interakcji	Ranga
duże koszty wdrożenia		0	0	1	1	0	1	3	9	3
brak znajomości technologii		1	1	1	1	1	1	1	6	2
potrzeba przeszkolenia pracowników		1	0	1	1	1	1	4	20	5
ograniczenia czasowe		0	0	1	1	1	0	5	15	4
zależność od sieci energetycznej i Internetu		1	0	1	0	1	1	5	20	5
WAGA		5	5	4	5	5	4	**suma interakcji 21**		
Iloczyn wag i interakcji		15	5	20	20	20	16			
RANGA		3	2	5	5	5	4	suma iloczynów		166

Źródło: opracowanie własne

Tabela 5.77. Czy słaba strona OLAP może mieć wpływ na zagrożenia?

słabe strony	zagrożenia	podatność na ataki	awaria infrastruktury teleinformatycznej może unieruchomić technologię	błąd ludzki	awaria infrastruktury energetycznej może unieruchomić technologię	WAGA	Iloczyn wag i interakcji	Ranga
duże koszty wdrożenia		0	0	0	0	3	0	2
brak znajomości technologii		1	0	1	0	1	2	3
potrzeba przeszkolenia pracowników		1	0	1	0	4	8	5
ograniczenia czasowe		0	0	0	0	5	0	2
zależność od sieci energetycznej i Internetu		0	1	0	1	5	10	5
WAGA		5	3	1	5	**suma interakcji 6**		
Iloczyn wag i interakcji		10	3	2	5			
RANGA		5	3	2	4	suma iloczynów		40

Źródło: opracowanie własne

Tabela 5.78. Czy szanse OLAP wpływają na mocne strony?

Szanse	Mocne strony	eksploracja danych	wspomaganie decyzji i raportowanie	szybka analiza wielowymiarowych informacji	elastyczność	łatwość dostępu do danych	Konsolidacja	łatwa analiza i obliczenia na danych	szybkie zapytania analityczne	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji		1	1	1	1	1	1	1	1	5	40	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń		1	1	1	1	1	1	1	1	5	40	5
możliwość klasyfikacji zagrożeń		1	1	1	1	1	1	1	1	4	32	4
cyfryzacja		1	1	1	1	1	1	1	1	5	40	5
możliwość gromadzenia dużej ilości danych		1	1	1	1	1	1	1	1	5	40	5
szybki dostęp do danych z dowolnego miejsca		1	1	1	1	1	1	1	1	4	32	4
WAGA		5	5	5	5	5	5	5	5	**suma interakcji 48**		
Iloczyn wag i interakcji		30	30	30	30	30	30	30	30			
RANGA		5	5	5	5	5	5	5	5	suma iloczynów		464

Źródło: opracowanie własne

Tabela 5.79. Czy zagrożenia OLAP wpływają na mocne strony?

Zagrożenia	Mocne strony	eksploracja danych	wspomaganie decyzji i raportowanie	szybka analiza wielowymiarowych informacji	elastyczność	łatwość dostępu do danych	Konsolidacja	łatwa analiza i obliczenia na danych	szybkie zapytania analityczne	WAGA	Iloczyn wag i interakcji	Ranga
podatność na ataki		0	0	0	0	0	0	0	0	5	0	4
awaria infrastruktury teleinformatycznej może unieruchomić technologię		0	0	0	0	0	0	0	0	3	0	4
błąd ludzki		1	1	1	0	1	1	1	1	1	7	5
awaria infrastruktury energetycznej może unieruchomić technologię		0	0	0	0	0	0	0	0	1	0	4
WAGA		5	5	5	5	5	5	5	5	**suma interakcji 7**		
ILOCZYN WAG		5	5	5	0	5	5	5	5			
RANGA		5	5	5	4	5	5	5	5	suma iloczynów		42

Źródło: opracowanie własne

Tabela 5.80. Czy szanse OLAP wpływają na słabe strony?

Szanse	Słabe strony	duże koszty wdrożenia	brak znajomości technologii	potrzeba przeszkolenia pracowników	ograniczenia czasowe	zależność od sieci energetycznej i Internetu	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji		0	0	1	0	1	5	10	2
zwiększenie świadomości sytuacyjnej na temat zagrożeń		0	0	1	1	1	5	15	3
możliwość klasyfikacji zagrożeń		0	0	0	1	1	4	8	1
cyfryzacja		1	0	1	0	1	5	15	3
możliwość gromadzenia dużej ilości danych		1	0	1	1	1	5	20	5
szybki dostęp do danych z dowolnego miejsca		1	0	1	1	1	4	16	4
WAGA		3	1	4	5	5	**suma interakcji 18**		
Iloczyn wag i interakcji		9	0	20	20	30			
RANGA		3	2	4	4	5	suma iloczynów		163

Źródło: opracowanie własne

Tabela 5.81. Czy zagrożenia OLAP wpływają na słabe strony?

Zagrożenia	Słabe strony	duże koszty wdrożenia	brak znajomości technologii	potrzeba przeszkolenia pracowników	ograniczenia czasowe	zależność od sieci energetycznej i Internetu	WAGA	Iloczyn wag i interakcji	Ranga
podatność na ataki		0	1	1	1	1	5	20	5
awaria infrastruktury teleinformatycznej może unieruchomić technologię		0	0	0	0	1	3	3	2
błąd ludzki		0	1	1	1	1	1	4	3
awaria infrastruktury energetycznej może unieruchomić technologię		0	0	0	0	1	5	5	4
WAGA		3	1	4	5	5	**suma interakcji 10**		
Iloczyn wag i interakcji		0	2	8	10	20			
RANGA		1	2	3	4	5	suma iloczynów		72

Źródło: opracowanie własne

SWOT/TOWS - *OLTP*

Tabela 5.82. Czy mocne strony OLTP mogą wykorzystać szanse?

Mocne strony / Szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość klasyfikacji zagrożeń	cyfryzacja	możliwość gromadzenia dużej ilości danych	szybki dostęp do danych z dowolnego miejsca	WAGA	Iloczyn wag i interakcji	Ranga
współbieżność	1	1	1	1	1	1	5	30	5
integralność danych	1	1	1	1	1	1	5	30	5
proste transakcje	1	1	1	1	1	1	5	30	5
zindeksowane zestawy danych	1	1	1	1	1	1	5	30	5
czas reakcji	1	1	1	1	1	1	5	30	5
dostępność	1	1	1	1	1	1	5	30	5
rozmiar danych	1	1	1	1	1	1	5	30	5
atomowość	1	1	1	1	1	1	5	30	5
WAGA	5	5	3	4	4	4	**suma interakcji 48**		440
Iloczyn wag i interakcji	40	40	24	32	32	32			
RANGA	5	5	3	4	4	4	suma iloczynów		

Źródło: opracowanie własne.

Tabela 5.83. Czy mocne strony OLTP przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	utrata danych	podatność na ataki	błąd ludzki	awaria infrastruktury energetycznej może unieruchomić technologię	WAGA	Iloczyn wag i interakcji	Ranga
współbieżność	0	0	0	0	5	0	3
integralność danych	0	1	0	0	5	5	4
proste transakcje	0	1	1	0	5	10	5
zindeksowane zestawy danych	0	1	1	0	5	10	5
czas reakcji	0	1	1	0	5	10	5
dostępność	0	1	1	0	5	10	5
WAGA	5	3	4	5	**suma interakcji 9**		76
Iloczyn wag i interakcji	0	15	16	0			
RANGA	3	4	5	3	suma iloczynów		

Źródło: opracowanie własne.

Tabela 5.84. Czy słaba strona OLTP ogranicza wykorzystanie szansy?

słabe strony / szanse	ułatwiony przekaz informacji	zwiększenie świadomości sytuacyjnej na temat zagrożeń	możliwość klasyfikacji zagrożeń	cyfryzacja	możliwość gromadzenia dużej ilości danych	szybki dostęp do danych z dowolnego miejsca	WAGA	Iloczyn wag i interakcji	Ranga
kopie zapasowe	0	1	1	1	1	1	3	15	4
podatność na awarię	0	1	1	1	1	1	1	5	3
zapytania *SQL*	0	1	1	1	1	1	4	20	5
zależność od personelu	0	0	0	1	1	1	5	15	4
koszt wdrożenia	0	0	0	1	1	1	5	15	4
WAGA	5	5	3	4	4	4	**suma interakcji 21**		
Iloczyn wag i interakcji	0	15	9	20	20	20			
RANGA	2	4	3	5	5	5	suma iloczynów		154

Źródło: opracowanie własne

Tabela 5.85. Czy słaba strona OLTP może mieć wpływ na zagrożenia?

słabe strony / zagrożenia	utrata danych	podatność na ataki	błąd ludzki awaria infrastruktury energetycznej może unieruchomić technologię	WAGA	Iloczyn wag i interakcji	Ranga
kopie zapasowe	0	0	1	1	3	6	3
podatność na awarię	1	1	1	1	1	4	2
zapytania *SQL*	0	1	1	1	4	12	4
zależność od personelu	1	1	1	1	5	20	5
koszt wdrożenia	1	1	1	1	5	20	5
WAGA	5	3	4	5	**suma interakcji 17**		
Iloczyn wag i interakcji	15	12	20	25			
RANGA	3	4	4	5	suma iloczynów		134

Źródło: opracowanie własne

Tabela 5.86. Czy szanse OLTP wpływają na mocne strony?

Szanse / Mocne strony	współbieżność	integralność danych	proste transakcje	zindeksowane zestawy danych	czas reakcji	dostępność	rozmiar danych	atomowość	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji	1	1	1	1	1	1	1	1	5	40	5
zwiększenie świadomości sytuacyjnej na temat zagrożeń	1	1	1	1	1	1	1	1	5	40	4
możliwość klasyfikacji zagrożeń	1	1	1	1	1	1	1	1	3	24	2
cyfryzacja	1	1	1	1	1	1	1	1	4	44	3
możliwość gromadzenia dużej ilości danych	1	1	1	1	1	1	1	1	4	32	1
szybki dostęp do danych z dowolnego miejsca	1	1	1	1	1	1	1	1	4	32	3
WAGA	5	5	5	5	5	5	5	5	**suma interakcji 48**		
Iloczyn wag i interakcji	30	30	30	30	30	30	30	30			
RANGA	5	5	5	5	5	5	5	5	suma iloczynów		452

Źródło: opracowanie własne

Tabela 5.87. Czy zagrożenia OLTP wpływają na mocne strony ?

Zagrożenia / Mocne strony	współbieżność	integralność danych	proste transakcje	zindeksowane zestawy danych	czas reakcji	dostępność	rozmiar danych	atomowość	WAGA	Iloczyn wag i interakcji	Ranga
utrata danych	0	0	0	0	0	0	0	0	5	0	2
podatność na ataki	0	0	0	0	0	0	0	0	3	0	3
błąd ludzki	1	1	1	0	1	1	1	1	4	28	5
awaria infrastruktury energetycznej może unieruchomić technologię	0	0	0	0	0	0	0	0	4	12	4
WAGA	5	5	5	5	5	5	5	5	**suma interakcji 7**		
Iloczyn wag i interakcji	5	5	5	0	5	5	5	5			
RANGA	5	5	5	4	5	5	5	5	suma iloczynów		63

Źródło: opracowanie własne

Tabela 5.88. Czy szanse OLTP wpływa na słabe strony?

Szanse / Słabe strony	kopie zapasowe	podatność na awarię	zapytania *SQL*	zależność od personelu	koszt wdrożenia	WAGA	Iloczyn wag i interakcji	Ranga
ułatwiony przekaz informacji	0	0	1	0	1	5	10	3
zwiększenie świadomości sytuacyjnej na temat zagrożeń	0	0	1	1	1	5	15	4
możliwość klasyfikacji zagrożeń	0	0	0	1	1	3	6	1
cyfryzacja	1	0	1	0	1	4	12	3
możliwość gromadzenia dużej ilości danych	1	0	1	1	1	4	16	5
szybki dostęp do danych z dowolnego miejsca	1	0	1	1	1	4	16	5
WAGA	3	1	4	5	5	**suma interakcji 18**		
Iloczyn wag i interakcji	9	0	20	20	0			
RANGA	4	3	5	5	3	suma iloczynów		124

Źródło: opracowanie własne

Tabela 5.89. Czy zagrożenia OLTP wpływają na słabe strony?

Zagrożenia / Słabe strony	kopie zapasowe	podatność na awarię	zapytania *SQL*	zależność od personelu	koszt wdrożenia	WAGA	Iloczyn wag i interakcji	Ranga
utrata danych	0	1	1	1	1	5	20	5
podatność na ataki	0	0	0	0	1	3	3	2
błąd ludzki	0	1	1	1	1	4	16	4
awaria infrastruktury energetycznej może unieruchomić technologię	0	0	0	0	1	5	5	3
WAGA	3	1	4	5	5	**suma interakcji 10**		
Iloczyn wag i interakcji	0	2	8	10	20			
RANGA	1	2	5	4	5	suma iloczynów		84

Źródło: opracowanie własne

SWOT/TOWS - *BUSINESS INTELIGENCE*

Tabela 5.90. Czy mocne strony Business Inteligence mogą wykorzystać szanse?

Mocne strony / Szanse	zwiększenie świadomości sytuacyjnej na temat zagrożeń	opracowanie raportów na temat przyszłych	dostęp do danych	wizualizacja danych	cyfryzacja	usprawniony proces zarządzania kryzysowego	WAGA	Iloczyn wag i interakcji	Ranga
ułatwienie podejmowania decyzji	1	1	1	1	1	1	5	30	5
wgląd w kluczowe informacje	1	1	1	1	1	1	5	30	5
dodatkowa baza danych	1	1	1	1	1	1	5	30	5
raporty	1	1	1	1	1	1	5	30	5
łatwa lokalizacja punktów newralgicznych	1	1	1	1	1	1	5	30	5
aktualność danych	1	1	1	1	1	1	5	30	5
prosty interfejs oprogramowania	1	1	1	1	1	1	5	30	5
\krótki czas odpowiedzi na zapytania	1	1	1	1	1	1	5	30	5
WAGA	5	5	3	5	5	5	**suma interakcji 48**		
Iloczyn wag i interakcji	40	40	24	40	40	40			
RANGA	5	5	4	5	5	5	suma iloczynów		464

Źródło: opracowanie własne

Tabela 5.91. Czy mocne strony Business Inteligence przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	podatność na ataki	błąd ludzki	utrata danych	podatność na awarie systemu	WAGA	Iloczyn wag i interakcji	Ranga
ułatwienie podejmowania decyzji	0	0	0	0	5	0	3
wgląd w kluczowe informacje	1	1	1	0	5	15	5
dodatkowa baza danych	1	0	0	0	5	5	4
raporty	1	0	0	0	5	5	4
łatwa lokalizacja punktów newralgicznych	1	0	0	0	5	5	4
aktualność danych	1	0	0	0	5	5	4
WAGA	5	3	3	5	**suma interakcji 7**		
Iloczyn wag i interakcji	25	3	3	0			
RANGA	5	4	4	3	suma iloczynów		66

Źródło: opracowanie własne

Tabela 5.92. Czy słaba strona Business Inteligence ogranicza wykorzystanie szansy?

słabe strony	szanse	zwiększenie świadomości sytuacyjnej na temat zagrożeń	opracowanie raportów na temat przyszłych	dostęp do danych	wizualizacja danych	cyfryzacja	usprawniony proces zarządzania kryzysowego	WAGA	Iloczyn wag i interakcji	Ranga
koszt wdrożenia		0	0	0	1	1	1	5	15	3
wysokie wymagania sprzętowe		0	0	1	1	1	1	5	20	5
wymaga stałego nadzoru		0	0	1	1	1	1	4	16	4
zależność od sieci energetycznej lub Internetu		0	0	1	1	1	1	5	20	5
koszt szkoleń pracowników		0	0	1	1	1	1	5	20	5
WAGA		5	5	3	5	5	5	**suma interakcji 19**		
Iloczyn wag i interakcji		0	0	12	25	25	25			
RANGA		3	3	4	5	5	5	suma iloczynów		178

Źródło: opracowanie własne

Tabela 5.93. Czy słabe strony Business Inteligence mogą mieć wpływ na zagrożenia?

słabe strony	zagrożenia	podatność na ataki	błąd ludzki	utrata danych	podatność na awarie systemu	WAGA	Iloczyn wag i interakcji	Ranga
koszt wdrożenia		0	0	1	1	5	10	3
wysokie wymagania sprzętowe		1	1	1	1	5	20	5
wymaga stałego nadzoru		0	1	1	1	4	12	4
zależność od sieci energetycznej lub Internetu		1	1	1	1	5	20	5
koszt szkoleń pracowników		1	1	1	1	5	20	5
WAGA		5	3	3	5	**suma interakcji 17**		
Iloczyn wag i interakcji		15	12	15	25			
RANGA		4	3	4	5	suma iloczynów		149

Źródło: opracowanie własne

Tabela 5.94. Czy szanse Business Inteligence wpływają na mocne strony?

Szanse	Mocne strony	ułatwienie podejmowania decyzji	wgląd w kluczowe informacje	dodatkowa baza danych	raporty	łatwa lokalizacja punktów newralgicznych	aktualność danych	prosty interfejs oprogramowania	krótki czas odpowiedzi na zapytania	WAGA	Iloczyn wag i interakcji	Ranga
zwiększenie świadomości sytuacyjnej na temat zagrożeń		1	1	1	1	1	1	1	1	5	55	5
opracowanie raportów na temat przyszłych		1	1	1	1	1	1	1	1	5	50	4
dostęp do danych		1	1	1	1	1	1	1	1	3	33	3
wizualizacja danych		1	1	1	1	1	1	1	1	5	55	5
cyfryzacja		1	1	1	1	1	1	1	1	5	40	3
usprawniony proces zarządzania kryzysowego		1	1	1	1	1	1	1	1	5	55	5
WAGA		5	5	5	5	5	5	5	5	**suma interakcji 48**		
Iloczyn wag i interakcji		30	30	30	30	30	30	30	30			
RANGA		5	5	5	5	5	5	5	5	suma iloczynów		528

Źródło: opracowanie własne

Tabela 5.95. Czy zagrożenia Business Inteligence wpływają na mocne strony?

Zagrożenia / Mocne strony	ułatwienie podejmowania decyzji	wgląd w kluczowe informacje	dodatkowa baza danych	raporty	łatwa lokalizacja punktów newralgicznych	aktualność danych	prosty interfejs oprogramowania	krótki czas odpowiedzi na zapytania	WAGA	Iloczyn wag i interakcji	Ranga
podatność na ataki	0	1	0	0	0	0	0	0	5	10	2
błąd ludzki	0	1	0	0	0	0	0	0	3	9	3
utrata danych	0	1	0	0	1	0	0	0	3	6	4
podatność na awarie systemu	0	1	0	0	0	0	0	0	3	12	1
WAGA	5	5	5	5	5	5	5	5	**suma interakcji 5**		
Iloczyn wag i interakcji	0	20	0	0	5	0	0	0			
RANGA	0	1	0	0	2	0	0	0	suma iloczynów		62

Źródło: opracowanie własne

Tabela 5.96. Czy szanse Business Inteligence wpływają na słabe strony?

Szanse / Słabe strony	koszt wdrożenia	wysokie wymagania sprzętowe	wymaga stałego nadzoru	zależność od sieci energetycznej lub Internetu	koszt szkoleń pracowników	WAGA	Iloczyn wag i interakcji	Ranga
zwiększenie świadomości sytuacyjnej na temat zagrożeń	1	1	1	1	1	5	25	5
opracowanie raportów na temat przyszłych	1	1	1	1	1	5	25	5
dostęp do danych	1	1	1	1	1	3	15	4
wizualizacja danych	1	1	1	1	1	5	25	5
cyfryzacja	1	1	1	1	1	5	25	5
usprawniony proces zarządzania kryzysowego	1	1	1	1	1	5	25	5
WAGA	5	5	4	5	5	**suma interakcji 30**		
Iloczyn wag i interakcji	30	30	24	30	0			
RANGA	5	5	4	5	3	suma iloczynów	254	

Źródło: opracowanie własne

Tabela 5.97. Czy zagrożenia Business Inteligence wpływają na słabe strony?

Zagrożenia / Słabe strony	koszt wdrożenia	wysokie wymagania sprzętowe	wymaga stałego nadzoru	zależność od sieci energetycznej lub Internetu	koszt szkoleń pracowników	WAGA	Iloczyn wag i interakcji	Ranga
podatność na ataki	0	0	1	0	1	5	15	5
błąd ludzki	0	0	1	0	1	3	9	4
utrata danych	0	0	1	0	1	3	6	3
podatność na awarie systemu	0	0	1	0	1	5	15	5
WAGA	5	5	4	5	5	**suma interakcji 8**		
Iloczyn wag i interakcji	0	0	16	0	0			
RANGA	4	4	5	4	4	suma iloczynów	61	

Źródło: opracowanie własne

SWOT/TOWS - *BIG DATA*

Tabela 5.98. Czy mocne strony Big Data mogą wykorzystać szanse?

Mocne strony / Szanse	przetwarzanie danych	zwiększenie poziomu świadomości sytuacyjnej	dostępność	WAGA	Iloczyn wag i interakcji	Ranga
duża dostępność danych	1	1	1	5	15	5
różnorodność danych	1	1	1	5	15	5
dodatkowa baza danych	1	1	1	5	15	5
szczegółowość danych	1	1	1	5	15	5
zbieranie danych	1	1	1	5	15	5
gromadzenie danych	1	1	1	5	15	5
WAGA	5	5	5	suma interakcji 18		
Iloczyn wag i interakcji	30	30	30			
RANGA	5	5	5	suma iloczynów		180

Źródło: opracowanie własne

Tabela 5.99. Czy mocne strony Big Data przeważają nad zagrożeniami?

Mocne strony / Zagrożenia	niewłaściwe wykorzystanie danych	podatność na ataki	zależność od dostępu do internetu lub sieci energetycznej	nieznajomość technologii	WAGA	Iloczyn wag i interakcji	Ranga
duża dostępność danych	1	1	0	0	5	10	4
różnorodność danych	1	1	0	0	5	10	4
dodatkowa baza danych	0	1	0	0	5	5	3
szczegółowość danych	1	1	0	0	5	10	4
zbieranie danych	1	1	1	0	5	15	5
gromadzenie danych	1	1	1	0	5	15	5
WAGA	5	3	3	5	**suma interakcji 13**		
Iloczyn wag i interakcji	25	18	6	0			
RANGA	5	4	3	2	suma iloczynów		114

Źródło: opracowanie własne

Tabela 5.100. Czy słaba strona Big Data ogranicza wykorzystanie szansy?

słabe strony / szanse	przetwarzanie danych	zwiększenie poziomu świadomości sytuacyjnej	dostępność	WAGA	Iloczyn wag i interakcji	Ranga
wymaga szkolenia personelu	1	1	0	5	10	5
niska jakość danych	0	0	0	5	0	3
koszty urządzeń wspomagających	1	1	0	4	8	4
zależność od technologii	1	1	0	5	10	5
błędne wyniki	1	1	0	5	10	5
WAGA	5	5	5	**suma interakcji 8**		
Iloczyn wag i interakcji	20	20	0			
RANGA	5	5	4	suma iloczynów		78

Źródło: opracowanie własne

Tabela 5.101. Czy słaba strona Big Data może mieć wpływ na zagrożenia?

słabe strony / zagrożenia	niewłaściwe wykorzystanie danych	podatność na ataki	zależność od dostępu do internetu lub sieci energetycznej	nieznajomość technologii	WAGA	Iloczyn wag i interakcji	Ranga
wymaga szkolenia personelu	1	1	1	1	5	20	5
niska jakość danych	0	0	0	1	5	5	3
koszty urządzeń wspomagających	0	0	0	1	4	4	2
zależność od technologii	0	0	0	1	5	5	3
błędne wyniki	1	0	0	1	5	10	4
WAGA	5	3	3	5	**suma interakcji 9**		
Iloczyn wag i interakcji	10	3	3	25			
RANGA	4	3	3	5	suma iloczynów		85

Źródło: opracowanie własne

Tabela 5.102. Czy szanse Big Data wpływają na mocne strony?

Szanse / Mocne strony	duża dostępność danych	różnorodność danych	dodatkowa baza danych	szczegółowość danych	zbieranie danych	gromadzenie danych	WAGA	Iloczyn wag i interakcji	Ranga
przetwarzanie danych	1	1	1	1	1	1	5	45	5
zwiększenie poziomu świadomości sytuacyjnej	1	1	1	1	1	1	5	40	4
dostępność	1	1	1	1	1	1	5	45	5
WAGA	5	5	5	5	5	5	**suma interakcji 18**		
Iloczyn wag i interakcji	15	15	15	15	15	15			
RANGA	5	5	5	5	5	5	suma iloczynów		220

Źródło: opracowanie własne

Tabela 5.103. Czy zagrożenia Big Data wpływają na mocne strony?

Zagrożenia / Mocne strony	duża dostępność danych	różnorodność danych	dodatkowa baza danych	szczegółowość danych	zbieranie danych	gromadzenie danych	WAGA	Iloczyn wag i interakcji	Ranga
niewłaściwe wykorzystanie danych	1	1	1	1	1	1	5	35	5
podatność na ataki	1	1	1	1	1	1	3	24	4
zależność od dostępu do Internetu lub sieci energetycznej	0	0	0	0	0	0	3	0	3
nieznajomość technologii	0	0	0	0	0	0	3	0	3
WAGA	5	5	5	5	5	5	**suma interakcji 12**		
Iloczyn wag i interakcji	10	10	10	10	10	10			
RANGA	5	5	5	5	5	5	suma iloczynów		119

Źródło: opracowanie własne

Tabela 5.104. Czy szanse Big Data wpływają na słabe strony?

Szanse	Słabe strony	wymaga szkolenia per-sonelu	niska jakość danych	koszty urządzeń wspo-magających	zależność od technologii	błędne wyniki	WAGA	Iloczyn wag i interakcji	Ranga
przetwarzanie danych		1	0	0	1	0	5	10	5
zwiększenie poziomu świadomości sytuacyjnej		1	0	1	0	0	5	10	5
dostępność		1	0	0	1	0	5	10	5
WAGA		5	5	4	5	5	**suma interakcji 6**		
Iloczyn wag i interakcji		15	0	4	10	0			
RANGA		5	2	3	4	2	suma iloczynów		59

Źródło: opracowanie własne

Tabela 5.105. Czy zagrożenia Big Data wpływają na słabe strony?

Zagrożenia	Słabe strony	wymaga szkolenia personelu	niska jakość danych	koszty urządzeń wspomagających	zależność od technologii	błędne wyniki	WAGA	Iloczyn wag i interakcji	Ranga
niewłaściwe wykorzystanie danych		1	0	0	1	1	5	20	5
podatność na ataki		1	0	0	1	1	3	12	4
zależność od dostępu do Internetu lub sieci energetycznej		0	0	0	1	0	3	3	3
nieznajomość technologii		1	0	0	1	1	5	20	5
WAGA		5	5	4	5	5	**suma interakcji 10**		
Iloczyn wag i interakcji		15	0	0	20	0			
RANGA		4	3	3	5	3	suma iloczynów		90

Źródło: opracowanie własne

Załącznik nr 6 - Kwestionariusz wywiadu eksperckiego

Szanowna Pani, Szanowny Panie,

Nazywam się Marcin Staruch i jestem doktorantem WAT w dziedzinie nauk społecznych, w dyscyplinie nauk o bezpieczeństwie, w trybie eksternistycznym. Realizuję rozprawę doktorską nt.: Kształtowanie świadomości sytuacyjnej w systemach zarządzania kryzysowego z wykorzystaniem wybranych platform IT.

W ramach tematu swojej rozprawy doktorskiej prowadziłem badania doskonalenia systemu zapewnienia świadomości sytuacyjnej w systemach zarządzania kryzysowego, a w szczególności nad stanem i sposobami systematycznego oraz systemowego wsparcia procesu podwyższenia stanu świadomości ludności i osób zarządzających.

W związku z tym zwracam się do Pani/Pana z uprzejmą prośbą o udzielenie odpowiedzi o charakterze eksperckim na poniżej sformułowane pytania. Zebrane tą metodą dane będą mieć dla mnie szczególną wartość i posłużą mi do obiektywizacji uzyskanych przeze mnie wyników oraz będą wykorzystane wyłącznie do realizacji celów naukowych założonych w mojej dysertacji. Pytania mają charakter półotwarty i ukierunkowane są na opis i wyjaśnienie ważnych problemów związanych kreowaniem pożądanego poziomu świadomości sytuacyjnej w Polsce. Dlatego też bardzo proszę o wszelkie uwagi i sugestie, które będą dla mnie bardzo cennym zasobem analitycznym do weryfikacji moich koncepcji naukowych w tym obszarze problemowym.

Z góry bardzo dziękuję za udzielone odpowiedzi, z wyrazami szacunku,

Marcin Staruch

Pytanie 1. Ostatnie dekady przyniosły zmiany w postrzeganiu świadomości sytuacyjnej (zagrożenia naturalne, zagrożenia wywołane działalnością człowieka, terroryzm i zagrożenia militarne oraz cyberterroryzm) w Polsce.

Stale ewoluujące zagrożenia wymagają wdrożenia odpowiednich działań ochronnych. Odpowiednio przygotowany system zarządzania kryzysowego powinien gwarantować bezpieczeństwo państwa w warunkach materializacji wybranych zagrożeń dla tego bezpieczeństwa. Racjonalne i efektywne działanie prowadzi do realizacji zamierzonego celu i skutecznego przeciwdziałania. W koncepcji zwrócono uwagę na fakt, że funkcjonujące w Polsce rozwiązania w zakresie działania systemu zarządzania kryzysowego i procesu informowania ludności o zagrożeniach wymagają udoskonalenia. **Jak ocenia Pani/Pan możliwości wykorzystania zaproponowanej klasyfikacji zagrożeń oraz tabeli zasobów (w aspekcie kreowania świadomości sytuacyjnej (postrzeganie, zrozumienie, prognozowanie) ludności na temat zagrożeń?**

	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Tabela klasyfikacji zagrożeń	☐	☐	☐	☐	☐
Tabela zasobów	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……..……

Pytanie 2. Postęp technologiczny spowodował, że głównym, a zarazem najszybszym sposobem przekazywania informacji na temat zagrożeń stał się telefon komórkowy niezależnie od jego rodzaju (klasyczny, Smartfon). Aktualnie wykorzystywanym systemem informowania o zagrożeniach jest alert RCB stanowiący główną formę przekazywania informacji. Istnieją również alternatywne jego odpowiedniki. Funkcjonalność tego rozwiązania opiera się na wysłaniu wiadomości tekstowej na telefon komórkowy. Niemniej jednak jak można zauważyć nie każda osoba dysponuje lub potrafi obsługiwać tego typu urządzenie. **Jak ocenia Pani/Pan możliwości rozszerzenia systemu informowania ludności o: ulotki, reklamy w miejscach publicznych i komunikacji miejskiej, audycje radiowo telewizyjne, a także o technologie sztucznej inteligencji takie jak np. chatbot (*rozumiany jako wirtualny asystent głosowo-tekstowy w zależności od wykorzystywanej technologii – tekst udzielenie odpowiedzi za tekstowych za pośrednictwem stron internetowych,***

***głos – rozmowa telefoniczna z botem*), których zadaniem jest udzielanie odpowiedzi na zadawane pytania?**

WYBRANE MOŻLIWOSCI	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Ulotki	☐	☐	☐	☐	☐
Reklamy w miejscach publicznych i komunikacji miejskiej	☐	☐	☐	☐	☐
Audycje radiowo- telewizyjne	☐	☐	☐	☐	☐
chatboty	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……..……

Pytanie 3. Rozwój technologii spowodował, że proces informowania ludności o zagrożeniach w znacznym stopniu przeniósł się do świata cyfrowego. Wszelkiego rodzaju poradniki rozumiane jako zbiór wskazówek na temat tego, jak należy albo jak jest najkorzystniej postępować w momencie wystąpienia zagrożenia dostępne są na stronach internetowych, do których nie każdy ma dostęp lub mogą być niedostępne w momencie zaistnienia sytuacji kryzysowej np. na skutek uszkodzenia infrastruktury krytycznej/telekomunikacyjnej. **Jak ocenia Pani/Pan przydatność poradników w formie papierowej zawierających informacje o zagrożeniach oraz sposoby radzenia sobie z nimi rozszerzonych o zaproponowaną klasyfikację zagrożeń (oraz tabelę zasobów.**

WYBRANE MOŻLIWOŚCI	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Poradniki w formie papierowej rozszerzone o klasyfikację zagrożeń	☐	☐	☐	☐	☐
Poradniki w formie papierowej rozszerzone o tabelę zasobów	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……..……

Pytanie 4. Analiza i gromadzenie danych na temat zagrożeń w postaci elektronicznej (pliki w różnych formatach) odgrywa istotną rolę w procesie skutecznego zarządzania kryzysowego. Odpowiednie wykorzystanie takich technologii jak systemy gromadzenia danych bieżących w trybie on-line i raportowania o sytuacji bieżącej w różnych obszarach działalności ludzkiej typu *OLTP*, systemy eksploracji i analizy danych historycznych/długookresowych typu *OLAP* wraz z mechanizmami odkrywania wiedzy/trendów rozwoju sytuacji typu DM określane często mianem systemów *Business Inteligence* oraz systemy *Big Data* umożliwiają realizację wszystkich tych funkcji w świecie danych wielopostaciowych (dane tabelaryczne, graficzne/obrazy, filmy,

schematy, dane tekstowe), a także systemy wizualizacji danych i systemy informacji geograficznej GIS mogą zwiększyć poziom świadomości sytuacyjnej obywateli na temat zagrożeń. **Jak ocenia Pani/Pan możliwości wykorzystania wymienionych technologii w odniesieniu do zwiększania poziomu świadomości sytuacyjnej na temat zagrożeń, a w konsekwencji do usprawnienia procesu zarządzania kryzysowego, a w szczególności do usprawnienia działania służb ratowniczych?**

1. *OLTP*

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Współbieżność	☐	☐	☐	☐	☐
Indeksowanie zbiorów danych	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Wyszukiwania i zapytania w bazie danych	☐	☐	☐	☐	☐
Tworzenie kopii zapasowych	☐	☐	☐	☐	☐
Monitorowanie sytuacji kryzysowych	☐	☐	☐	☐	☐
Zabezpieczenie danych	☐	☐	☐	☐	☐
Monitorowanie danych	☐	☐	☐	☐	☐
Raportowanie i wsparcie procesów decyzyjnych	☐	☐	☐	☐	☐

2. OLAP

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Analiza danych	☐	☐	☐	☐	☐
Przechowywanie danych	☐	☐	☐	☐	☐
Eksploracja danych	☐	☐	☐	☐	☐
Tworzenie raportów	☐	☐	☐	☐	☐
Zobrazowanie danych	☐	☐	☐	☐	☐

3. *Business Inteligence*

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Analiza danych	☐	☐	☐	☐	☐
Kontrola dostępu do danych	☐	☐	☐	☐	☐
Raportowanie i wizualizacja danych	☐	☐	☐	☐	☐
Monitorowanie zagrożeń	☐	☐	☐	☐	☐
Poodejmowanie decyzji	☐	☐	☐	☐	☐
Przetwarzanie danych	☐	☐	☐	☐	☐
Wymiana informacji	☐	☐	☐	☐	☐
Analiza danych historycznych	☐	☐	☐	☐	☐
Filtrowanie, sortowanie i grupowanie danych	☐	☐	☐	☐	☐

4. *Big Data*

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Identyfikacja i śledzenie populacji	☐	☐	☐	☐	☐
Mapowanie sytuacji kryzysowych	☐	☐	☐	☐	☐
Gromadzenie danych i modelowanie scenariuszy zagrożeń	☐	☐	☐	☐	☐
Lokalizacja zasobów	☐	☐	☐	☐	☐
Wysyłanie informacji o zagrożeniach	☐	☐	☐	☐	☐
Analiza danych	☐	☐	☐	☐	☐
Planowanie przyszłych działań	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……..……

Pytanie 5. Skuteczne zarządzanie kryzysowe opiera się na wykorzystaniu narzędzi i technologii w celu zwalczania skutków zagrożeń. **Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania Internetu Rzeczy (*IoT*, czyli łączenia różnych urządzeń/sensorów/czujników z systemami nadrzędnymi lub między sobą) oraz Internetu Wszechrzeczy (*IoE* czyli łączenia różnych urządzeń/sensorów/czujników z ludźmi lub bezpośrednio z ich urządzeniami) w zarządzaniu kryzysowym w kreowaniu świadomości sytuacyjnej zespołów zarządzania kryzysowego oraz obywateli?**

a. Dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Monitorowanie zagrożeń i aktualnego stanu	☐	☐	☐	☐	☐
Udostępnianie informacji	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Wykrywanie zagrożeń i otrzymywanie alertów	☐	☐	☐	☐	☐
Monitoring niezbędnych zasobów	☐	☐	☐	☐	☐
Identyfikacja zagrożeń	☐	☐	☐	☐	☐
Poszukiwanie poszkodowanych	☐	☐	☐	☐	☐
Sprawdzanie statusu siec np. energetycznej	☐	☐	☐	☐	☐
Sprawdzanie parametrów życiowych	☐	☐	☐	☐	☐
Wysyłanie alertów	☐	☐	☐	☐	☐
Odbieranie alertów	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……..……

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Monitorowanie zagrożeń i aktualnego stanu	☐	☐	☐	☐	☐
Udostępnianie informacji	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Wykrywanie zagrożeń i otrzymywanie alertów	☐	☐	☐	☐	☐
Monitoring niezbędnych zasobów	☐	☐	☐	☐	☐
Identyfikacja zagrożeń	☐	☐	☐	☐	☐
Poszukiwanie poszkodowanych	☐	☐	☐	☐	☐
Sprawdzanie statusu siec np. energetycznej	☐	☐	☐	☐	☐
Sprawdzanie parametrów życiowych	☐	☐	☐	☐	☐
Wysyłanie alertów	☐	☐	☐	☐	☐
Odbieranie alertów	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 6. Sztuczna Inteligencja umożliwia zastępowanie człowieka, decydenta lub odbiorcę wiadomości w złożonych procesach wnioskowania, łączenia faktów lub przewidywania rozwoju sytuacji. Oznaczać to może poprawę poziomu świadomości sytuacyjnej na temat zagrożeń, wsparcie dla służb ratowniczych w zakresie prowadzenia akcji ratunkowych, a także przygotowanie scenariuszy zagrożeń oraz przewidywanie ich skutków. **Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania sztucznej inteligencji w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego?**

a. Dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Robotyka(operacje ratowniczo-poszukiwawcze)	☐	☐	☐	☐	☐
Wymiana informacji	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Tworzenie chatbotów	☐	☐	☐	☐	☐
chatboty	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

b. **Dla obywateli**

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Wymiana informacji	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
chatboty	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 7. Technologia *VR* i *AR* umożliwia usprawnienie prowadzenia działań w zakresie przygotowania się na zagrożenia poprzez przeprowadzenie szkoleń oraz ćwiczeń w środowisku wirtualnym bez ryzyka strat w ludziach oraz sprzęcie, a także istotnie wpływa na poprawę świadomości sytuacyjnej na temat zagrożeń. **Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania *VR* i AR w zarządzaniu kryzysowym oraz w aspekcie poprawy świadomości sytuacyjnej zespołów zarządzania kryzysowego?**

a. dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Symulowanie realistycznych zagrożeń	☐	☐	☐	☐	☐
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	☐	☐	☐	☐	☐
Tworzenie realistycznych szkoleń dla służb ratowniczych	☐	☐	☐	☐	☐
Wyświetlanie nazw ulic, śledzenie służb ratowniczych	☐	☐	☐	☐	☐
Komunikacja głosowa	☐	☐	☐	☐	☐
Lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar	☐	☐	☐	☐	☐
Nanoszenie obrazów 3D na rzeczywiste środowisko	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Symulowanie realistycznych zagrożeń	☐	☐	☐	☐	☐
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	☐	☐	☐	☐	☐
Tworzenie realistycznych szkoleń dla służb ratowniczych	☐	☐	☐	☐	☐
Wyświetlanie nazw ulic, śledzenie służb ratowniczych	☐	☐	☐	☐	☐
Komunikacja głosowa	☐	☐	☐	☐	☐
Lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar	☐	☐	☐	☐	☐
Nanoszenie obrazów 3D na rzeczywiste środowisko	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 8. Wykorzystanie chmury obliczeniowej umożliwia dostęp do danych niezależnie od miejsca, w którym się znajdujemy za pośrednictwem np. telefonu, kompute-

ra czy tabletu. Chmura eliminuje wykluczenie informacyjne oraz ograniczenia czasowo – przestrzenne (geograficzne) i dostęp do zawansowanych usług IT (jak wyżej w innych pytaniach). **Jak ocenia Pani/Pan zaproponowane możliwości wykorzystania chmury obliczeniowej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego?**

a. dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Hosting w chmurze	☐	☐	☐	☐	☐
Dostęp do zasobów za pośrednictwem Internetu	☐	☐	☐	☐	☐
Komunikacja z dowolnego miejsca	☐	☐	☐	☐	☐
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	☐	☐	☐	☐	☐
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚR EDNIO	NISKO	BARDZO NISKO
Hosting w chmurze	☐	☐	☐	☐	☐
Dostęp do zasobów za pośrednictwem Internetu	☐	☐	☐	☐	☐
Komunikacja z dowolnego miejsca	☐	☐	☐	☐	☐
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	☐	☐	☐	☐	☐
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 9. Technologia *Blockchain* zapewnia szyfrowanie danych w taki sposób, aby niezbędne informacje i dane nie dostały się w niepowołane ręce. **Jak ocenia Pani/Pan możliwości wykorzystania *Blockchain* w zarządzaniu kryzysowym oraz**

w aspekcie kreowania świadomości sytuacyjnej zespołów zarządzania kryzysowego?

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Współpraca między interesariuszami zaangażowanymi w proces reagowania na katastrofy	☐	☐	☐	☐	☐
Identyfikacja poszkodowanych i zmarłych	☐	☐	☐	☐	☐
Weryfikacja tożsamości	☐	☐	☐	☐	☐
Szyfrowanie danych	☐	☐	☐	☐	☐
Rejestracja wolontariuszy	☐	☐	☐	☐	☐
Śledzenie dostaw	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 10. Systemy informacji geograficznej (GIS) mogą odgrywać istotną rolę na wszystkich szczeblach zarządzania kryzysowego, w procesie zwalczania klęsk żywiołowych oraz planowania działań zmierzających do likwidowania skutków zagrożeń. Wykorzystanie systemów GIS daje możliwość lokalizacji zdarzeń i posiadanych zasobów w przestrzeni geograficznej (na mapie cyfrowej) oraz ich wizualizacji, analizy sytuacyjnej, interpretowania i rozumienia danych w celu zrozumienia sytuacji kryzysowej z możliwością bardziej komunikatywnego procesu działania przed po i w trakcie wystąpienia zagrożenia. **Jak ocenia Pani/Pan możliwości wykorzystania Systemów Informacji Geoprzestrzennej w zarządzaniu kryzysowym oraz w aspekcie zwiększenia poziomu świadomości sytuacyjnej zespołów zarządzania kryzysowego oraz obywateli?**

a. dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Wizualizacja danych	☐	☐	☐	☐	☐
Analiza danych	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Ocena ryzyka	☐	☐	☐	☐	☐
Lokalizowanie ważnych punktów np. szpital, komisariat policji itp. Za pomocą zapytań *SQL*	☐	☐	☐	☐	☐
Szacowanie szkód	☐	☐	☐	☐	☐
Ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli	☐	☐	☐	☐	☐
Identyfikacja dróg ewakuacyjnych	☐	☐	☐	☐	☐
Tworzenie planów odbudowy	☐	☐	☐	☐	☐
Odbieranie alertów	☐	☐	☐	☐	☐
Analiza danych historycznych	☐	☐	☐	☐	☐

Opracowanie scenariuszy sytuacji kryzysowych	☐	☐	☐	☐	☐
Analiza skutków zagrożenia	☐	☐	☐	☐	☐
Planowanie przyszłych działań	☐	☐	☐	☐	☐
Zobrazowanie sytuacji kryzysowej	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Wizualizacja danych	☐	☐	☐	☐	☐
Analiza danych	☐	☐	☐	☐	☐
Pobieranie danych	☐	☐	☐	☐	☐
Lokalizowanie ważnych punktów np. szpital, komisariat policji itp. Za pomocą zapytań *SQL*	☐	☐	☐	☐	☐
Ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli	☐	☐	☐	☐	☐
Identyfikacja dróg ewakuacyjnych	☐	☐	☐	☐	☐
Odbieranie alertów	☐	☐	☐	☐	☐
Analiza danych historycznych	☐	☐	☐	☐	☐
Analiza skutków zagrożenia	☐	☐	☐	☐	☐
Planowanie przyszłych działań	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

Pytanie 11. Współczesne i tradycyjne technologie odgrywają istotną rolę w procesie informowania ludności o zagrożeniach. Technologie takie jak *IoT*, sztuczna inteligencja, portale społecznościowe, Smartfon czy systemy informacji geograficznej (GIS) mogą zwiększyć poziom świadomości sytuacyjnej na temat zagrożeń oraz usprawnić proces zarządzania kryzysowego. Ich tradycyjne odpowiedniki takie jak poradniki w wersji papierowej zawierające informacje o zagrożeniach oraz sposobie radzenia sobie z nimi, radio telewizja, klasyczny telefon komórkowy czy mapy w wersji papierowej stanowią alternatywne rozwiązanie dla współczesnych technologii, a także mogą zapewnić przekaz informacji w momencie awarii jednej ze współczesnych technologii. Pomimo iż tradycyjne technologie mają wiele ograniczeń są one nadal wykorzystywane przez część obywateli. **Jak ocenia Pani/Pan możliwości wykorzystania współczesnych i tradycyjnych technologii w procesie kształtowania świadomości sytuacyjnej na temat zagrożeń?**

1. **Współczesne technologie IT/ICT**
   a. **dla zespołów zarządzania kryzysowego**

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
IoT/IoE	☐	☐	☐	☐	☐
Sztuczna inteligencja - chatboty	☐	☐	☐	☐	☐
Media społecznościowe	☐	☐	☐	☐	☐
Informacje o zagrożeniach na ekranach wielkoformatowych	☐	☐	☐	☐	☐
Informacje o zagrożeniach za pośrednictwem poczty e-mail	☐	☐	☐	☐	☐
Informacje o zagrożeniach w środkach transportu	☐	☐	☐	☐	☐
Informacje o zagrożeniach w miejscach publicznych	☐	☐	☐	☐	☐

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSKO	ŚREDNIO	NISKO	BARDZO NISKO
IoT/IoE	☐	☐	☐	☐	☐
Sztuczna inteligencja - chatboty	☐	☐	☐	☐	☐
Media społecznościowe	☐	☐	☐	☐	☐
Informacje o zagrożeniach na ekranach wielkoformatowych	☐	☐	☐	☐	☐
Informacje o zagrożeniach za pośrednictwem poczty e-mail	☐	☐	☐	☐	☐
Informacje o zagrożeniach w środkach transportu	☐	☐	☐	☐	☐
Informacje o zagrożeniach w miejscach publicznych	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

2. Tradycyjne technologie

a. dla zespołów zarządzania kryzysowego

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Klasyczny telefon komórkowy - komunikaty o zagrożeniach	☐	☐	☐	☐	☐
Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach)	☐	☐	☐	☐	☐
Informacje o zagrożeniach za pośrednictwem poczty(list, telegram)	☐	☐	☐	☐	☐
Poradniki w wersji papierowej	☐	☐	☐	☐	☐
Szkolenia	☐	☐	☐	☐	☐
Konferencje	☐	☐	☐	☐	☐
Syreny alarmowe	☐	☐	☐	☐	☐
Środki masowego przekazu (radio, telewizja)	☐	☐	☐	☐	☐

b. dla obywateli

FUNKCJE	BARDZO WYSOKO	WYSOKO	ŚREDNIO	NISKO	BARDZO NISKO
Klasyczny telefon komórkowy - komunikaty o zagrożeniach	☐	☐	☐	☐	☐
Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach)	☐	☐	☐	☐	☐

Informacje o zagrożeniach za pośrednictwem poczty(list, telegram)	☐	☐	☐	☐	☐
Poradniki w wersji papierowej	☐	☐	☐	☐	☐
Szkolenia	☐	☐	☐	☐	☐
Konferencje	☐	☐	☐	☐	☐
Syreny alarmowe	☐	☐	☐	☐	☐
Środki masowego przekazu (radio, telewizja)	☐	☐	☐	☐	☐

Uzasadnienie wyboru i sugestia udoskonalenia

……

SUPLEMENT DO ZAŁĄCZNIKA NR 6 – WYWIADU EKSPERCKIEGO

Tabele:

KLASYFIKACJA ZAGROŻEŃ																		
	Katastrofy naturalne					Awarie techniczne						Zagrożenia wynikające z działalności człowieka						
												Katastrofy techniczne i naturalne powstałe na skutek działalności człowieka						
Rodzaj zagrożeń	Powodzie	Pożary	Susze	Wyładowania atmosferyczne	Silne wiatry	awarie sieci energetycznych	awarie sieci wodociągowych	awarie instalacji gazowej	awarie telekomunikacyjne	katastrofy budowlane	Zakłócenia bezpieczeństwa i porządku publicznego	awarie urządzeń infrastruktury technicznej	katastrofy budowlane	katastrofy komunikacyjne	awarie chemiczne	katastrofy ekologiczne	epidemie	Akty terroru
	W – Wymaga ewakuacji, N – Wymaga informowania, I – Wymaga izolacji																	
Wymaga ewakuacji	**W**	**W**						**W**		**W**			**W**	**W**				
wymaga informowania			**N**	**N**	**N**	**N**	**N**		**N**		**N**	**N**				**N**		
Wymaga izolacji	**I**	**I**	**I**		**I**			**I**			**I**				**I**		**I**	**I**

TABELA ZASOBÓW																		
Rodzaj zagrożenia	Katastrofy naturalne					Awarie techniczne						Zagrożenia wynikające z działalności człowieka						
												Katastrofy techniczne i naturalne powstałe na skutek działalności człowieka						
	Powodzie	Pożary	Susze	Wyładowania atmosferyczne	Silne wiatry	awarie sieci energetycznych	awarie sieci wodociągowych	awarie instalacji gazowej	awarie telekomunikacyjne	katastrofy budowlane	Zakłócenia bezpieczeństwa i porządku publicznego	awarie urządzeń infrastruktury technicznej	katastrofy budowlane	katastrofy komunikacyjne	awarie chemiczne	katastrofy ekologiczne	epidemie	Akty terroru
Rodzaj zasobu niezbędny w czasie sytuacji kryzysowej	Istotne zasoby dla ludności w momencie wystąpienia zagrożenia: **I** – istotne																	
Woda	I	I	I		I		I	I		I	I		I		I	I	I	I
Pożywienie	I	I	I		I			I		I	I		I		I	I	I	I
Odzież	I	I									I							I
Apteczka	I	I								I	I		I	I	I	I	I	I
Latarka	I	I		I	I	I				I		I	I					I
Gaśnica		I												I				
Dokumenty	I	I									I		I	I				I
Środki higieniczne	I	I								I	I		I		I	I	I	I
Zapasowe źródła energii: - baterie -powerbank	I	I		I	I	I			I	I	I	I	I	I		I		I
Dostęp do informacji: - telefon komórkowy - radio przenośne - krótkofalówki	I	I	I	I	I	I		I	I	I	I	I	I	I	I	I	I	I

Wpływ wykorzystania poszczególnych technologii na poziomy świadomości sytuacyjnej

TECHNOLOGIE \ POZIOMY ŚWIADOMOŚCI SYTUACYJNEJ	POSTRZEGANIE	ZROZUMIENIE	PROJEKCJA
IoT/IoE			
Monitorowanie zagrożeń i aktualnego stanu	+		+
Udostępnianie informacji	+		+
Pobieranie danych	+		+
Wykrywanie zagrożeń i otrzymywanie alertów	+		+
Monitoring niezbędnych zasobów	+		+
Identyfikacja zagrożeń	+		+
Poszukiwanie poszkodowanych	+		
Sprawdzanie statusu siec np. energetycznej	+		
Sprawdzanie parametrów życiowych	+		
Wysyłanie alertów	+	+	+
Odbieranie alertów	+	+	+
Sztuczna inteligencja			
Robotyka(operacje ratowniczo-poszukiwawcze)	+		
Wymiana informacji	+	+	+
Pobieranie danych	+	+	+
Symulowanie zagrożeń	+	+	+
Tworzenie Chatbotów	+	+	+
Chatboty	+	+	+
VR/AR			
Symulowanie realistycznych zagrożeń	+	+	+
Tworzenie zagrożeń w wirtualnym środowisku zbliżonych do tych w świecie rzeczywistym	+	+	+
Tworzenie realistycznych szkoleń dla służb ratowniczych	+	+	+
Wyświetlanie nazw ulic, śledzenie służb ratowniczych	+		
Komunikacja głosowa	+	+	+
Lokalizacja punktów strategicznych (linie energetyczne, gazowe itp.) oraz ofiar	+		
Nanoszenie obrazów 3D na rzeczywiste środowisko	+		+
Cloud Computing			
Hosting w chmurze	+		+
Dostęp do zasobów za pośrednictwem Internetu	+	+	+
Komunikacja z dowolnego miejsca	+	+	+
Komunikacja za pośrednictwem dowolnego urządzenia mobilnego (telefon, tablet, komputer)	+	+	+
Dostęp przez Internet do współdzielonej puli zasobów obliczeniowych	+	+	+
Blockchain			
Współpraca między interesariuszami zaangażowanymi w proces reagowania na katastrofy	+		+
Identyfikacja poszkodowanych i zmarłych	+	+	
Weryfikacja tożsamości	+	+	
Szyfrowanie danych	+		+
Rejestracja wolontariuszy	+		
Śledzenie dostaw	+		

Systemy informacji geoprzestrzennej			
Wizualizacja danych		+	+
Analiza danych	+	+	+
Pobieranie danych	+	+	+
Ocena ryzyka	+	+	+
Opracowanie strategii analizy ryzyka	+	+	+
Lokalizowanie ważnych punktów np. szpital, komisariat policji itp. Za pomocą zapytań *SQL*	+		
Szacowanie szkód	+	+	+
Ocena wpływu zagrożenia na funkcjonowanie państwa i obywateli	+	+	+
Identyfikacja dróg ewakuacyjnych	+		
Tworzenie planów odbudowy	+		+
Odbieranie alertów	+	+	+
Analiza danych historycznych	+	+	+
Opracowanie scenariuszy sytuacji kryzysowych	+	+	+
Analiza skutków zagrożenia	+	+	+
Planowanie przyszłych działań	+		+
Zobrazowanie sytuacji kryzysowej	+	+	+
OLAP			
Analiza danych	+	+	+
Przechowywanie danych			+
Eksploracja danych			+
Tworzenie raportów			+
Zobrazowanie danych		+	+
OLTP			
Współbieżność	+	+	+
Indeksowanie zbiorów danych	+	+	+
Pobieranie danych	+		+
Wyszukiwania i zapytania w bazie danych	+		+
Tworzenie kopii zapasowych	+	+	+
Monitorowanie sytuacji kryzysowych	+	+	+
Zabezpieczenie danych	+		+
Monitorowanie danych	+	+	+
Raportowanie i wsparcie procesów decyzyjnych	+	+	+
Business Inteligence			
Analiza danych	+	+	+
Kontrola dostępu do danych	+		
Raportowanie i wizualizacja danych	+	+	+
Monitorowanie zagrożeń	+		+
Podejmowanie decyzji	+	+	+
Przetwarzanie danych	+	+	+
Wymiana informacji	+	+	+
Analiza danych historycznych	+	+	+
Filtrowanie, sortowanie i grupowanie danych	+	+	+
Big Data			
Identyfikacja i śledzenie populacji	+		+
Mapowanie sytuacji kryzysowych	+		
Gromadzenie danych i modelowanie scenariuszy zagrożeń	+		+
Lokalizacja zasobów	+		+
Wysyłanie informacji o zagrożeniach	+		
Analiza danych	+		+
Planowanie przyszłych działań	+		+

TECHNOLOGIE \ POZIOMY ŚWIADOMOŚCI SYTUACYJNEJ	POSTRZEGANIE	ZROZUMIENIE	PROJEKCJA
Klasyczny telefon komórkowy - komunikaty o zagrożeniach			
Alerty o zagrożeniach np. RCB	+	+	+
Strony internetowe (portale społecznościowe, wyszukiwanie informacji o zagrożeniach)			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami	+	+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej	+	+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach	+	+	+
Informacje o zagrożeniach za pośrednictwem poczty (list, telegram)			
Wiadomości tekstowe na temat zagrożeń			+
Poradniki w wersji papierowej			
Informacje o zagrożeniach	+	+	+
Informacje na temat zachowania się w sytuacjach kryzysowych	+	+	+
Szkolenia			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+
Konferencje			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+
Syreny alarmowe			
Analiza zagrożenia	+	+	+
Środki masowego przekazu (radio, telewizja)			
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Informacje na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+

TECHNOLOGIE \ POZIOMY ŚWIADOMOŚCI SYTUACYJNEJ	POSTRZEGANIE	ZROZUMIENIE	PROJEKCJA
IoT/IoE			
Monitorowanie zagrożeń i aktualnego stanu	+	+	+
Udostępnianie informacji		+	+
Pobieranie danych	+	+	+
Wykrywanie zagrożeń i otrzymywanie alertów	+	+	+
Identyfikacja zagrożeń	+	+	+
Sprawdzanie statusu siec np. energetycznej	+	+	+
Smartfon - komunikaty o zagrożeniach			
Alerty o zagrożeniach np. RCB	+	+	+
Alerty o zagrożeniach np. wiadomości z komunikatorów		+	+
Alerty o zagrożeniach np. wiadomości ze stron internetowych	+	+	+
Alerty o zagrożeniach np. wiadomości ze stron internetowych np. połą-czenia telefoniczne	+	+	+
Alerty o zagrożeniach z urządzeń *IoT/IoE* np. czujniki poziomu wody	+	+	+
Sztuczna inteligencja - chatboty			
Uzyskiwanie odpowiedzi na pytania związane z zagrożeniami		+	+
Analiza konkretnej sytuacji kryzysowej		+	+
Pytania odnośnie pomocy w momencie wystąpienia sytuacji kryzysowej		+	+
Uzyskiwanie szczegółowych informacji o zagrożeniach		+	+
Media społecznościowe			
Informacje o zagrożeniach za pośrednictwem mediów społecznościowych - posty	+	+	+
Informacje o zagrożeniach za pośrednictwem mediów społecznościowych – prywatne wiadomości	+	+	+
Informacje o zagrożeniach za pośrednictwem audycji wideo (youtube.pl, wykop.pl itp.)	+	+	+
Informacje o zagrożeniach na ekranach wielkoformatowych			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo -graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+
Informacje o zagrożeniach za pośrednictwem poczty e-mail			
Wiadomości na temat zagrożeń	+	+	+
Komunikaty na temat zagrożeń	+	+	+
Informacje o zagrożeniach w środkach transportu			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo -graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+
Informacje o zagrożeniach w miejscach publicznych			
Alerty RCB	+	+	+
Reklamy o zagrożeniach (klęski żywiołowe, wypadki drogowe itp.)	+	+	+
Wiadomości tekstowo -graficzne na temat zagrożeń	+	+	+
Poradniki na temat zachowania się w sytuacjach kryzysowych	+	+	+