Sławomir Żurawski[1]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

https://doi.org/10.29316/9788368103359_3

ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM JAKO WYZWANIE DLA ADMINISTRACJI PUBLICZNEJ – PORÓWNANIE I REKOMENDACJE DLA SYSTEMÓW POLSKI I SŁOWACJI

CYBERSECURITY MANAGEMENT AS A CHALLENGE FOR PUBLIC ADMINISTRATION – A COMPARISON AND RECOMMENDATIONS FOR THE POLISH AND SLOVAKIAN SYSTEMS

Streszczenie

Celem rozdziału jest analiza i porównanie systemów cyberbezpieczeństwa Polski i Słowacji w oraz ocena skuteczności rozwiązań organizacyjnych, prawnych i edukacyjnych stosowanych w obu krajach. Opracowanie ma również na celu sformułowanie praktycznych rekomendacji dla administracji publicznej, które mogą przyczynić się do zwiększenia odporności cyfrowej i poprawy zarządzania bezpieczeństwem

[1] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl

informacji. Problem badawczy rozdziału sformułowano: Jakie są podobieństwa i różnice w funkcjonowaniu systemów cyberbezpieczeństwa Polski i Słowacji oraz w jaki sposób rozwiązania przyjęte w obu państwach mogą wzajemnie wspierać doskonalenie krajowych strategii? Odpowiedź na to pytanie wymaga analizy zarówno aspektów organizacyjnych, jak i prawnych oraz praktycznego funkcjonowania instytucji odpowiedzialnych za bezpieczeństwo informacyjne. Postawiona hipoteza badawcza zakłada, że system cyberbezpieczeństwa w Polsce, oparty na modelu wielosektorowym, sprzyja większej elastyczności operacyjnej i współpracy międzysektorowej, natomiast model scentralizowany w Słowacji zapewnia wyższą spójność organizacyjną i skuteczniejsze zarządzanie incydentami cybernetycznymi. Integracja najlepszych praktyk obu systemów może stanowić optymalny kierunek rozwoju dla krajowych strategii bezpieczeństwa cyfrowego w Europie Środkowo-Wschodniej. W rozdziale zastosowano metody teoretyczne, obejmujące analizę porównawczą, analizę systemową, analizę dokumentów źródłowych i aktów prawnych oraz metodę dedukcyjną. Wykorzystano także analizę dokumentów, takich jak ustawy o krajowych systemach cyberbezpieczeństwa, raporty CSIRT GOV, CERT Polska oraz sprawozdania NBÚ i SK-CERT, co pozwoliło na ocenę praktycznych aspektów wdrażania polityk bezpieczeństwa w obu krajach. W wyniku przeprowadzonej analizy stwierdzono, że mimo odmiennych modeli organizacyjnych Polska i Słowacja realizują wspólny cel, jakim jest zapewnienie wysokiego poziomu ochrony danych i stabilności infrastruktury informacyjnej.

Słowa kluczowe: cyberbezpieczeństwo, administracja publiczna, dyrektywa NIS2, ochrona danych osobowych, odporność cyfrowa

Abstract

The aim of the chapter is to analyze and compare the cybersecurity systems of Polish and Slovakia and to assess the effectiveness of organizational, legal and educational solutions used in both countries. The study also aims to formulate practical recommendations for public administrations that can contribute to increasing digital resilience and improving information security management. The research problem of the chapter is formulated: What are the similarities and differences in the functioning of the cybersecurity systems of Poland and Slovakia and how can the solutions adopted in both countries mutually support the improvement of national strategies? The answer to this question requires an analysis of both organizational and legal aspects and the practical functioning of institutions responsible for information security. The research hypothesis assumes that the cybersecurity system in Poland, based on a multi-sectoral model, is conducive to greater operational flexibility and

cross-sectoral cooperation, while the centralized model in Slovakia ensures higher organizational cohesion and more effective cyber incident management. The integration of the best practices of both systems can be the optimal direction of development for national digital security strategies in Central and Eastern Europe. The chapter uses theoretical methods, including comparative analysis, systems analysis, analysis of source documents and legal acts, and the deductive method. An analysis of documents such as the Acts on National Cybersecurity Systems, reports of CSIRT GOV, CERT Polska, and reports of the National Security Authority and SK-CERT was also used, which allowed for the assessment of practical aspects of the implementation of security policies in both countries. As a result of the analysis, it was concluded that despite different organizational models, Poland and Slovakia pursue a common goal, which is to ensure a high level of data protection and stability of the information infrastructure.

Keywords: cybersecurity, public administration, NIS2 directive, personal data protection, digital resilience

Wstęp

Postępująca cyfryzacja wszystkich obszarów życia społecznego, gospodarczego i administracyjnego sprawia, że kwestia cyberbezpieczeństwa nabiera strategicznego znaczenia dla współczesnych państw. Rosnące uzależnienie od technologii informacyjnych powoduje, że zarówno instytucje publiczne, jak i prywatne są coraz bardziej narażone na zagrożenia w cyberprzestrzeni. Ataki hakerskie, kradzież danych, manipulacja informacją, ransomware czy działania o charakterze dezinformacyjnym stają się nie tylko problemem technicznym, lecz także społecznym i politycznym, wpływającym bezpośrednio na bezpieczeństwo narodowe oraz stabilność gospodarczą.

Współczesne cyberbezpieczeństwo nie ogranicza się jedynie do ochrony infrastruktury teleinformatycznej, lecz obejmuje szeroki system działań organizacyjnych, prawnych i edukacyjnych, których celem jest zapewnienie poufności, integralności i dostępności danych. Szczególnego znaczenia nabiera ono w kontekście ochrony danych osobowych, która w świetle ogólnego rozporządzenia o ochronie danych (RODO) stanowi obowiązek każdej instytucji przetwarzającej informacje o obywatelach. Zgodnie z tymi regulacjami, organizacje zobowiązane są nie tylko do zapobiegania

naruszeniom, lecz także do natychmiastowego zgłaszania incydentów, co wymusza tworzenie skutecznych procedur reagowania i zarządzania kryzysowego.

Wspólna przestrzeń cyfrowa Unii Europejskiej wymaga spójnych mechanizmów ochrony. Polska i Słowacja, jako państwa o zbliżonym poziomie rozwoju cyfrowego i członkowie tych samych struktur europejskich, realizują podobne cele w zakresie budowy odporności cybernetycznej, jednak stosują odmienne rozwiązania organizacyjne i legislacyjne. Polska przyjęła model rozproszony, w którym funkcje bezpieczeństwa pełnią trzy krajowe zespoły reagowania na incydenty – CSIRT GOV, CSIRT NASK oraz CSIRT MON – działające w ramach krajowego systemu cyberbezpieczeństwa. Słowacja natomiast wdrożyła model scentralizowany, w którym główną rolę pełni Národný bezpečnostný úrad (NBÚ) wraz z jego jednostką SK-CERT. Oba państwa wdrażają regulacje unijne, w tym dyrektywę NIS i jej nowelizację NIS2, dostosowując systemy krajowe do wspólnych standardów bezpieczeństwa sieci i informacji.

Celem niniejszego rozdziału jest analiza znaczenia cyberbezpieczeństwa oraz porównanie rozwiązań stosowanych w Polsce i Słowacji. W rozdziale omówiono podstawy prawne i instytucjonalne funkcjonowania systemów ochrony cyberprzestrzeni, przedstawiono dane dotyczące incydentów z lat 2023-2024 oraz zaproponowano rekomendacje praktyczne mające na celu doskonalenie krajowych strategii bezpieczeństwa cyfrowego. Szczególny nacisk położono na analizę skuteczności działań prewencyjnych, roli edukacji w budowaniu świadomości zagrożeń oraz konieczności integracji krajowych systemów z europejską infrastrukturą bezpieczeństwa informacyjnego.

Rozdział stanowi próbę ukazania cyberbezpieczeństwa jako elementu nie tylko technicznego, ale także społecznego i organizacyjnego, ściśle powiązanego z ochroną danych i funkcjonowaniem instytucji publicznych. Przedstawione rozważania mają na celu wskazanie, że skuteczna ochrona informacji w dobie cyfrowej transformacji wymaga współdziałania państw, administracji, sektora prywatnego i obywateli oraz budowy kultury bezpieczeństwa opartej na odpowiedzialności i wiedzy.

Definicja i znaczenie cyberbezpieczeństwa

Cyberbezpieczeństwo definiowane jako zdolność systemów teleinformatycznych do odpierania działań zagrażających ich dostępności, integralności, poufności oraz autentyczności przetwarzanych danych, jest kluczowym elementem współczesnej infrastruktury cyfrowej. Według dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej celem cyberbezpieczeństwa jest zapewnienie odporności systemów krytycznych na zdarzenia przypadkowe i działania złośliwe, które mogą naruszyć funkcjonowanie całych społeczeństw (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148). Zdefiniowane tam podstawowe pojęcia wskazują, że ochrona cyberprzestrzeni obejmuje szeroki zakres działań prewencyjnych i reakcyjnych, mających na celu przeciwdziałanie zagrożeniom. W polskim kontekście Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej rozwija to pojęcie, włączając w nie zarówno ochronę materialnej infrastruktury cyfrowej, jak i aspekt społeczny, jakim jest edukacja użytkowników oraz rozwijanie zdolności przeciwdziałania cyberatakom (Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, 2015, s. 9)

Znaczenie cyberbezpieczeństwa rośnie wraz z rozwojem technologii. Ważnym zadaniem jest ochrona kluczowej infrastruktury, takie jak systemy energetyczne, transportowe i komunikacyjne. W czasach RODO (Ogólnego Rozporządzenia o Ochronie Danych), które wymaga od organizacji lepszej ochrony danych, cyberbezpieczeństwo stało się kluczowe dla zachowania prywatności. Firmy muszą wdrażać skuteczne zasady zarządzania danymi takie jak szyfrowanie, kontrole i szkolenia pracowników. RODO wymaga także zgłaszania incydentów związanych z naruszeniem danych osobowych w ciągu 72 godzin, co wymusza stworzenie efektywnych strategii zarządzania kryzysowego.

Cyberbezpieczeństwo odgrywa ważną rolę w rozwoju gospodarki cyfrowej i zapewnia stabilne warunki działalności korporacyjnej. Ataki oprogramowania ransomware, które składają się z okupów przez szyfrowanie danych, powodują znaczne straty finansowe. W 2024 r. globalne płatności oprogramowania ransomware osiągnęły 813 mln USD. Odpowiada to spadku o ponad jedną trzecią w porównaniu do 1,25 mld dolarów w 2023 roku. Przyczyną tego trendu jest szczególnie rosnąca liczba firm, które odmówiły zapłaty okupów przez organy ścigania i odmówiły zwiększenia środków w stosunku do cyberprzestępców (Milmo, 2025).

Technologie takie jak IoT (Internet of Things – Internet Rzeczy), sztuczna inteligencja i systemy chmurowe przynoszą nowe korzyści, ale także wyzwania. IoT, poprzez swoją wielokierunkową integrację urządzeń tworzy potencjalne luki bezpieczeństwa, które mogą być wykorzystywane przez cyberprzestępców. Harmonizacja standardów ochrony tych technologii na poziomie międzynarodowym jest kluczowa dla zapobiegania cyberzagrożeniom (Szczęsna, Stachoń, 2023, s. 6-7). Edukacja społeczna i szkolenia pracowników to istotne elementy strategii cyberbezpieczeństwa. Regularne szkolenia mogą znacznie zmniejszyć ryzyko udanych ataków phishingowych (https://nflo.pl).

Dyrektywa NIS oraz RODO, które wprowadziły bardziej surowe wymogi ochrony danych, nakładają na państwa członkowskie obowiązek opracowywania strategii narodowych. RODO wymaga regularnego sprawdzania zabezpieczeń i zgłaszania naruszeń, co pomaga podnieść ogólny poziom bezpieczeństwa w organizacjach (Hydzik, 2019, s. 85-86). Współczesne cyberbezpieczeństwo nie tylko może chronić użytkowników przed zagrożeniami, ale również może wspierać rozwój gospodarczy i społeczny, tworząc stabilne warunki dla wdrażania nowości.

Cyberbezpieczeństwo odgrywa ważną rolę w utrzymaniu bezpieczeństwa wewnętrznego narodu, gdyż zapewnia ochrony systemów teleinformatycznych przed zagrożeniami, które mogą mieć wpływ na ich funkcjonowanie, a co za tym idzie, mieć wpływ na stabilność całego kraju. Obecnie, gdy technologia cyfrowa przenika niemal każdy aspekt życia, cyberprzestrzeń stwarza nowe zagrożenie dla bezpieczeństwa narodowego.

Zgodnie ze strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, jednym z głównych celów jest podniesienie poziomu odporności na cyberzagrożenia oraz ochrony informacji w sektorze publicznym, militarnym i prywatnym. W dokumencie wskazano, że cyberbezpieczeństwo to nie tylko kwestia techniczna, ale także społeczna, wymagająca edukacji społeczeństwa i rozwijania umiejętności reagowania na zagrożenia.

W Republice Słowackiej pojęcie cyberbezpieczeństwa zostało formalnie zdefiniowane w Ustawie nr 69/2018 o cyberbezpieczeństwie, zgodnie z którą oznacza ono *zdolność zapewnienia poufności, integralności, dostępności oraz autentyczności informacji przetwarzanych w sieciach i systemach teleinformatycznych, a także zdolność zapobiegania incydentom i minimalizacji ich skutków*. Zadania w tym zakresie realizuje Národný bezpečnostný

úrad (NBÚ), w ramach którego funkcjonuje National Cyber Security Centre SK-CERT, odpowiedzialne za monitorowanie, analizę i koordynację działań w przypadku incydentów.

Słowacka Strategia Cyberbezpieczeństwa na lata 2021-2025 (Národná koncepcia kybernetickej bezpečnosti) określa cyberbezpieczeństwo jako *element bezpieczeństwa narodowego, warunkujący ciągłość funkcjonowania administracji, sektora gospodarczego i społeczeństwa informacyjnego*. Dokument wskazuje, że ochrona cyberprzestrzeni wymaga nie tylko środków technicznych, ale również edukacji społecznej, wymiany informacji międzysektorowej i międzynarodowej współpracy.

Na Słowacji system prawny został już dostosowany do dyrektywy NIS2 poprzez nowelizację ustawy nr 69/2018 (Dz. U. 366/2024), która weszła w życie 1 stycznia 2025 r. Nowe przepisy nakładają na operatorów usług kluczowych i podmioty sektora publicznego obowiązek raportowania incydentów w ciągu 24 godzin, prowadzenia regularnych audytów bezpieczeństwa oraz wdrażania planów zarządzania ryzykiem.

W porównaniu z Polską, gdzie podstawą systemu jest ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Słowacja cechuje się bardziej centralistyczną strukturą zarządzania. Wszystkie działania koordynuje NBÚ i SK-CERT, podczas gdy w Polsce funkcjonują trzy krajowe CSIRTy: CSIRT GOV (ABW), CSIRT NASK oraz CSIRT MON Polska Strategia Cyberbezpieczeństwa RP na lata 2019-2024 zawiera podobne założenia, lecz kładzie większy nacisk na współpracę z sektorem prywatnym i rozwój krajowych zdolności obronnych.

W obu państwach cyberbezpieczeństwo stanowi kluczowy komponent bezpieczeństwa narodowego i gospodarczego, jednak Słowacja szybciej dostosowała swoje ramy prawne do wymogów UE. Z kolei Polska dysponuje bardziej rozbudowaną infrastrukturą CSIRT-ową i wyższym poziomem dojrzałości w rankingach ENISA oraz NCSI (Polska – 7 miejsce, Słowacja – 19 miejsce wg NCSI 2024).

Rozwoju i ewolucja cyberzagrożeń

Cyberbezpieczeństwo jest dziś bardzo ważny, ale jego początki sięgają lat 70. Wtedy zagrożenia w sieci były proste i miały charakter eksperymentalny.

Jednym z pierwszych wirusów komputerowych był creeper, stworzony w 1971 roku. Nie miał na celu niszczenia systemów-jego twórca chciał tylko sprawdzić, jak daleko może Rozprzestrzenić się w sieci. Poza zainfekowaniu komputera wyświetlał komunikat: „I'M THE CREEPER: CATCH ME IF YOU CAN" i przenosił się na kolejne urządzenie. W odpowiedzi powstał Reaper, pierwszy program antywirusowy, którego zadaniem było odnalezienie i usunięcie Creepera. Można więc powiedzieć, że już na samym początku historii komputerów zaczęła się walka między wirusami, a programami ochronnymi (https://www.maturaminds.pl).

W latach 80. zagrożenia cybernetyczne zaczęły przybierać bardziej destrukcyjny charakter. Robak Morris, który pojawił się w 1988 roku, zainfekował około 10% ówczesnego internetu, co uczyniło go jednym z najważniejszych wydarzeń w historii cyberbezpieczeństwa. W tym okresie zaczęto tworzyć pierwsze zespoły reagowania na awarie komputerowe, znane jako CERT (Computer Emergency Response Team), które miały na celu monitorowanie i przeciwdziałanie zagrożeniom (https://digitalheritage.pl).

W latach 90. cyberprzestępczość zaczęła się rozwijać na dużą skalę, a hakerzy coraz częściej atakowali dla pieniędzy, a nie tylko z ciekawości. Wirus ILOVEYOU (2000) rozprzestrzeniał się po całym świecie, powodując ogromne straty finansowe. Pokazało to, jak groźne mogą być cyberataki i jak ważna jest ochrona danych. W odpowiedzi rządy różnych krajów zaczęły wprowadzać pierwsze przepisy dotyczące cyberbezpieczeństwa, a firmy zaczęły tworzyć coraz lepsze programy antywirusowe i systemy ochrony, aby zapobiegać kolejnym zagrożeniom (Colby, 2021).

Rozwój cyberbezpieczeństwa na Słowacji, podobnie jak w Polsce, był ściśle związany z postępującą cyfryzacją administracji publicznej i gospodarki. Początki instytucjonalnych działań w tym obszarze sięgają początku XXI wieku, kiedy to w ramach Słowackiego Uniwersytetu Technicznego i Ministerstwa Obrony zaczęto prowadzić pierwsze badania nad bezpieczeństwem systemów informatycznych. W 2008 r. w strukturze Národného bezpečnostného úradu (NBÚ) utworzono pierwsze komórki zajmujące się analizą incydentów komputerowych i ochroną informacji niejawnych. Był to etap odpowiadający powstawaniu w Polsce zespołu CERT Polska (1996) i wczesnych działań ABW w zakresie ochrony infrastruktury krytycznej.

Kluczowym momentem w rozwoju słowackiego systemu cyberbezpieczeństwa było przyjęcie w 2015 roku pierwszej Strategii Cyberbezpieczeństwa

Republiki Słowackiej, która ustanowiła ramy dla budowy krajowego systemu reagowania na incydenty. W 2016 r. powołano National Cyber Security Centre SK-CERT, które w 2018 roku zostało formalnie osadzone w strukturze NBÚ. Tego samego roku przyjęto ustawę nr 69/2018 o cyberbezpieczeństwie, wdrażającą dyrektywę NIS i określającą obowiązki operatorów usług kluczowych, dostawców cyfrowych oraz organów administracji publicznej.

Od tego momentu Słowacja rozwijała narodowy system bezpieczeństwa cyberprzestrzeni w oparciu o model centralny – wszystkie kompetencje skupiono w NBÚ i SK-CERT. Działania te obejmowały m.in. tworzenie krajowych procedur reagowania, opracowanie standardów audytów bezpieczeństwa oraz rozwój krajowej sieci ostrzegania. W 2021 r. rząd przyjął nową Strategię Cyberbezpieczeństwa 2021-2025, która rozszerzyła zakres działań na sektor edukacji i administracji lokalnej oraz zapowiedziała pełne wdrożenie dyrektywy NIS2 do prawa krajowego.

W Polsce rozwój cyberbezpieczeństwa nabrał tempa w pierwszej dekadzie XXI wieku. Wprowadzono pierwsze krajowe regulacje chroniące systemy teleinformatyczne, a w 2019 roku przyjęto Strategię Cyberbezpieczeństwa RP na lata 2019-2024, która podkreśla potrzebę ochrony infrastruktury krytycznej, współpracy międzynarodowej oraz edukacji publicznej. Obecnie cyberbezpieczeństwo w Polsce jest jednym z kluczowych obszarów polityki bezpieczeństwa narodowego.

W ostatnich latach, w miarę pojawiania się nowych technologii takich jak Internet Rzeczy (IoT) czy sztuczna inteligencja, cyberprzestępczość osiągnęła nowy poziom złożoności. Jednym z największych problemów stały się ataki ransomware, które powodują straty gospodarcze rzędu miliardów dolarów rocznie. W odpowiedzi na te zagrożenia rozwijane są nowoczesne systemy ochrony, takie jak analiza zagrożeń w czasie rzeczywistym i automatyczne systemy wykrywania incydentów.

Zdaniem autora historia cyberbezpieczeństwa pokazuje, że dziedzina ta stale rozwija się w odpowiedzi na zmieniające się zagrożenia. Nowoczesne strategie ochrony to połączenie technologii, edukacji oraz współpracy międzynarodowej, co może czynić cyberbezpieczeństwo jednym z filarów globalnego bezpieczeństwa.

Zagrożenia w cyberprzestrzeni obejmują szeroki zakres działań, od cyberprzestępczości i cyberterroryzmu po bardziej wyrafinowane działania, takie jak manipulacja informacjami, które mogą destabilizować

społeczeństwa. Poniżej w tabeli przedstawiono najskuteczniejsze metody w ochronie przed cyberzagrożeniami.

Tabela 1. Najskuteczniejsza metoda w ochronie przed cyberzagrożeniami według respondentów

Metoda	Udział procentowy
Programy antywirusowe	68.8%
Backup danych	15.1%
Szkolenia	9.6%
Procedury bezpieczeństwa	5.6%
Inne	0.9%

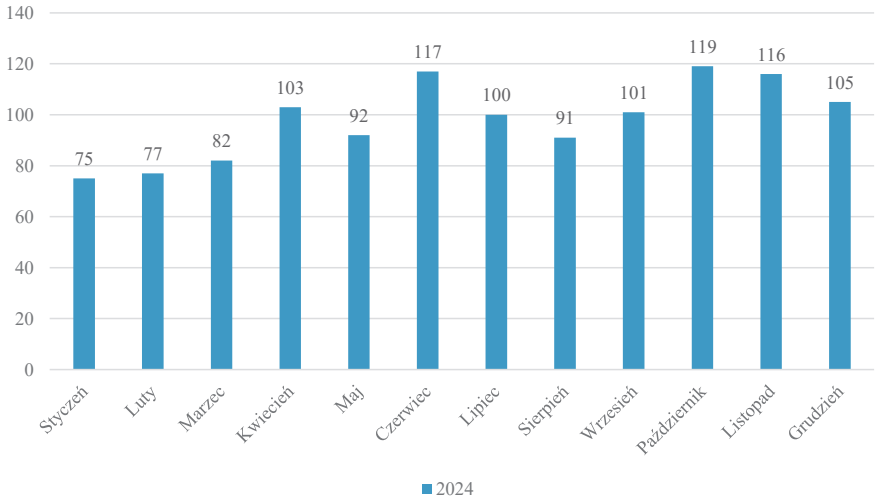
Źródło: opracowanie własne na podstawie: Vecto Sp. z o.o. (2023). *Cyberbezpieczeństwo w polskich firmach 2023*, s. 10-12 (dostęp: 27.09.2025 r.).

Wnioski dotyczącej tabeli o najskuteczniejszych metodach ochrony przed cyberzagrożeniami:

- dominacja programów antywirusowych – największa część respondentów (68,8%) uważa, że programy antywirusowe są najskuteczniejszym środkiem ochrony przed cyberzagrożeniami. Wskazuje to na powszechne postrzeganie zabezpieczeń opartych na oprogramowaniu jako kluczowego narzędzia obrony przed atakami. Może to wynikać z łatwej dostępności oraz szerokiego zastosowania takich rozwiązań zarówno w firmach jak i u użytkowników indywidualnych,
- niedocenianie backupu jako metody ochrony – mimo, że regularne tworzenie kopii zapasowych danych jest jednym z najlepszych sposobów minimalizowania skutków ataków ransomware i innych incydentów, tylko 15,1% respondentów wskazało tę metodę jako najskuteczniejszą. Może to sugerować, że wciąż brakuje świadomości na temat znaczenia strategii przywracania danych w przypadku naruszenia bezpieczeństwa,
- niskie znaczenie procedur bezpieczeństwa – jedynie 5,6% badanych uznało, że procedury bezpieczeństwa są kluczowe w ochronie przed zagrożeniami. Może to świadczyć o tym, że organizacje często koncentrują się na narzędziach technicznych, pomijając znaczenie formalnych regulacji i procedur, takich jak kontrola dostępu, polityka haseł czy systemy zarządzania ryzykiem,

- szkolenia jako niewykorzystany potencjał – tylko 9,6% respondentów wskazało, że szkolenia stanowią skuteczną metodę ochrony. Biorąc pod uwagę, że większość ataków opiera się na błędach ludzkich (np. phishing), niski udział tej kategorii może sugerować, że firmy i instytucje nie przywiązują dostatecznej wagi do edukacji pracowników w zakresie cyberbezpieczeństwa,
- marginalne znaczenie innych metod – inne metody ochrony zostały wskazane przez zaledwie 0,9% respondentów, co pokazuje, że większość osób skupia się na konwencjonalnych środkach zabezpieczeń, a mniej na zaawansowanych rozwiązaniach, takich jak monitorowanie sieci, systemy wykrywania zagrożeń czy segmentacja infrastruktury IT.

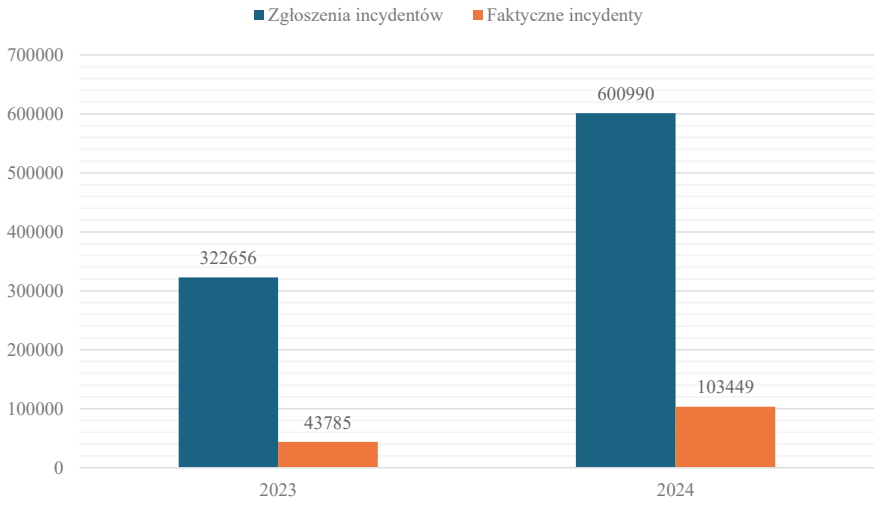
W 2024 roku w Słowacji większość zgłoszeń o incydentach cyberbezpieczeństwa wpłynęła w drugiej połowie roku. W 2024 roku SK-CERT otrzymał o 204 zgłoszenia więcej niż w roku poprzednim. Wzrost liczby zgłaszanych incydentów można przypisać procesowi legislacyjnemu transpozycji dyrektywy NIS2, która rozszerza jej zakres na kolejne podmioty. W związku z tym zwiększona liczba zgłaszanych incydentów nie pozwala na wyciągnięcie jednoznacznej odpowiedzi, że słowacka cyberprzestrzeń stała się mniej bezpieczna. Poniżej na rysunku przedstawiono liczbę incydentów w Słowacji w 2024 r.



Rysunek 1. Liczba zgłoszonych incydentów w Słowacji w 2024 r.

Źródło: Národný bezpečnostný úrad. (2025). *Annual Report on cybersecurity of the Slovak Republic 2024*, s. 10-11.

Dane te potwierdzają potrzebę ciągłego monitorowania sytuacji w cyberprzestrzeni, dostosowywania środków ochronnych do sezonowych wzrostów aktywności cyberprzestępczej oraz prowadzenia działań edukacyjnych w okresach szczególnie narażonych na wzmożone ataki. Natomiast poniżej przedstawiono liczbę zarejestrowanych zgłoszeń oraz incydentów cyberbezpieczeństwa w latach 2023-2024 w Polsce.

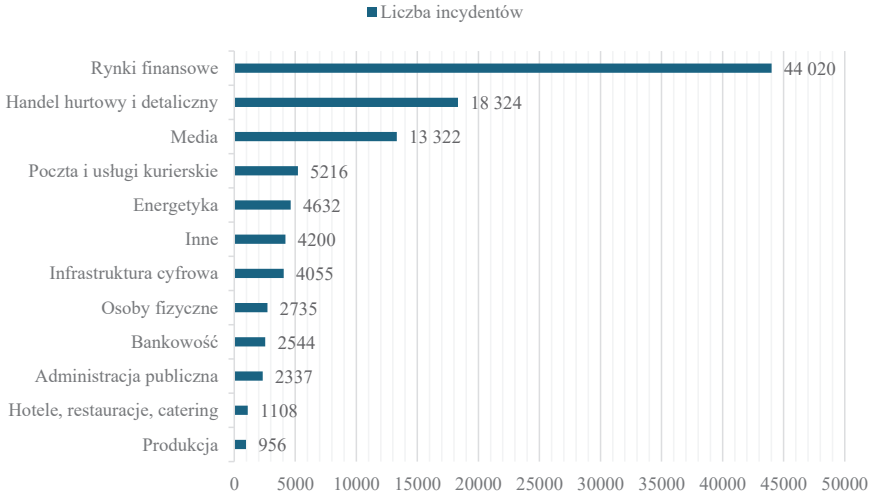


Rysunek 2. Liczba zarejestrowanych zgłoszeń oraz incydentów cyberbezpieczeństwa w latach 2023-2024

Źródło: CSIRT GOV. (2023). *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, s. 8; CERT Polska. (2024). *Raport roczny 2024,* s. 88.

Rysunek 2 pokazuje wyraźny wzrost zarówno liczby zgłoszeń incydentów cyberbezpieczeństwa, jak i faktycznie potwierdzonych przypadków w latach 2023-2024. W 2023 roku zgłoszono ponad 322 tysiące incydentów, z czego niecałe 44 tysiące zostały potwierdzone jako realne zagrożenia. W kolejnym roku zgłoszeń było już ponad 600 tysięcy, a faktycznych incydentów ponad 103 tysiące. Taki skok może świadczyć o większej świadomości użytkowników i skuteczniejszym systemie zgłaszania, ale też o rosnącej aktywności cyberprzestępców. Jednocześnie różnica pomiędzy liczbą zgłoszeń a rzeczywistymi incydentami również się powiększyła, co sugeruje, że użytkownicy coraz częściej reagują na podejrzane sytuacje, nawet jeśli nie zawsze są one faktycznym zagrożeniem. Pokazuje to, że edukacja

w zakresie cyberbezpieczeństwa przynosi efekty, ale też, że konieczne jest dalsze wzmacnianie systemów ochrony oraz lepsze metody weryfikacji zgłoszeń.



Rysunek 3. Statystyka incydentów w roku 2024 z podziałem na sektory gospodarki

Źródło: CERT Polska. (2024). *Raport roczny 2024,* s. 91.

Rysunek 3 przedstawia statystykę incydentów cyberbezpieczeństwa w 2024 roku z podziałem na sektory gospodarki. Najwięcej zgłoszeń dotyczyło infrastruktury rynków finansowych, gdzie odnotowano aż 44 020 incydentów. Na drugim miejscu znalazł się handel hurtowy i detaliczny z wynikiem 18 324, a zaraz za nim media – 13 322 incydenty. Wyraźnie widać, że największe zagrożenia dotykają sektorów o dużym znaczeniu dla gospodarki i z intensywnym przetwarzaniem danych, takich jak finanse, handel czy media. Mniejsze liczby incydentów odnotowano w sektorach takich jak produkcja, administracja publiczna czy gastronomia, jednak nawet tam skala zagrożeń nie jest pomijalna. Zestawienie pokazuje, że cyberbezpieczeństwo to problem obejmujący praktycznie każdą branżę, a różnice w liczbach wynikają nie tylko z poziomu zagrożeń, ale też z różnic w wykrywaniu i zgłaszaniu incydentów. Szczególną uwagę należy poświęcić sektorom o największej liczbie ataków, ale nie można zapominać o mniej narażonych branżach, które często nie mają wystarczających środków na odpowiednią ochronę.

Dane przedstawione na rysunku wyraźnie pokazują, że w 2024 roku żadna branża nie była całkowicie wolna od zagrożeń w cyberprzestrzeni. Chociaż największe liczby incydentów odnotowano w sektorach finansowych i handlowych, to obecność zagrożeń w niemal każdej dziedzinie gospodarki potwierdza, że cyberbezpieczeństwo musi być traktowane jako wspólny priorytet – niezależnie od wielkości organizacji czy profilu jej działalności.

Porównując oba kraje, widać różnice w podejściu instytucjonalnym i dynamice rozwoju. Polska wcześniej zbudowała rozbudowaną strukturę trzech krajowych CSIRT-ów (GOV, NASK, MON), a jej Strategia Cyberbezpieczeństwa 2019-2024 położyła nacisk na współpracę z sektorem prywatnym i budowę krajowych zdolności obronnych. Słowacja natomiast przyjęła model scentralizowany, koncentrując zarządzanie w jednym ośrodku – NBÚ, co przyczyniło się do szybszej koordynacji działań, ale ograniczyło poziom specjalizacji sektorowej.

W obu krajach istotną rolę odgrywa współpraca międzynarodowa – zarówno w ramach ENISA, jak i Centrum Doskonałości CCDCOE w Tallinnie, którego członkiem Słowacja jest od 2013 r. Dzięki temu słowacki system w ostatnich latach osiągnął wysoki poziom integracji z unijnymi strukturami bezpieczeństwa i cyberobrony.

Historia cyberbezpieczeństwa na Słowacji pokazuje, że rozwój tej dziedziny przebiegał od prostych działań technicznych w administracji do pełnoprawnego systemu narodowego, opartego na regulacjach prawnych, szkoleniach i międzynarodowej współpracy. Podobnie jak w Polsce, ewolucja ta dowodzi, że bezpieczeństwo cyfrowe stało się jednym z kluczowych elementów współczesnego bezpieczeństwa narodowego i publicznego.

Poprawa systemu cyberbezpieczeństwa – praktyczne rekomendacje dla Polski i Słowacji

Dynamiczny rozwój technologii cyfrowych, rosnąca liczba incydentów w cyberprzestrzeni oraz nasilające się zagrożenia o charakterze hybrydowym sprawiają, że systemy cyberbezpieczeństwa w państwach Europy Środkowo-Wschodniej wymagają stałego doskonalenia. Polska i Słowacja, jako kraje członkowskie Unii Europejskiej oraz NATO, stają przed podobnymi wyzwaniami związanymi z ochroną infrastruktury krytycznej,

zapewnieniem odporności instytucji publicznych i prywatnych, a także podnoszeniem świadomości społecznej w zakresie zagrożeń cyfrowych. Oba państwa wypracowały własne modele organizacji systemu bezpieczeństwa informacyjnego, które – mimo różnic strukturalnych – mają zbliżony cel: zwiększenie odporności państwa na ataki cybernetyczne i zapewnienie stabilności funkcjonowania gospodarki cyfrowej.

W Polsce system cyberbezpieczeństwa opiera się na trzech krajowych zespołach reagowania na incydenty bezpieczeństwa komputerowego: CSIRT GOV działającym przy Agencji Bezpieczeństwa Wewnętrznego, CSIRT NASK zajmującym się sektorem cywilnym oraz CSIRT MON obsługującym resort obrony. Rozbudowana struktura umożliwia specjalizację sektorową, lecz jednocześnie komplikuje centralną koordynację i spójność działań. Słowacja przyjęła bardziej scentralizowany model, w którym za wszystkie działania odpowiada Národný bezpečnostný úrad (NBÚ) wraz z Narodowym Centrum Cyberbezpieczeństwa SK-CERT. Takie rozwiązanie usprawnia przepływ informacji i podejmowanie decyzji na poziomie krajowym, jednak ogranicza sektorową specjalizację i elastyczność w reagowaniu na incydenty o różnym charakterze.

W obu państwach niezbędne jest zacieśnienie współpracy regionalnej, szczególnie w ramach Grupy Wyszehradzkiej. Utworzenie wspólnej platformy wymiany informacji o incydentach mogłoby usprawnić reagowanie na transgraniczne zagrożenia, takie jak ataki phishingowe, szkodliwe oprogramowanie czy kampanie dezinformacyjne. Polska mogłaby rozważyć powołanie centralnego ośrodka koordynującego działania trzech krajowych CSIRT-ów, co pozwoliłoby na szybszą wymianę informacji i ujednolicenie procedur reagowania. Z kolei Słowacja, mająca już wypracowany model centralny, mogłaby wprowadzić sektorowe centra reagowania, zwłaszcza w obszarach finansów, energetyki i ochrony zdrowia, które są najbardziej narażone na cyberataki.

Istotnym kierunkiem doskonalenia systemów ochrony informacji jest dalsze dostosowanie przepisów prawa do wymogów dyrektywy NIS2. Słowacja zakończyła proces wdrażania tej dyrektywy z początkiem 2025 roku, wprowadzając bardziej rygorystyczne zasady raportowania incydentów i obowiązkowe audyty bezpieczeństwa. Polska wciąż prowadzi prace legislacyjne nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, co wskazuje na potrzebę przyspieszenia procesu legislacyjnego

i ściślejszej współpracy administracji publicznej z sektorem prywatnym. W obu krajach niezbędne jest również rozwinięcie jednolitego systemu raportowania incydentów oraz włączenie do systemu ochrony jednostek samorządowych, uczelni i podmiotów ochrony zdrowia, które przetwarzają duże zbiory danych wrażliwych.

Kolejnym obszarem wymagającym wzmocnienia jest rozwój kompetencji i edukacji cyfrowej. Zarówno Polska, jak i Słowacja borykają się z niedoborem wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, co stanowi poważne ograniczenie dla dalszego rozwoju systemu ochrony informacji. Wymaga to zwiększenia liczby programów kształcenia akademickiego, uruchamiania laboratoriów i centrów symulacyjnych, a także organizowania regularnych ćwiczeń krajowych i międzynarodowych, które pozwolą na doskonalenie współpracy między instytucjami publicznymi a sektorem prywatnym. Polska może rozwijać istniejące już inicjatywy w ramach programu „Cyber.Mil.pl", natomiast Słowacja powinna kontynuować projekty edukacyjne prowadzone przez NBÚ, w tym program „Kyberbezpečná škola", skierowany do uczniów i urzędników administracji publicznej.

Rozwój technologiczny stanowi kolejny kluczowy element doskonalenia systemów bezpieczeństwa. Zarówno w Polsce, jak i na Słowacji niezbędne są inwestycje w nowoczesne systemy analizy i monitorowania zagrożeń, takie jak Security Operations Center, narzędzia SIEM czy platformy automatyzacji reakcji SOAR. Wzrost znaczenia przetwarzania danych w chmurze wymaga także opracowania krajowych ram zaufania dla usług chmurowych administracji publicznej, co pozwoli na bezpieczne zarządzanie danymi wrażliwymi. Szczególnej ochrony wymagają systemy energetyczne, transportowe i telekomunikacyjne, które w przypadku ataku mogą sparaliżować funkcjonowanie państwa. W tym kontekście zarówno Polska, jak i Słowacja powinny rozwijać zdolności w zakresie cyberobrony i ochrony infrastruktury krytycznej przed zagrożeniami hybrydowymi.

Niezwykle ważnym aspektem doskonalenia systemu cyberbezpieczeństwa jest także kształtowanie kultury bezpieczeństwa cyfrowego. Wymaga to włączenia zagadnień związanych z ochroną informacji i higieną cyfrową do programów nauczania na wszystkich poziomach edukacji, a także prowadzenia kampanii społecznych promujących bezpieczne korzystanie z Internetu. Edukacja społeczeństwa powinna być traktowana jako element obrony narodowej, gdyż większość cyberataków opiera się na błędach

ludzkich i braku świadomości użytkowników. Wspólnym celem dla Polski i Słowacji powinno być opracowanie programu regionalnego „CyberSafe V4", który zintegrowałby działania edukacyjne i prewencyjne państw Grupy Wyszehradzkiej.

Analiza systemów cyberbezpieczeństwa Polski i Słowacji wskazuje, że oba państwa poczyniły znaczne postępy w budowie struktur ochrony cyberprzestrzeni, jednak ich dalszy rozwój wymaga konsekwentnego doskonalenia. Polska powinna skoncentrować się na uproszczeniu struktury instytucjonalnej, wzmocnieniu koordynacji działań i przyspieszeniu wdrażania przepisów NIS2. Słowacja z kolei powinna zwiększyć specjalizację sektorową i wzmocnić praktyczne kompetencje administracji publicznej w zakresie reagowania na incydenty. W obu krajach konieczne jest także dalsze inwestowanie w technologię, edukację i kulturę bezpieczeństwa. Tylko dzięki synergii tych działań możliwe będzie stworzenie spójnego, odpornego i skutecznego systemu cyberbezpieczeństwa, stanowiącego fundament bezpieczeństwa narodowego w erze transformacji cyfrowej.

Podsumowanie

Analiza porównawcza systemów cyberbezpieczeństwa Polski i Słowacji pozwala stwierdzić, że oba państwa osiągnęły znaczący postęp w budowie struktur chroniących cyberprzestrzeń oraz w implementacji unijnych standardów bezpieczeństwa informacji. Polska wypracowała model wielosektorowy, oparty na współpracy trzech krajowych zespołów reagowania na incydenty CSIRT, co zapewnia wysoki poziom specjalizacji, lecz utrudnia centralną koordynację działań. Z kolei Słowacja, stosując model scentralizowany z Národným bezpečnostným úradem (NBÚ) i jednostką SK-CERT w roli głównej, uzyskała większą spójność organizacyjną, lecz mniejszą elastyczność w reagowaniu na zróżnicowane zagrożenia.

W obu przypadkach cyberbezpieczeństwo zostało uznane za kluczowy element bezpieczeństwa narodowego, a implementacja dyrektyw RODO, NIS oraz NIS2 wymusiła stworzenie skutecznych systemów monitorowania, raportowania i zarządzania incydentami. Polska, mimo trwających prac legislacyjnych nad pełnym wdrożeniem NIS2, posiada rozbudowaną infrastrukturę reagowania, rozwinięte programy edukacyjne oraz rosnące doświadczenie w koordynacji międzyresortowej. Słowacja natomiast wyróżnia się

szybkim tempem harmonizacji prawa i konsekwentnym budowaniem centralnych struktur nadzoru nad bezpieczeństwem cyfrowym.

Wnioski płynące z analizy wskazują, że oba kraje powinny kontynuować proces wzmacniania odporności na cyberzagrożenia poprzez integrację systemów krajowych, rozwój współpracy transgranicznej oraz podnoszenie kompetencji pracowników administracji publicznej. Kluczowe znaczenie mają inwestycje w technologie monitorowania i automatyzacji, wdrażanie standardów chmurowych o wysokim poziomie zaufania oraz włączenie zagadnień cyberhigieny do programów edukacyjnych i szkoleniowych.

Polska i Słowacja, jako członkowie Unii Europejskiej i NATO, powinny traktować cyberbezpieczeństwo jako wspólną przestrzeń odpowiedzialności i współpracy. Tylko poprzez konsekwentne wdrażanie zasad dobrej praktyki, wymianę doświadczeń oraz tworzenie wspólnych inicjatyw edukacyjnych możliwe będzie osiągnięcie wysokiego poziomu odporności cyfrowej. W dłuższej perspektywie skuteczna ochrona danych i infrastruktury informacyjnej stanowi nie tylko wymóg prawny, ale przede wszystkim warunek stabilności, zaufania społecznego i bezpieczeństwa narodowego w erze transformacji cyfrowej.

Literatura

1. Biuro Bezpieczeństwa Narodowego, *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015.
2. CERT Polska, *Raport roczny 2024*, Warszawa 2024.
3. CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku*, Warszawa 2023.
4. Colby, S. (2021). *ILOVEYOU:* The Computer Worm that Went Global by Exploiting Human Psychology. *The Synapse: Intercollegiate Science Magazine, 29*(1), Article 13.
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii", Dziennik Urzędowy Unii Europejskiej, https://eur-lex.europa.eu (dostęp: 01.02.2026).
6. ECSO, NIS2 Directive Transposition Tracker 2025, European Cyber Security Organisation, Brussels 2025.

7. ENISA Threat Landscape 2024.
8. Hydzik, W. (2019). Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych. *Przegląd Ustawodawstwa Gospodarczego*, nr 3, 84-87.
9. Matura Minds, *Historia cyberbezpieczeństwa – od Creepera do nowoczesnych zagrożeń*, https://www.maturaminds.pl (dostęp: 01.02.2026).
10. Milmo D., *Global ransomware payments plunge by a third amid crackdown*, The Guardian, https://www.theguardian.com (dostęp: 01.02.2026).
11. Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Warszawa 2019.
12. Národný bezpečnostný úrad, Zákon č. 69/2018 *Z.z. o kybernetickej bezpečnosti*, Bratislava 2018.
13. Národný bezpečnostný úrad, *Annual Report on cybersecurity of the Slovak Republic 2024*. Bratislava 2025.
14. Národný bezpečnostný úrad, *Annual Report 2023 – Cyber Security Centre SK-CERT*, Bratislava 2024.
15. nFlo, *Jakie są najlepsze praktyki w zapobieganiu cyberatakom na samorządy?* https://nflo.pl (dostęp: 25.09.2025).
16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), art. 32 ust. 1 oraz art. 33 ust. 1, Dziennik Urzędowy Unii Europejskiej L 119, Luksemburg 2016.
17. Szczęsna, A., Stachoń, M. (red.) (2023). *Cyberbezpieczeństwo AI. AI w cyberbezpieczeństwie*, Warszawa: NASK-PIB.
18. Digital Heritage. *The digital heritage of the Morris Worm*. https://digitalheritage.pl (dostęp: 08.12.2025).
19. Vecto Sp. z o.o., *Cyberbezpieczeństwo w polskich firmach 2023*, Warszawa 2023.