dr Marek Ciekanowski
Społeczna Akademia Nauk w Warszawie
ORCID: 0009-0009-1271-0652

dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

mgr Weronika Parczewska
Wojskowa Akademia Techniczna w Warszawie
ORCID: 0000-0001-8991-4068

https://doi.org/10.29316/9788368103205_8

BEZPIECZEŃSTWO TELEINFORMATYCZNE W ZARZĄDZANIU KRYZYSOWYM

ICT SECURITY IN CRISIS MANAGEMENT

Streszczenie

Celem rozdziału jest analiza znaczenia bezpieczeństwa systemów teleinformatycznych w zarządzaniu kryzysowym oraz identyfikacja głównych zagrożeń i skutecznych strategii ochrony. W pierwszej części rozdziału opisano rolę systemów teleinformatycznych w zarządzaniu kryzysowym, podkreślając ich znaczenie dla komunikacji, analizy danych i podejmowania decyzji. Druga część przedstawia główne zagrożenia i wyzwania,

Summary

The aim of the chapter is to analyze the importance of ICT systems security in crisis management and to identify the main threats and effective protection strategies. The first part of the chapter describes the role of ICT systems in crisis management, emphasizing their importance for communication, data analysis and decision-making. The second part presents the main threats and challenges, such as cyberattacks, technical failures and

takie jak cyberataki, awarie techniczne i dezinformacja. Trzecia część koncentruje się na najlepszych praktykach i strategiach zabezpieczeń, wskazując na znaczenie szyfrowania danych, systemów wykrywania zagrożeń, redundancji infrastruktury oraz szkoleń personelu. Problem badawczy sformułowano: Jakie są kluczowe zagrożenia dla systemów teleinformatycznych w zarządzaniu kryzysowym i jakie środki mogą zwiększyć ich odporność? W badaniu wykorzystano metody teoretyczne, takie jak analiza literatury naukowej, przegląd norm i regulacji dotyczących cyberbezpieczeństwa oraz studia przypadków dotyczące incydentów naruszenia bezpieczeństwa systemów teleinformatycznych w zarządzaniu kryzysowym.

Słowa kluczowe: zarządzanie kryzysowe, bezpieczeństwo teleinformatyczne, cyberzagrożenia, strategie ochrony

disinformation. The third part focuses on security best practices and strategies, highlighting the importance of data encryption, threat detection systems, infrastructure redundancy, and staff training. The research problem was formulated: What are the key threats to ICT systems in crisis management and what measures can increase their resilience? The study used theoretical methods such as an analysis of the scientific literature, a review of cybersecurity standards and regulations, and case studies on ICT security incidents in crisis management.

Keywords: crisis management, ICT security, cyber threats, protection strategies

Wstęp

Współczesne zarządzanie kryzysowe w dużym stopniu opiera się na wykorzystaniu nowoczesnych systemów teleinformatycznych, które umożliwiają sprawną komunikację, gromadzenie i analizę danych oraz podejmowanie szybkich decyzji w sytuacjach zagrożenia. Od niezawodności i bezpieczeństwa tych systemów zależy skuteczność działań podejmowanych przez służby ratunkowe, administrację publiczną oraz inne podmioty odpowiedzialne za minimalizowanie skutków katastrof i kryzysów.

Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym obejmuje szeroki zakres zagadnień, w tym ochronę przed cyberatakami, odporność na awarie techniczne, zapewnienie ciągłości działania oraz zabezpieczenie integralności i poufności informacji. W dobie rosnących zagrożeń cybernetycznych oraz coraz większej zależności od technologii cyfrowych, kluczowe staje się opracowanie skutecznych strategii i narzędzi zapewniających bezpieczeństwo infrastruktur krytycznych oraz systemów wspomagających podejmowanie decyzji.

Celem niniejszego rozdziału jest analiza kluczowych aspektów związanych z bezpieczeństwem systemów teleinformatycznych w kontekście zarządzania kryzysowego. Przedstawione zostaną zagrożenia, wyzwania oraz najlepsze praktyki w zakresie ochrony tych systemów, ze szczególnym uwzględnieniem technologii wykorzystywanych w instytucjach odpowiedzialnych za reagowanie na sytuacje kryzysowe.

Zagrożenia i wyzwania dla bezpieczeństwa systemów teleinformatycznych

Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym wiąże się z wieloma zagrożeniami, które mogą znacząco wpłynąć na ich funkcjonowanie i skuteczność podejmowanych działań. Jednym z kluczowych zagrożeń są cyberataki, obejmujące m.in. ataki typu DDoS (Distributed Denial of Service), próby przejęcia kontroli nad systemami, złośliwe oprogramowanie oraz phishing skierowany do pracowników instytucji zarządzających kryzysowo. Ataki te mogą prowadzić do zakłócenia działania systemów, wycieku poufnych informacji, a nawet przejęcia infrastruktury przez podmioty nieuprawnione[1]. Ataki DDoS wykorzystują słabość architektury TCP/IP oraz serwerów DNS umożliwiającą przeciążenie zasobów systemowych sztucznie wygenerowanym ruchem sieciowym[2]. Przeprowadzenie tego typu ataku wymaga zaangażowania znacznych zasobów sprzętowych. Jako że mało kto dysponuje własnym rozbudowanym centrum obsługi danych, osoby przeprowadzające ataki DDoS wykorzystują w tym celu systemy komputerowe, nad którymi przejmują kontrolę za pomocą szkodliwego oprogramowania[3].

Phishing również stanowi jedno z najpoważniejszych zagrożeń dla systemów teleinformatycznych[4], a jego wpływ na zarządzanie kryzysowe może być katastrofalny. Ataki phishingowe, polegające na podszywaniu się pod

[1] E. Niewiadomska-Szynkiewicz, R. Litka, *Ataki na urządzenia mobilne i metody ich wykrywania*, Cybersecurity and Law, nr 1(9), 2023, s. 91.

[2] Ł. Apiecionek, *Fuzzy Observation of DDoS Attack,* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor* , W. Kosiński, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017, s. 240.

[3] I. Protasowicki, *Wpływ zagrożenia atakami DOS/DDOS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej*, Modern Management Review, vol. XXIII, 25 (1/2018), 2018, s. 134.

[4] S. Grzebielec, *Analiza podatności użytkowników systemów informatycznych na atak phishingowy*, Journal of Computer Sciences Institute, vol. 15, 2020, s. 164.

zaufane instytucje lub osoby w celu wyłudzenia danych uwierzytelniających, mogą prowadzić do przejęcia kontroli nad systemami, wycieku poufnych informacji oraz zakłócenia koordynacji działań w sytuacjach kryzysowych. Ataki phishingowe często prowadzą do przejęcia danych logowania do systemów zarządzania kryzysowego. Cyberprzestępcy mogą w ten sposób uzyskać dostęp do baz danych, narzędzi monitorujących czy systemów komunikacyjnych wykorzystywanych przez służby ratunkowe. W efekcie może dojść do paraliżu operacyjnego, opóźnień w reakcji na zagrożenia oraz dezinformacji, co zwiększa ryzyko strat ludzkich i materialnych. Phishing może być wykorzystywany do rozpowszechniania fałszywych informacji w celu wywołania paniki lub skierowania działań kryzysowych w niewłaściwym kierunku. Atakujący, przejmując dostęp do oficjalnych kanałów komunikacyjnych, mogą rozsyłać fałszywe ostrzeżenia, podawać błędne instrukcje lub publikować zmanipulowane dane, co prowadzi do chaosu i dezinformacji wśród ludności oraz służb ratunkowych.

Systemy teleinformatyczne w zarządzaniu kryzysowym przechowują wrażliwe informacje, takie jak plany ewakuacyjne, dane osobowe ofiar, szczegóły dotyczące zagrożeń czy taktyki działań ratowniczych. Phishing umożliwia cyberprzestępcom uzyskanie dostępu do tych informacji i ich nieautoryzowane wykorzystanie, co może skutkować szantażem, sprzedażą danych lub wykorzystaniem ich do dalszych ataków na infrastrukturę krytyczną.

Ataki phishingowe mogą również wpływać na łańcuchy dostaw i logistykę w zarządzaniu kryzysowym. Oszuści mogą podszywać się pod dostawców sprzętu medycznego, organizacje humanitarne czy instytucje rządowe, wprowadzając fałszywe zamówienia, przekierowując zasoby w niewłaściwe miejsca lub manipulując procesami zaopatrzenia. Takie działania prowadzą do opóźnień w dostarczaniu niezbędnej pomocy i osłabiają skuteczność operacji kryzysowych.

Kolejnym wyzwaniem są awarie techniczne[5], które mogą wynikać zarówno z błędów w oprogramowaniu, jak i problemów sprzętowych. Wysoka niezawodność systemów teleinformatycznych jest kluczowa, zwłaszcza w sytuacjach kryzysowych, gdzie każda przerwa w dostępie do informacji może prowadzić do opóźnień w reagowaniu i zwiększenia strat. W szczegól-

[5] M. Elszkowski, *Działalność Policji w sytuacjach kryzysowych. Podejście formalne*, Zeszyty Naukowe SGSP, Nr 61(2), 2017, s. 95.

ności zagrożeniem są awarie sieci telekomunikacyjnych, utrata zasilania oraz uszkodzenia infrastruktury IT na skutek klęsk żywiołowych, aktów sabotażu lub błędów ludzkich[6].

Dodatkowym ryzykiem jest manipulacja danymi oraz dezinformacja, które mogą prowadzić do podejmowania błędnych decyzji w sytuacjach kryzysowych[7]. Ataki na integralność danych, np. fałszowanie informacji dotyczących zagrożeń, mogą skutkować nieprawidłowym rozmieszczeniem zasobów i opóźnieniem działań ratunkowych.

Dezinformacja stanowi jedno z najpoważniejszych wyzwań w zarządzaniu kryzysowym, wpływając na procesy decyzyjne, reakcję społeczeństwa oraz skuteczność działań instytucji odpowiedzialnych za bezpieczeństwo i porządek publiczny. W dobie powszechnego dostępu do informacji i mediów społecznościowych dezinformacja może szybko eskalować, prowadząc do chaosu, paniki oraz podważania zaufania do organów państwowych. Dezinformacja w zarządzaniu kryzysowym może pochodzić z różnych źródeł, w tym:

- aktorów państwowych prowadzących działania hybrydowe,
- grup ekstremistycznych i terrorystycznych,
- osób prywatnych, które nieświadomie rozpowszechniają fałszywe informacje,
- mediów społecznościowych, które ułatwiają szybkie rozprzestrzenianie się fake newsów.

Dezinformacja stanowi istotne zagrożenie w zarządzaniu kryzysowym, mogąc prowadzić do chaosu i utraty zaufania do instytucji publicznych. Kluczowe znaczenie mają skuteczne strategie komunikacyjne, monitorowanie źródeł dezinformacji oraz edukacja społeczeństwa, które mogą ograniczyć negatywne skutki manipulacji informacyjnej w sytuacjach kryzysowych. Dezinformacja może znacząco utrudnić skuteczne zarządzanie kryzysowe, prowadząc do:

- opóźnień w podejmowaniu decyzji,
- spadku zaufania do instytucji publicznych,
- rozprzestrzeniania się paniki i chaosu społecznego,
- błędnych alokacji zasobów, gdy służby reagują na fałszywe informacje.

[6] M. Witkowski, *Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym*, Zeszyty Naukowe WSOWL, nr 4(162), 2011, s. 83.

[7] J. Pyka, *Komunikacja w zarządzaniu kryzysowym – problemy i wyzwania*, Zeszyty Naukowe Akademii Górnośląskiej, Nr 7, 2023, s. 127.

Klasyczne reakcje systemów zabezpieczeń w produkcyjnych systemach teleinformatycznych zmierzają do jak najszybszego zablokowania możliwości oddziaływania zdalnego napastnika na atakowane zasoby[8]. Rosnąca liczba zagrożeń cybernetycznych oraz rosnąca zależność od technologii cyfrowych sprawiają, że kluczowe staje się wdrażanie skutecznych środków ochrony. Niezbędne są zaawansowane systemy monitorowania, wykrywania zagrożeń, mechanizmy redundancji infrastruktury oraz procedury zapewniające ciągłość działania. Odpowiednia polityka bezpieczeństwa i szkolenie personelu to kolejne istotne elementy minimalizowania ryzyka w zarządzaniu kryzysowym.

Rola systemów teleinformatycznych w zarządzaniu kryzysowym

Współczesne zarządzanie kryzysowe w dużym stopniu opiera się na zaawansowanych systemach teleinformatycznych, które odgrywają kluczową rolę w zapewnieniu sprawnej komunikacji, gromadzenia i analizy danych oraz podejmowania szybkich i trafnych decyzji w sytuacjach nadzwyczajnych. Systemy te umożliwiają integrację informacji z różnych źródeł, co pozwala na kompleksową ocenę zagrożeń i skuteczniejsze zarządzanie zasobami.

Jednym z podstawowych zadań systemów teleinformatycznych jest zapewnienie niezawodnej komunikacji między służbami ratunkowymi, administracją publiczną oraz innymi podmiotami zaangażowanymi w działania kryzysowe. Dzięki nowoczesnym technologiom, takim jak sieci radiowe, systemy łączności satelitarnej czy platformy wymiany danych w czasie rzeczywistym, możliwe jest szybkie przekazywanie kluczowych informacji oraz koordynacja działań w terenie. Na rysunku poniżej przedstawiono sieci i systemy teleinformatyczne wykorzystywane na potrzeby systemu kierowania bezpieczeństwem państwa.

[8] A. Patkowski, *„Cicha reakcja" na zdalne ataki teleinformatyczne*, Przegląd Teleinformatyczny, T. 5, nr 3(44), 2017, s. 38.



Rysunek 1. Sieci i systemy teleinformatyczne wykorzystywane na potrzeby systemu kierowania bezpieczeństwem państwa

Źródło: G. Michalewski, M. Witkowski, R*ola sieci i systemów teleinformatycznych w procesie podejmowania decyzji w sytuacjach kryzysowych*, Rocznik Kolegium Analiz Ekonomicznych, nr 49, 2018, s. 325.

Ponadto systemy teleinformatyczne wspomagają proces decyzyjny poprzez analizę dużych zbiorów danych, prognozowanie zagrożeń oraz modelowanie scenariuszy kryzysowych. Narzędzia oparte na sztucznej inteligencji i analizie Big Data pozwalają na skuteczniejsze przewidywanie sytuacji kryzysowych, co umożliwia odpowiednie przygotowanie i minimalizację strat. Właściwie zaprojektowany i funkcjonujący system obiegu informacji w procesie podejmowania decyzji w sytuacjach kryzysowych powinien pozwalać na:

- monitorowanie sytuacji bezpieczeństwa;
- ostrzeganie (system alarmowania i ostrzegania) – prognozowanie zagrożeń i rozwoju sytuacji,
- podejmowanie decyzji,
- opracowanie niezbędnych dokumentów (plany działania, rozkazu, dyrektywy),
- reagowanie na sytuacje kryzysowe (wypadki, siły szybkiego reagowania (QRF) itp.),
- podejmowanie działań (ratowniczych itp.),
- wprowadzanie korekt w działaniu (decyzjach),
- aktualizację i modyfikację planów,
- modyfikację procedur (system „Lessons Learned”14),

- bieżące zaspokajanie potrzeb materiałowych i zasobowych (logistyka), w celu utrzymywania żywotności i gotowości elementów wykonawczych systemu bezpieczeństwa do działania[9].

Współczesne zarządzanie kryzysowe opiera się na skutecznej koordynacji działań wielu podmiotów, takich jak administracja publiczna, służby ratownicze oraz siły zbrojne. Kluczową rolę w tym procesie odgrywają zaawansowane systemy teleinformatyczne, które umożliwiają sprawną wymianę informacji, monitorowanie sytuacji w czasie rzeczywistym oraz podejmowanie szybkich i trafnych decyzji.

Jednym z przykładów systemów wspierających zarządzanie kryzysowe jest system Jaśmin, który znajduje zastosowanie zarówno w działaniach wojskowych, jak i cywilnych.

Systemy teleinformatyczne pozwalają na szybkie przekazywanie informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo, co umożliwia skuteczne reagowanie na sytuacje kryzysowe. Dzięki zdolności do przetwarzania ogromnych ilości danych w czasie rzeczywistym, wspierają one analizę zagrożeń oraz przewidywanie ich potencjalnych skutków. Narzędzia te pozwalają na monitorowanie kluczowych zasobów, takich jak pojazdy ratownicze, sprzęt czy infrastruktura krytyczna, co znacząco usprawnia zarządzanie operacyjne w trakcie sytuacji nadzwyczajnych.

System Jaśmin został opracowany jako kompleksowe rozwiązanie teleinformatyczne, które integruje dane z różnych źródeł i umożliwia ich wizualizację na interaktywnych mapach. Jego zastosowanie obejmuje zarówno działania wojskowe, jak i cywilne operacje ratunkowe, w tym zarządzanie klęskami żywiołowymi czy zagrożeniami terrorystycznymi. Wykorzystanie systemu pozwala na lepsze planowanie i realizację operacji dzięki zaawansowanym narzędziom do analizy danych i zarządzania logistyką[10]. Na poniższym rysunku przedstawiono struktury zarządzania kryzysowego w systemie Jaśmin.

[9] G. Michalewski, M. Witkowski, *Rola sieci i systemów teleinformatycznych w procesie podejmowania decyzji w sytuacjach kryzysowych*, Rocznik Kolegium Analiz Ekonomicznych, nr 49, 2018, s. 323.

[10] SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego – TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, [dostęp: 26.03.2025].



Rysunek 2. SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego

Źródło: SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego – TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, [dostęp: 26.03.2025].

Podczas katastrof naturalnych system Jaśmin wspierał działania służb ratowniczych, umożliwiając efektywne monitorowanie rozwoju sytuacji i koordynację pracy zespołów w terenie. W przypadku zagrożeń terrorystycznych pozwalał na szybką identyfikację ryzyka oraz organizację działań prewencyjnych[11]. Jego zastosowanie w operacjach wojskowych potwierdziło skuteczność w zakresie dowodzenia i zarządzania zasobami, co czyni go istotnym narzędziem także w ramach współpracy międzynarodowej, na przykład w strukturach NATO[12].

Systemy teleinformatyczne, takie jak Jaśmin, znacząco zwiększają efektywność zarządzania kryzysowego, pozwalając na skuteczniejsze reagowanie na sytuacje nadzwyczajne. Dzięki zdolności do integracji danych, monitorowania sytuacji w czasie rzeczywistym oraz wspomagania podejmowania decyzji, ich rola w zapewnianiu bezpieczeństwa publicznego jest nie do przecenienia. Dynamiczny rozwój technologii teleinformatycznych wskazuje na to, że w przyszłości ich zastosowanie w zarządzaniu kryzysowym będzie

[11] System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i--wsparciu-akcji-antykryzysowych, [dostęp: 26.03.2025].

[12] NATO CWIX 2023 – kolejny sukces systemu JAŚMIN, https://zbiam.pl/nato-cwix-2023-kolejny-sukces-systemu-jasmin/, [dostęp: 26.03.2025].

jeszcze szersze, co wpłynie na dalszą poprawę skuteczności działań ratowniczych i operacyjnych.

Niezawodność i efektywność systemów teleinformatycznych mają zatem kluczowe znaczenie dla skutecznego zarządzania kryzysowego. Ich rozwój i doskonalenie stanowią istotny element polityki bezpieczeństwa, ponieważ w sytuacjach zagrożenia każda sekunda ma znaczenie, a sprawny przepływ informacji może decydować o powodzeniu działań ratunkowych i ochronie ludności.

Najlepsze praktyki i strategie zabezpieczeń

W celu zwiększenia odporności systemów teleinformatycznych na zagrożenia kluczowe jest wdrażanie nowoczesnych metod ochrony, które minimalizują ryzyko cyberataków, awarii oraz utraty integralności danych. Jednym z podstawowych środków zabezpieczeń jest szyfrowanie danych, które zapewnia poufność informacji i chroni je przed nieautoryzowanym dostępem. Stosowanie silnych algorytmów kryptograficznych w komunikacji i przechowywaniu danych znacząco utrudnia przechwycenie lub manipulację informacjami.

Kolejnym istotnym elementem ochrony są systemy wykrywania i zapobiegania zagrożeniom (IDS/IPS – Intrusion Detection/Prevention Systems), które monitorują ruch sieciowy i automatycznie reagują na podejrzane aktywności[13]. W połączeniu z analizą behawioralną i sztuczną inteligencją systemy te pozwalają na wczesne wykrywanie ataków oraz podejmowanie działań zapobiegawczych.

Strategie zabezpieczeń w kontekście sztucznej inteligencji (AI) w zarządzaniu kryzysowym odgrywają kluczową rolę w zapewnieniu bezpieczeństwa zarówno samych systemów teleinformatycznych, jak i danych, które są zbierane i przetwarzane w czasie rzeczywistym. W przypadku kryzysów, szczególnie takich o charakterze międzynarodowym, terrorystycznym czy związanym z katastrofami naturalnymi, informacje przekazywane między służbami ratunkowymi, administracją publiczną i obywatelami muszą być nie tylko dokładne, ale również chronione przed nieautoryzowanym dostępem, manipulacjami czy atakami cybernetycznymi.

[13] M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, Studia i Materiały Informatyki Stosowanej, nr 7, 2012, s. 166.

Pierwszym aspektem strategii zabezpieczeń jest zapewnienie integralności danych. W sytuacjach kryzysowych, gdzie dane pochodzą z różnych źródeł – takich jak drony, czujniki, media społecznościowe, czy systemy monitoringu – istotne jest, aby były one wiarygodne i nie zostały zmienione. AI odgrywa tutaj rolę w szyfrowaniu przesyłanych informacji, stosowaniu metod detekcji anomalii w danych oraz weryfikacji ich autentyczności[14]. Zabezpieczenie tych informacji przed złośliwymi atakami czy manipulacjami jest podstawą do podejmowania właściwych decyzji, które mogą mieć krytyczne znaczenie dla życia i zdrowia ludzi.

W kontekście prywatności danych, szczególnie gdy wykorzystuje się AI do analizy danych osobowych, takich jak lokalizacje użytkowników czy informacje o zdrowiu, niezbędne jest stosowanie odpowiednich regulacji i technologii ochrony prywatności. W tym przypadku chodzi o zastosowanie zaawansowanych metod szyfrowania danych, anonimizacji, a także zapewnienia, że dostęp do wrażliwych informacji będzie możliwy tylko dla uprawnionych osób, zgodnie z obowiązującymi przepisami prawa, takimi jak RODO w Unii Europejskiej.

Wyzwanie stanowi również ochrona przed cyberatakami, które mogą mieć na celu zakłócenie działania systemów zarządzania kryzysowego. W tym kontekście, systemy AI muszą być wyposażone w mechanizmy wykrywania prób nieautoryzowanego dostępu, takich jak ataki DDoS (rozproszona odmowa usługi) czy złośliwe oprogramowanie, które mogłyby sparaliżować funkcjonowanie całych sieci zarządzania kryzysowego. Odpowiednia detekcja takich zagrożeń w czasie rzeczywistym, a także szybka reakcja na nie, są kluczowe dla utrzymania stabilności i bezpieczeństwa systemów teleinformatycznych.

Kolejnym aspektem zabezpieczeń jest właściwe zarządzanie dostępem do systemów AI. W sytuacjach kryzysowych, dostęp do systemów zarządzania kryzysowego i platform AI powinien być ściśle kontrolowany i ograniczony do osób posiadających odpowiednie uprawnienia. Zastosowanie rozwiązań, takich jak autentykacja dwuskładnikowa (2FA) czy biometria, które zapewniają dodatkową warstwę ochrony, jest niezbędne, by zapobiec nieuprawnionemu dostępowi do wrażliwych informacji.

[14] K. Sienkiewicz-Małyjurek, *Możliwości i problemy zastosowania sztucznej inteligencji w zarządzaniu kryzysowym*, Bezpieczeństwo. Teoria i Praktyka, 1, 2024, s. 53.

Aby zapewnić ciągłość działania systemów, niezbędne jest także posiadanie rozwiązań awaryjnych i planów odzyskiwania danych w razie awarii systemów. Systemy AI wykorzystywane w zarządzaniu kryzysowym muszą być odporne na różne scenariusze awaryjne, takie jak przerwy w dostępie do sieci czy uszkodzenia infrastruktury[15]. Zapewne AI będzie też wspierać działania na rzecz sprawniejszego zarządzania infrastrukturą krytyczną i ogólnie usługami użyteczności publicznej, co obecnie jest skomplikowane i czasochłonne[16].

Zastosowanie redundancji systemów, zasilania awaryjnego oraz procedur na wypadek awarii pozwala na szybkie przywrócenie pełnej funkcjonalności systemu, co ma kluczowe znaczenie w sytuacjach kryzysowych.

Ostatecznie, strategia zabezpieczeń w kontekście AI w zarządzaniu kryzysowym wymaga nie tylko technologicznych rozwiązań, ale także odpowiednich regulacji i procedur w zakresie ochrony danych, zarządzania dostępem oraz reagowania na zagrożenia[17]. Skuteczna integracja sztucznej inteligencji z systemami kryzysowymi, przy jednoczesnym zapewnieniu najwyższych standardów bezpieczeństwa, pozwala na optymalne wykorzystanie potencjału AI w zarządzaniu kryzysowym, przy minimalizacji ryzyk związanych z cyberzagrożeniami. Ważnym aspektem jest również redundancja infrastruktury, czyli zastosowanie zapasowych systemów, serwerów i połączeń sieciowych. Rozwiązania, takie jak rozproszone centra danych, systemy automatycznego przełączania oraz backupy w chmurze, zapewniają ciągłość działania nawet w przypadku awarii lub ataku cybernetycznego.

Nieodzownym elementem skutecznej strategii bezpieczeństwa jest także rozwój procedur reagowania na incydenty. Opracowanie i regularne testowanie planów awaryjnych pozwalają na szybkie i skuteczne reagowanie na zagrożenia, minimalizując negatywne skutki ataków lub awarii technicznych[18]. Ich

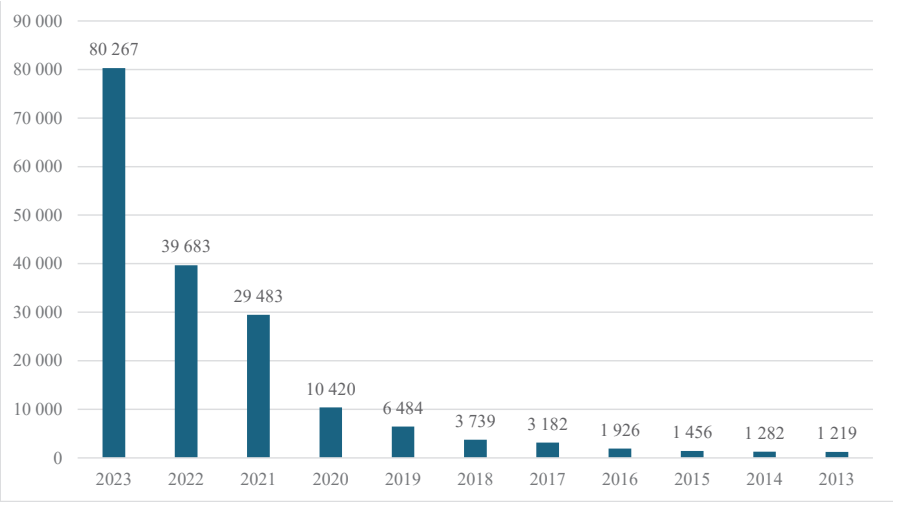
[15] W. Krasiński, *Sztuczna inteligencja w ochronie ludności w Polsce – możliwości i perspektywy wykorzystania*, DOCTRINA.Studia Społeczno-Polityczne, 21, 2024, s. 34.

[16] T. Michalak, *Sztuczna inteligencja i ochrona infrastruktury krytycznej*. „AI to broń obosieczna" (wywiad przeprowadzony przez M. Górskiego), https://cyberdefence24.pl/cybermagazyn/cybermagazyn-sztucznainteligencja-i-ochrona-infrastruktury-krytycznej-ai-to-bron-obosieczna, [dostęp: 26.03.2025].

[17] A. Manoj, A. Shweta, *A systematic review on artificial intelligence/deep learning applications and challenges to battle against covid-19 pandemic*, Disaster Advances 2021, vol. 14, nr 8, s. 90.

[18] P. Gibuła, *Działania na rzecz bezpieczeństwa teleinformatycznego Polski. Niebezpieczna cyberprzestrzeń*, Kontrola Państwowa, 4(369), 2016, s. 630.

liczba z roku na rok drastycznie wzrasta. Ilość incydentów obsłużonych przez CISIRT NAKS w latach 2013-2023 przestawiono na poniższym rysunku.



Rysunek 3. Zestawienie liczby obsłużonych incydentów przez CERT Polska w latach 2013-2023

Źródło: Raport roczny z działalności CERT POLSKA 2023.

Oprócz technologicznych środków ochrony kluczowe znaczenie ma szkolenie personelu oraz wdrażanie odpowiednich polityk bezpieczeństwa. Ludzki błąd jest jednym z najczęstszych powodów naruszeń systemów teleinformatycznych, dlatego edukacja pracowników w zakresie rozpoznawania zagrożeń, stosowania zasad cyberhigieny oraz przestrzegania procedur bezpieczeństwa jest niezbędna. Rozwiązania edukacyjne oraz konsekwentnie wdrażane rozwiązania i aplikacje, metody i sposoby ochrony informacji, mogą poprawić istniejący stan bezpieczeństwa informacji, co sprzyja skutecznej ochronie informacji w cyberprzestrzeni[19] również w odniesieniu do zarządzania kryzysowego.

Dynamicznie zmieniające się środowisko zagrożeń wymaga ciągłego doskonalenia strategii zabezpieczeń oraz dostosowywania ich do nowych wyzwań. Systematyczne audyty, testy penetracyjne oraz aktualizacje oprogramowania stanowią kluczowe elementy długoterminowej polityki bezpieczeństwa, która zapewnia stabilność i niezawodność systemów teleinformatycznych wykorzystywanych w zarządzaniu kryzysowym.

[19] M. Kowalewski, *Problemy i potrzeby kształcenia w zakresie bezpieczeństwa informacji i systemów teleinformatycznych*, Obronność. Zeszyty Naukowe, 4(28), 2018, s. 119.

Podsumowanie

Bezpieczeństwo systemów teleinformatycznych odgrywa kluczową rolę w skutecznym zarządzaniu kryzysowym. Współczesne technologie umożliwiają szybkie gromadzenie i analizę danych, efektywną komunikację oraz podejmowanie trafnych decyzji w sytuacjach nadzwyczajnych. Jednak ich rosnąca zależność od technologii cyfrowych niesie ze sobą również poważne zagrożenia, takie jak cyberataki, awarie techniczne czy dezinformacja. W szczególności phishing stanowi jedno z najpoważniejszych wyzwań, mogąc prowadzić do utraty dostępu do kluczowych systemów, naruszenia poufności danych oraz dezorganizacji działań kryzysowych.

Analiza zagrożeń i najlepszych praktyk w zakresie ochrony systemów teleinformatycznych wskazuje na konieczność wdrażania wielopoziomowych mechanizmów bezpieczeństwa, takich jak szyfrowanie danych, systemy wykrywania zagrożeń, redundancja infrastruktury oraz procedury reagowania na incydenty. Niezwykle istotne jest również regularne szkolenie personelu, ponieważ czynniki ludzkie nadal pozostają jednym z najsłabszych ogniw w systemach zabezpieczeń.

Wnioski płynące z niniejszej analizy podkreślają, że zapewnienie bezpieczeństwa systemów teleinformatycznych wymaga podejścia kompleksowego i dynamicznego. Zagrożenia cybernetyczne ewoluują w szybkim tempie, co oznacza, że również strategie obronne muszą być stale aktualizowane i dostosowywane do nowych wyzwań. Kluczowe znaczenie ma tu współpraca między instytucjami odpowiedzialnymi za zarządzanie kryzysowe, sektorem IT oraz ekspertami ds. cyberbezpieczeństwa.

Dalsze badania w tym obszarze powinny koncentrować się na opracowywaniu bardziej zaawansowanych metod wykrywania i neutralizacji zagrożeń cybernetycznych w czasie rzeczywistym. Szczególnie istotne jest rozwijanie technologii sztucznej inteligencji i uczenia maszynowego, które mogą automatycznie analizować anomalie w systemach teleinformatycznych i skutecznie identyfikować potencjalne ataki. Ponadto warto prowadzić badania nad odpornością systemów zarządzania kryzysowego na ataki socjotechniczne, a także doskonalić metody edukacji i szkolenia personelu w zakresie cyberhigieny i reagowania na incydenty.

Ostatecznie, bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym nie jest jednorazowym działaniem, lecz ciągłym procesem

wymagającym zaangażowania, innowacyjnych rozwiązań oraz współpracy między różnymi sektorami. Skuteczna ochrona tych systemów jest niezbędna do zapewnienia stabilności i bezpieczeństwa społeczeństwa w obliczu różnorodnych zagrożeń.

Literatura

1. Apiecionek Ł., *Fuzzy Observation of DDoS Attack,* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor*, W. Kosiński, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017.
2. Elszkowski M., *Działalność Policji w sytuacjach kryzysowych. Podejście formalne*, Zeszyty Naukowe SGSP, Nr 61 (tom 2)/1, 2017.
3. Gibuła P., *Działania na rzecz bezpieczeństwa teleinformatycznego Polski. Niebezpieczna cyberprzestrzeń*, Kontrola Państwowa, 4(369), 2016.
4. Grzebielec S., *Analiza podatności użytkowników systemów informatycznych na atak phishingowy*, Journal of Computer Sciences Institute, vol. 15, 2020.
5. Krasiński W., *Sztuczna inteligencja w ochronie ludności w Polsce – możliwości i perspektywy wykorzystania*, DOCTRINA.Studia Społeczno-Polityczne, 21, 2024.
6. Kowalewski M., *Problemy i potrzeby kształcenia w zakresie bezpieczeństwa informacji i systemów teleinformatycznych*, Obronność. Zeszyty Naukowe, 4(28), 2018.
7. Manoj A., Shweta A., *A systematic review on artificial intelligence/deep learning applications and challenges to battle against covid-19 pandemic*, Disaster Advances 2021, vol. 14, nr 8.
8. Michalak T., *Sztuczna inteligencja i ochrona infrastruktury krytycznej. „AI to broń obosieczna"* (wywiad przeprowadzony przez M. Górskiego), https://cyberdefence24.pl/cybermagazyn/cybermagazyn-sztuczna-inteligencja-i-ochrona-infrastruktury
9. NATO CWIX 2023 - kolejny sukces systemu JAŚMIN, https://zbiam.pl/nato-cwix-2023-kolejny-sukces-systemu-jasmin/
10. Niewiadomska-Szynkiewicz E., Litka R., *Ataki na urządzenia mobilne i metody ich wykrywania*, Cybersecurity and Law, nr 1(9), 2023.
11. Patkowski A., „*Cicha reakcja" na zdalne ataki teleinformatyczne*, Przegląd Teleinformatyczny, T. 5, nr 3(44), 2017.
12. Protasowicki I., *Wpływ zagrożenia atakami DOS/DDOS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej*, Modern Management Review, vol. XXIII, 25(1), 2018.
13. Pyka J., *Komunikacja w zarządzaniu kryzysowym – problemy i wyzwania*, Zeszyty Naukowe Akademii Górnośląskiej, Nr 7/2023, s. 127.
14. SZK JAŚMIN - Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego - TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html

15. System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych
16. Sienkiewicz-Małyjurek K., *Możliwości i problemy zastosowania sztucznej inteligencji w zarządzaniu kryzysowym*, Bezpieczeństwo. Teoria i Praktyka, 1, 2024.
17. Witkowski M., *Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym*, Zeszyty Naukowe WSOWL, nr 4(162), 2011.
18. Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, Studia i Materiały Informatyki Stosowanej, nr 7, 2012.