Gabriel Kagankiewicz https://orcid.org/0009-0009-6649-8570
Wyższa Szkoła Biznesu i Nauk o Zdrowiu
e-mail: gabri3l.kagankiewicz@gmail.com

Wiktoria Urbańska https://orcid.org/0009-0005-8208-8708
Wyższa Szkoła Biznesu i Nauk o Zdrowiu
e-mail: wiktoriaurbanska277@gmail.com

Zarządzanie bezpieczeństwem informacji w instytucjach publicznych

Information security management in public institutions

https://doi.org/10.25312/ziwgib.906

Streszczenie

Celem artykułu jest przedstawienie głównych założeń i mechanizmów zarządzania bezpieczeństwem informacji w instytucjach publicznych ze szczególnym uwzględnieniem aspektów organizacyjnych, prawnych i ludzkich. Analizę oparto na przeglądzie literatury przedmiotu, obowiązujących aktów prawnych, w tym ustawy o krajowym systemie cyberbezpieczeństwa, rozporządzenia RODO i Krajowych Ram Interoperacyjności, normy ISO/IEC 27001 oraz przykładów rzeczywistych incydentów bezpieczeństwa informacji. W artykule omówiono znaczenie triady CIA, funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), analizę ryzyka, zarządzanie kryzysowe, plany ciągłości działania oraz zadania jednostek odpowiedzialnych za ochronę informacji w administracji publicznej. Przeprowadzona analiza wykazała, że skuteczność zarządzania bezpieczeństwem informacji zależy od integracji wymagań prawnych, organizacyjnych i technicznych z właściwym przygotowaniem pracowników. Szczególne znaczenie przypisano czynnikowi ludzkiemu, obejmującemu przestrzeganie procedur,

właściwe zarządzanie uprawnieniami oraz udział w szkoleniach podnoszących świadomość bezpieczeństwa. W rezultacie stwierdzono, że skuteczna ochrona informacji wymaga holistycznego modelu obejmującego zarządzanie ryzykiem, funkcjonowanie SZBI, rozwój kultury bezpieczeństwa, reagowanie na incydenty oraz zapewnianie ciągłości działania administracji publicznej.

Słowa kluczowe: bezpieczeństwo informacji, administracja publiczna, cyberbezpieczeństwo, triada CIA, zarządzanie kryzysowe, analiza ryzyka

Abstract

The aim of this article is to present the main principles and mechanisms of information security management in public institutions, with particular emphasis on organizational, legal, and human factors. The analysis is based on a review of the relevant literature, applicable legal regulations, including National Cybersecurity System Act, the General Data Protection Regulation (GDPR), the National Interoperability Framework, the ISO/IEC 27001 standard and examples of real information security incidents. The article discusses the significance of the CIA triad, the Information Security Management System (ISMS), risk assessment, crisis management, business continuity planning, and the responsibilities of organizational units responsible for information protection in public administration. The conducted analysis demonstrates that the effectiveness of information security management depends on the integration of legal, organizational, and technical requirements with appropriate employee preparation. Particular attention is paid to the human factor, including compliance with established procedures, proper privilege management, and participation in security awareness training. The findings indicate that effective information protection requires a holistic management model encompassing risk management, the operation of the Information Security Management System, the development of a security culture, incident response, and the maintenance of business continuity in public administration.

Keywords: information security, public administration, cybersecurity, CIA triad, crisis management, risk analysis

Wprowadzenie

Dynamiczny rozwój technologii informacyjno-komunikacyjnych oraz postępująca cyfryzacja administracji publicznej sprawiają, że bezpieczeństwo informacji staje się jednym z kluczowych elementów funkcjonowania współczesnego państwa. Instytucje publiczne gromadzą, przetwarzają i udostępniają znaczne ilości danych, obejmujących zarówno dane osobowe obywateli, jak i informacje o istotnym znaczeniu dla realizacji zadań

publicznych. W związku z rosnącą liczbą cyberzagrożeń, takich jak ataki ransomware, phishing czy nieuprawniony dostęp do systemów teleinformatycznych, konieczne jest wdrażanie skutecznych mechanizmów ochrony informacji, uwzględniających aspekty organizacyjne, prawne, techniczne i ludzkie. Zapewnienie odpowiedniego poziomu bezpieczeństwa wymaga nie tylko stosowania zabezpieczeń technicznych, ale również tworzenia odpowiednich struktur organizacyjnych, procedur zarządzania ryzykiem oraz podnoszenia świadomości pracowników. Szczególne znaczenie odgrywa System Zarządzania Bezpieczeństwem Informacji (SZBI), oparty na zasadach poufności, integralności i dostępności informacji oraz wspierany przez międzynarodowe normy z rodziny ISO/IEC 27000.

Celem niniejszego artykułu jest przedstawienie podstawowych założeń zarządzania bezpieczeństwem informacji w instytucjach publicznych ze szczególnym uwzględnieniem roli Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), struktur organizacyjnych odpowiedzialnych za ochronę informacji, analizy ryzyka, zarządzania kryzysowego oraz czynnika ludzkiego w zapewnianiu bezpieczeństwa danych. Analizę oparto na opracowaniach naukowych dotyczących problematyki bezpieczeństwa informacji i aktach prawnych regulujących bezpieczeństwo informacji w administracji publicznej, w tym ustawie o krajowym systemie cyberbezpieczeństwa, przepisach RODO, Krajowych Ramach Interoperacyjności oraz normie ISO/IEC 27001. Uzupełnieniem rozważań są wybrane przykłady rzeczywistych incydentów, ukazujące praktyczne znaczenie omawianych zagadnień. W kolejnych częściach opracowania omówiono podstawowe założenia bezpieczeństwa informacji, rolę instytucji publicznych oraz struktur organizacyjnych odpowiedzialnych za ochronę danych, zagadnienia związane z analizą ryzyka i zarządzaniem kryzysowym, znaczenie czynnika ludzkiego. Przyjęte podejście pozwala na kompleksową ocenę czynników wpływających na skuteczność zarządzania bezpieczeństwem danych w administracji publicznej.

Triada CIA

Triada CIA, znana również jako triada bezpieczeństwa informacji, jest podstawowym modelem w dziedzinie bezpieczeństwa informatycznego, który określa trzy główne cele ochrony danych: poufność, integralność i dostępność (*Co to jest Triada CIA i na czym polega?*, 2024).

Poufność (*Confidentiality*) to funkcja, która gwarantuje, że tylko osoby upoważnione, mające dostęp do danych ze względu na zakres swoich obowiązków służbowych, mają możliwość wykonywania na nich operacji. Inaczej mówiąc, nieuprawnione osoby nie powinny mieć żadnego dostępu do danych, co za tym idzie – nie należy ich im ujawniać bądź udostępniać. Dotyczy to osób zarówno z zewnątrz, jak i pracowników danej organizacji, którzy wykonują obowiązki bez dostępu do określonych informacji. Najbardziej znanym środkiem realizacji ochrony poufności jest kontrola dostępu, czyli między innymi loginy, hasła, uwierzytelnienie wieloskładnikowe. Ważnym zabezpieczeniem jest także szyfrowanie danych, na przykład podczas przesyłania komuś informacji oraz przechowywania.

Informacje dzielimy na tajne i poufne. Innym środkiem realizacji jest także polityka bezpieczeństwa i szkolenie pracowników w tym zakresie. Głównym celem poufności jest ochrona danych przed nieuprawnionym dostępem, co zapobiega ich wyciekowi, kradzieży lub nieautoryzowanemu ujawnieniu. Wdrażanie skutecznych środków ochrony poufności jest niezbędne dla zapewnienia prywatności użytkowników, zgodności z regulacjami prawnymi – na przykład RODO, czyli 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 (ogólne rozporządzenie o ochronie danych) – oraz utrzymania zaufania klientów i partnerów biznesowych (*Incydenty bezpieczeństwa – definicja, przykłady i zarządzanie*, 2024). Poufność jest fundamentem bezpieczeństwa informacji, który chroni krytyczne dane przed zagrożeniami wewnętrznymi i zewnętrznymi. Dbałość o poufność jest kluczowa dla każdej organizacji, która przetwarza lub przechowuje wrażliwe informacje.

W dobie cyfryzacji i rosnącej zależności od technologii informatycznych kwestia bezpieczeństwa informacji nabiera szczególnego znaczenia. Incydenty bezpieczeństwa mogą mieć poważne konsekwencje dla organizacji, związane ze stratami finansowymi, utratą reputacji oraz naruszeniem przepisów prawnych. Wśród popularnych cyberzagrożeń wyróżniamy między innymi ataki ransomware, phishing, nieautoryzowany dostęp czy incydent bezpieczeństwa teleinformatycznego. Ataki typu ransomware polegają na tym, że przestępcy wykorzystują złośliwe oprogramowanie, aby zaszyfrować dane ofiary i żądają okupu za ich odblokowanie. Przykładem takiego incydentu jest atak WannaCry z 2017 roku, który dotknął setki tysięcy komputerów na całym świecie. Phishing to metoda polegająca na podszywaniu się pod zaufane podmioty w celu wyłudzenia poufnych informacji, takich jak hasła czy dane karty kredytowej. Przykładem może być kampania phishingowa, która miała miejsce w 2020 roku wycelowana w użytkowników platformy Office 365. Nieautoryzowany dostęp to naruszenie bezpieczeństwa polegające na uzyskaniu dostępu do systemów lub danych bez odpowiednich uprawnień. Przykładem może być incydent z 2018 roku, kiedy dane milionów użytkowników Facebooka zostały wykradzione przez firmę Cambridge Analytica. Incydent bezpieczeństwa teleinformatycznego odnosi się do naruszenia bezpieczeństwa systemów telekomunikacyjnych i informatycznych. Może obejmować zarówno fizyczne, jak i cyfrowe ataki na infrastrukturę IT. Przykładem może być atak DDoS (*Distributed Denial of Service*), który polega na przeciążeniu serwera lub sieci przez nadmiar fałszywych żądań, co prowadzi do niedostępności usług dla użytkowników (*Co to jest Triada CIA i na czym polega?*, 2024).

Drugim filarem triady jest integralność (*Integrity*), stanowiąca ochronę przed nieautoryzowanym modyfikowaniem danych. Gwarantuje, że informacje są dokładne i nie zostały zmienione w sposób nieautoryzowany. Integralność zapewnia, że dane są wiarygodne i niezmienione przez osoby nieuprawnione.

Do ochrony integralności służą różne środki, wśród których wyróżniamy sumy kontrolne (*Checksums*). Są to wartości wyliczane na podstawie danych, które pozwalają na weryfikację ich integralności. Jeśli dane zostaną zmienione, suma kontrolna również ulegnie zmianie, sygnalizując potencjalne naruszenie integralności. Podpisy cyfrowe

(*Digital Signatures*) używają kryptografii do weryfikacji autentyczności i integralności danych. Podpis cyfrowy jest generowany przy użyciu klucza prywatnego nadawcy i może być zweryfikowany przy użyciu jego klucza publicznego, co zapewnia, że dane nie zostały zmienione po ich podpisaniu. Mechanizmy Kontroli Wersji (*Version Control Mechanisms*) to systemy kontroli wersji, takie jak Git, które umożliwiają śledzenie zmian w plikach oraz przywracanie wcześniejszych wersji, co pomaga w zarządzaniu i zabezpieczaniu integralności kodu źródłowego oraz dokumentacji (*Co to jest Triada CIA i na czym polega?*, 2024). Systemy wykrywania i zapobiegania włamaniom (IDS/IPS) monitorują sieci i systemy pod kątem podejrzanych aktywności, które mogą wskazywać na próby nieautoryzowanego dostępu lub modyfikacji danych. IDS (*Intrusion Detection System*) wykrywa takie aktywności, a IPS (*Intrusion Prevention System*) podejmuje działania zapobiegawcze. Głównym celem integralności jest zapewnienie, że dane pozostają niezmienione i dokładne przez cały cykl ich życia, od momentu ich utworzenia do momentu wykorzystania. Integralność danych jest kluczowa dla podejmowania prawidłowych decyzji biznesowych, zachowania zgodności z regulacjami oraz utrzymania zaufania użytkowników i klientów. Ochrona integralności danych obejmuje zarówno zabezpieczenia techniczne, jak i procedury operacyjne, które mają na celu zapobieganie nieautoryzowanym modyfikacjom oraz szybkie wykrywanie i reagowanie na potencjalne naruszenia (*Co to jest Triada CIA i na czym polega?*, 2024).

Dostępność, znana również jako *availability*, jest trzecim filarem triady CIA, które definiują podstawowe cele bezpieczeństwa informacji. Dostępność koncentruje się na zapewnieniu, że informacje i systemy informatyczne są dostępne dla uprawnionych użytkowników w momencie, gdy są im potrzebne. Jest to kluczowe dla ciągłości działania organizacji i jej zdolności do realizacji zadań operacyjnych (*Co to jest Triada CIA i na czym polega?*, 2024).

Do środków ochrony dostępności zaliczamy redundancję systemów (*System Redundancy*). Jest to implementacja nadmiarowych systemów i komponentów, takich jak zasilanie awaryjne (UPS), zapasowe serwery i dyski, które mogą przejąć funkcje w przypadku awarii głównego systemu. Kolejnym środkiem są kopie zapasowe (*Backups*). Regularne tworzenie kopii zapasowych danych i systemów umożliwia ich szybkie przywrócenie w przypadku awarii, uszkodzenia lub utraty danych. Kopie zapasowe powinny być przechowywane w bezpiecznych, oddzielnych lokalizacjach. Planowanie ciągłości działania (*Business Continuity Planning*) to metoda mająca na celu opracowanie i wdrożenie planów ciągłości działania, które określają procedury i zasoby potrzebne do utrzymania operacyjności organizacji podczas incydentu i po jego wystąpieniu. Planowanie obejmuje analizę ryzyka, procedury awaryjne oraz testowanie planów. Z kolei systemy odporności na awarie (*Failover Systems*) automatycznie przełączają operacje na zapasowy sprzęt lub oprogramowanie w razie awarii, minimalizując przestoje i zapewniając ciągłość działania. Zabezpieczenia przeciwko atakom DDoS (*DDoS Protection*) polegają na implementacji rozwiązań chroniących przed atakami DDoS (*Distributed Denial of Service*), które mogą przeciążyć i unieruchomić systemy poprzez zalewanie ich ogromną liczbą fałszywych żądań. Zabezpieczenie tego typu może obejmować użycie firewalla, systemów detekcji i mitygacji DDoS oraz usług CDN (*Content Delivery Network*). Głównym celem

dostępności jest zapewnienie, że systemy, aplikacje i dane są dostępne dla uprawnionych użytkowników zawsze, gdy są potrzebne. Dostępność jest kluczowa dla zapewnienia nieprzerwanej działalności biznesowej, efektywności operacyjnej oraz zadowolenia klientów. Dbanie o dostępność wymaga nie tylko technologicznych rozwiązań, ale także procedur operacyjnych i zarządzania ryzykiem. Organizacje muszą być przygotowane na różnorodne zagrożenia, w tym awarie sprzętu, błędy ludzkie, ataki cybernetyczne oraz klęski żywiołowe. Zapewnienie wysokiego poziomu dostępności jest nieodzowne dla utrzymania stabilności i niezawodności systemów informatycznych, co przekłada się na efektywność i sukces organizacji (*Co to jest Triada CIA i na czym polega?*, 2024).

Rola instytucji publicznych w zarządzaniu bezpieczeństwem informacji

Instytucje publiczne spełniają najbardziej istotne zadania w zarządzaniu bezpieczeństwem informacji, ponosząc odpowiedzialność za gromadzenie, przetwarzanie i ochronę danych obywateli. Ich działalność w tym zakresie obejmuje zarówno stosowanie zabezpieczeń technicznych, jak i organizację procesów, podejmowanie decyzji oraz tworzenie właściwych struktur odpowiedzialnych za bezpieczeństwo informacji. Organy administracji pełnią zatem funkcje ustawodawcze, operacyjne, koordynacyjne oraz kontrolne, zapewniając ciągłość funkcjonowania państwa.

Podstawową rolą podmiotów państwowych jest stanowienie prawa, określającego zasady w obszarze bezpieczeństwa informacji. Regulacje, takie jak ustawa o krajowym systemie cyberbezpieczeństwa, ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne oraz przepisy formułujące normy w zakresie ochrony danych osobowych (RODO), wyznaczają ramy funkcjonowania instytucji publicznych w tym zakresie. Wymienione akty nakładają na podmioty administracyjne obowiązek zapewnienia odpowiedniego poziomu informacji poprzez wdrażanie środków organizacyjnych i technicznych adekwatnych do poziomu ryzyka (Włodyka, 2022: 301–306). Przy zarządzaniu tak pojętym zasobem pierwszorzędnym zadaniem staje się utrzymanie podstawowych atrybutów – poufności, integralności oraz dostępności (triada CIA). W instytucjach publicznych szczególne znaczenie przypisuje się typom danych informacyjnych, takim jak informacja publiczna, której udostępnienie stanowi obowiązek ustawowy, oraz informacja niejawna, wymagająca szczególnej ochrony ze względu na interesy państwa. Należy jednak podkreślić, że realizacja tych wymagań wykracza poza ramy ich formalnego spełniania i wiąże się z koniecznością przyjęcia odpowiedniego podejścia organizacyjnego oraz zarządczego (Kifner, 2016: 8–11).

System Zarządzania Bezpieczeństwem Informacji jako narzędzie ochrony danych

W celu zapewnienia skutecznej ochrony zasobów informatycznych organy administracji publicznej wdrażają SZBI – ustrukturyzowane podejście ochrony bezpieczeństwa informacyjnego, oparte na zarządzaniu ryzykiem, a także na wdrażaniu, monitorowaniu i doskonaleniu procedur związanych z bezpieczeństwem informacji. Stosowanie SZBI ma na celu zapewnienie ochrony przed zagrożeniami o różnej skali, minimalizując ryzyko strat, jednocześnie gwarantując autentyczność, rozliczalność i niezawodność danych. Identyfikacja ryzyka ocena zagrożeń i podatności umożliwiają dobranie odpowiednich zabezpieczeń, a także eliminowanie incydentów. SZBI jest ciągłym procesem, który bazuje na modelu PDCA – planuj, wykonuj, sprawdzaj, działaj. Etapy te obejmują kolejno: ustanowienie polityki bezpieczeństwa, wdrożenie zaplanowanych procedur i szkolenie kadry pracowniczej oraz mierzenie wydajności. W długofalowej perspektywie SZBI pozwala również na optymalizację kosztów związanych z usuwaniem awarii (Pietras, 2016: 22–24).

W instytucjach publicznych wdrożenie SZBI staje się szczególnie istotne ze względu na ochronę znacznej ilości danych osobowych. W Polsce podmioty realizujące zadania publiczne są do tego ustawowo zobowiązane, co wynika z Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773).

Istotnym elementem skutecznego zarządzania bezpieczeństwem informacji jest również stosowanie uznanych norm technicznych, które ujednolicają wymagania dotyczące ochrony informacji oraz wspierają organizacje w budowie dojrzałych systemów bezpieczeństwa. Szczególne znaczenie ma rodzina norm ISO/IEC 27000, stanowiąca międzynarodowy standard w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa. Kluczową rolę odgrywa norma ISO/IEC 27001, określająca wymagania dotyczące wdrożenia, utrzymania i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Uzupełnia ją norma ISO/IEC 27002, zawierająca zbiór praktyk oraz środków bezpieczeństwa wspierających zarządzanie ryzykiem. Wdrażanie norm z serii ISO/IEC 27000 pozwala instytucjom publicznym zwiększyć odporność na cyberzagrożenia, zapewnić zgodność z obowiązującymi regulacjami oraz budować zaufanie obywateli do sposobu przetwarzania i ochrony informacji. W praktyce normy te są obecnie uznawane za podstawowy międzynarodowy standard zarządzania bezpieczeństwem informacji i stanowią punkt odniesienia dla wielu krajowych oraz sektorowych regulacji dotyczących cyberbezpieczeństwa.

Struktura i znaczenie Systemu Zarządzania Bezpieczeństwem Informacji dla zapewnienia ciągłości i zaufania do administracji publicznej

Wdrożenie SZBI w instytucjach publicznych pozwala na organizację i koordynację działań związanych z ochroną danych. Rzeczywiste stosowanie procedur, przy odpowiednio realizowanym systemie, wpływa bezpośrednio na zdolność instytucji do zachowania ciągłości działania organów państwowych. Prawidłowa realizacja działań publicznych przekłada się na poziom bezpieczeństwa obywateli, a także na stopień zaufania względem administracji (Pietras, 2016: 23–24).

Skuteczne zarządzanie bezpieczeństwem informacji w instytucjach publicznych implikuje potrzebę odpowiedniego ukształtowania struktury organizacyjnej, uwzględniającej wyspecjalizowane komórki, takie jak Pion Ochrony Informacji, Zespół Reagowania na Incydenty Bezpieczeństwa Informacji wraz z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (*Computer Security Incident Response Team*, w skrócie CSIRT), Inspektor Ochrony Danych oraz audytorzy wewnętrzni. Określenie jednostek i ról organizacyjnych umożliwia sprawowanie nadzoru nad bezpieczeństwem informacji w oparciu o jednoznaczne przypisanie odpowiedzialności (Romaniuk, 2014: 11–15).

Poszczególne komórki organizacyjne realizują odmienne, lecz uzupełniające się zadania. W instytucjach przetwarzających informacje niejawne Pion Ochrony Informacji Niejawnych (w skrócie POIN) jest komórką o priorytetowym znaczeniu, która zarządzana jest przez kierownika jednostki i wyznaczonego pełnomocnika ochrony. POIN zajmuje się przede wszystkim zapewnianiem fizycznej ochrony informacji oraz nadzorem stref bezpieczeństwa i zabezpieczeń miejsc, w których przechowywane są informacje wyłączone z jawności. Do zasadniczych obszarów działalności opisywanej komórki organizacyjnej należy również ochrona sieci systemów wytwarzających i przetwarzających informacje niejawne (Jatkiewicz, 2016: 64). Zespół Reagowania na Incydenty Bezpieczeństwa Informacji (w skrócie ZRIBI) to grupa, której zadaniem jest bieżąca obsługa naruszeń bezpieczeństwa danych jednostek oraz koordynacja działań naprawczych. Zespół analizuje zgłoszenia oraz dokonuje klasyfikacji incydentów, a w przypadku ich stwierdzenia podejmuje działania naprawcze lub kryzysowe (Wołowski, Zawiła-Niedźwiecki, 2012: 145–151). Współpraca między wewnętrznymi ZRIBI a krajowymi grupami CSIRT stanowi podstawę do zarządzania ryzykiem na poziomie całego kraju. Wdrożenie sformalizowanych procedur zgłaszania incydentów do CSIRT wynika z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560 ze zm.). CSIRT stanowi zatem integralny element procedur operacyjnych ZRIBI, co przejawia się w postaci wczesnego ostrzegania podczas przekazywania komunikatów na temat zidentyfikowanych zagrożeń. Wymiana informacji oraz działania zespołów w zakresie gromadzenia dowodów umożliwiają analizę przypadków o ponadsektorowym charakterze (Włodyka, 2022: 304–311).

Powołanie Inspektora Ochrony Danych (w skrócie IOD) stanowi obowiązek dla wszystkich podmiotów sektora publicznego. Osoba pełniąca tę funkcję ponosi ogólną

odpowiedzialność za zapewnienie wdrożenia zabezpieczeń prywatności informacji oraz koordynację zgodności (*Narodowy Standard Cyberbezpieczeństwa NSC 800-12. Bezpieczeństwo informacji – wprowadzenie*, 2023). Wśród głównych zadań IOD znajduje się w szczególności monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych regulacji organizacji. Do jego obowiązków należy również prowadzenie działań audytowych oraz dbałość o realizację szkoleń podnoszących świadomość i kwalifikacje pracowników (Gerwatowski, 2019: 102–103). Z kolei rola audytorów w instytucjach publicznych jest istotna dla zapewnienia transparentności działania jednostki. Działalność podmiotu musi być niezależna i obiektywna, ponieważ audytorzy koncentrują się na nadzorze mechanizmów kontrolnych oraz ich prawidłowości względem ograniczania ryzyka.

Zadania i funkcje kluczowych jednostek odpowiedzialnych za bezpieczeństwo informacji

Zarządzanie bezpieczeństwem informacji w instytucjach publicznych wymaga systemowego podejścia, opartego na określonych strukturach, które posiadają jednoznacznie przypisany obszar odpowiedzialności. Znaczenia przy tym nabiera ciągłość doskonalenia przyjętych rozwiązań i dostosowywanie procedur do zmieniającej się specyfiki zagrożeń. W tym kontekście zasadniczym elementem skutecznego zarządzania bezpieczeństwem informacji staje się analiza i szacowanie ryzyka, a także przygotowanie organizacji do reagowania na sytuacje kryzysowe (Zawiła-Niedźwiecki, Rakoczy, 2018: 50–51).

Szacowanie i zarządzanie ryzykiem bezpośrednio determinują proces zarządzania bezpieczeństwem informacji w instytucjach publicznych. Stanowią podstawę do orzekania w tym obszarze, umożliwiając adekwatny dobór zabezpieczeń oraz funkcjonalne wykorzystanie zasobów. Analiza i szacowanie ryzyka to powiązane etapy jednego procesu, którego punktem wyjścia jest identyfikacja aktywów, zagrożeń oraz podatności systemu. Podczas analizy określa się prawdopodobieństwo wystąpienia zdarzeń oraz ich potencjalnych skutków. Etap szacowania polega na nadaniu ryzyku wartości liczbowej lub jakościowej w celu porównania poszczególnych zagrożeń. Uzyskane rezultaty podlegają ewaluacji w odniesieniu do przyjętych kryteriów akceptowalności (Wiatrak, 2016: 117–120). Wyniki analizy ryzyka mają ścisłe przełożenie na formułowanie strategii bezpieczeństwa informacji. Zapewniają one stosowanie środków proporcjonalnych względem poziomu zagrożeń, co zapobiega zarówno nadmiernemu angażowaniu środków publicznych, jak i pozostawianiu niezgodności w obszarach szczególnie wrażliwych. Szacowanie ryzyka pozwala na hierarchizację działań – priorytety ustalane są poprzez identyfikację zasobów o głównym znaczeniu, których utrata naraziłaby instytucje na najbardziej katastrofalne skutki. W instytucjach publicznych proces ten ma dodatkowy wymiar, wynikający z uwarunkowań prawnych oraz społecznych. Szczególnego znaczenia nabiera konieczność uwzględnienia ryzyka naruszenia praw i wolności osób fizycznych, których dane są przetwarzane (Olender, 2020: 145–146).

Rola planów ciągłości działania i koordynacji w sytuacjach kryzysowych

Zarządzanie kryzysowe, obejmujące działania podejmowane w przypadku incydentów oraz zakłóceń funkcjonowania organizacji, jest koniecznością zabezpieczenia instytucji państwowych oraz przetwarzanych w nich informacji. Jego istotnym elementem są plany ciągłości działania, które określają sposób działania instytucji w przypadku wystąpienia nieprawidłowości (Bajor, Krakowiak, 2018: 652–654).

Aktywność współczesnej administracji jest w dużym stopniu uzależniona od sprawności systemów informatycznych. Podstawowym celem zarządzania kryzysowego jest utrzymanie ciągłości działania instytucji oraz szybkie przywrócenie ich biegłości w wykonywaniu zadań. Zasadniczo oznacza to konieczność przygotowania podmiotów publicznych do działania w warunkach zakłóceń, w których decyzje są podejmowane pod presją czasu oraz ograniczonego dostępu do informacji (Majchrzak, 2018: 39–42). W tym zakresie decydującą rolę odgrywają plany ciągłości działania. Obejmują one między innymi identyfikację procesów krytycznych, ocenę prawdopodobieństwa, a następnie działania związane z odtwarzaniem systemów, zapewnieniem alternatywnych kanałów komunikacji oraz organizacją pracy w warunkach awaryjnych. Skuteczność planów ciągłości działania zależy jednak od ich regularnego testowania oraz aktualizacji.

Istotnym elementem procesów zarządzania kryzysowego jest również zapewnienie sprawnego obiegu informacji. W sytuacjach nadzwyczajnych dostęp do aktualnych danych stanowi podstawę do podejmowania decyzji o rozwiązaniach kryzysu, a zakłócenia w przepływie informacji mogą doprowadzić do pogłębiania skutków incydentów. Zarządzanie kryzysowe w obszarze bezpieczeństwa informacji wymaga także koordynacji struktur organizacyjnych oraz współpracy pomiędzy zespołami reagowania. Skuteczność zharmonizowania podmiotów odpowiedzialnych za bezpieczeństwo pozwala na szybsze wykrywanie zagrożeń oraz minimalizację ich skutków (Bajor, Krakowiak, 2018: 654–657). W konsekwencji reagowanie kryzysowe oraz instrukcje odnośnie do utrzymania procesów administracyjnych stanowią konieczny filar w zapewnianiu odporności instytucji publicznych, umożliwiając przejście od podejścia reaktywnego do proaktywnego zarządzania bezpieczeństwem informacji.

Rola ludzi w bezpieczeństwie informacji

Rola ludzi w bezpieczeństwie informacji jest często określana jako najważniejszy i jednocześnie najsłabszy element systemu ochrony danych. Wynika to z faktu, że człowiek podejmuje decyzje, działa pod presją czasu, bywa zmęczony i popełnia błędy. Dlatego skuteczne zarządzanie bezpieczeństwem musi uwzględniać nie tylko technologie, ale przede wszystkim zachowania i świadomość pracowników (Whitman, Mattord, 2021: 34–36).

Szkolenia jako fundament bezpieczeństwa

Aby zmniejszyć ryzyko związane z błędami ludzkimi, organizacje muszą inwestować w edukację i szkolenie swoich pracowników. Regularne programy szkoleń z zakresu bezpieczeństwa informatycznego pomagają zwiększyć świadomość na temat zagrożeń, takich jak phishing, ransomware czy zagrożenia związane z zarządzaniem hasłami (Stallings, Brown, 2019: 210–214).

Szkolenia nie powinny być jednorazowym wydarzeniem, lecz procesem ciągłym. W praktyce oznacza to: szkolenia wstępne (onboardingowe), okresowe, specjalistyczne oraz symulacje. Za sprawą szkolenia wstępnego każdy nowy pracownik powinien od początku wiedzieć, jakie dane są chronione, jakie są podstawowe zasady bezpieczeństwa, jakie konsekwencje mają naruszenia (Whitman, Mattord, 2021: 96–99). Szkolenia okresowe przypominają i aktualizują wiedzę, ponieważ zagrożenia stale się zmieniają. Szkolenia specjalistyczne przeznaczone są dla osób mających dostęp do wrażliwych danych lub systemów (na przykład finanse, HR, administracja IT). Symulacje (na przykład phishingowe) pozwalają sprawdzić reakcje pracowników w praktyce i uczą przez doświadczenie.

Największym problemem nie jest brak wiedzy, ale brak jej stosowania. Dlatego ważne jest budowanie kultury bezpieczeństwa. Przykładem codziennych sytuacji jest na przykład kliknięcie linku z podejrzanego e-maila, używanie tego samego hasła w wielu systemach czy zostawienie odblokowanego komputera. Świadomy pracownik zatrzyma się i pomyśli przed działaniem, zweryfikuje nadawcę wiadomości, zgłosi coś, co wydaje się „podejrzane" – nawet jeśli nie ma pewności.

Procedury i polityki – wsparcie dla ludzi

Procedury mają pomagać w pracy, a nie ją utrudniać. Jeśli są zbyt skomplikowane, pracownicy ignorują je, szukają „skrótów", obchodzą zabezpieczenia. Jakie powinny być dobre procedury – jasne i krótkie, odpowiadające na konkretne sytuacje („co zrobić, gdy…"), łatwo dostępne (na przykład intranet, checklisty) oraz regularnie aktualizowane (*Rola czynnika ludzkiego w bezpieczeństwie informatycznym*, b.r.).

Błędy ludzkie

Błędy w konfiguracji systemów i aplikacji. Nieprawidłowa konfiguracja systemów i aplikacji może prowadzić do poważnych luk w zabezpieczeniach. Wśród przykładów można wymienić pozostawienie domyślnych haseł, otwarte porty na serwerach czy niewłaściwie ustawione uprawnienia dostępu. W takich przypadkach nawet najbardziej zaawansowane technologie ochrony nie będą wystarczające, jeśli użytkownicy lub administratorzy nie zadbają o odpowiednią konfigurację. Błędne zarządzanie dostępem i uprawnieniami, czyli nieodpowiednie przypisanie uprawnień do systemów i zasobów może prowadzić do sytuacji, w której osoby nieautoryzowane uzyskują dostęp do wrażliwych danych.

Często spotykanym problemem jest nadawanie zbyt szerokich uprawnień, co zwiększa ryzyko wycieku lub modyfikacji danych (Stallings, Brown, 2019: 210–214).

Phishing i socjotechnika

Zdarzenia związane z phishingiem są jednym z najczęstszych sposobów, w jaki cyberprzestępcy zdobywają dostęp do systemów informatycznych. Użytkownicy mogą zostać oszukani i kliknąć link prowadzący do złośliwej strony, pobrać zainfekowane oprogramowanie lub ujawnić swoje dane logowania. Tego rodzaju ataki opierają się na manipulacji psychologicznej, a ich skuteczność zależy od poziomu świadomości użytkowników (*Rola czynnika ludzkiego w bezpieczeństwie informatycznym*, b.r.).

Zła praktyka w zakresie zarządzania hasłami

Niewłaściwe zarządzanie hasłami, takie jak używanie słabych haseł, powielanie haseł w różnych systemach czy ich zapisywanie w niechronionych miejscach, stanowi ogromne ryzyko. Użytkownicy często ignorują zasady dotyczące tworzenia silnych haseł lub zmieniają je zbyt rzadko, co stwarza przestrzeń dla ataków. Każdy pracownik powinien przede wszystkim przestrzegać zasad bezpieczeństwa, chronić dane (na przykład klientów, firmy), zgłaszać incydenty i podejrzane sytuacje oraz brać udział w szkoleniach. Czynnik ludzki ma ogromny wpływ na poziom bezpieczeństwa informacji. Nawet najbardziej zaawansowane technologie nie zastąpią świadomego użytkownika. Dlatego organizacje powinny inwestować w: edukację, budowanie nawyków, proste i skuteczne procedury, kulturę odpowiedzialności (Stallings, Brown, 2019: 112–115).

Analiza wybranych incydentów bezpieczeństwa informacji

Analiza rzeczywistych incydentów bezpieczeństwa informacji pozwala lepiej zrozumieć konsekwencje niewystarczających zabezpieczeń oraz znaczenie skutecznego zarządzania bezpieczeństwem informacji w administracji publicznej.

Atak ransomware na infrastrukturę Urzędu Marszałkowskiego Województwa Mazowieckiego (2022)

W grudniu 2022 roku doszło do ataku z wykorzystaniem złośliwego oprogramowania typu ransomware na infrastrukturę Węzła Regionalnego Urzędu Marszałkowskiego Województwa Mazowieckiego. W wyniku incydentu zaszyfrowane zostały pliki wykorzystywane przez systemy informatyczne obsługujące projekty realizowane wspólnie z jednostkami samorządu terytorialnego. Atak spowodował utratę dostępności części danych oraz czasowe zakłócenia w funkcjonowaniu usług elektronicznych. Urząd zgłosił incydent do CSIRT

NASK oraz Prezesa Urzędu Ochrony Danych Osobowych, a następnie rozpoczął proces odtwarzania systemów z kopii zapasowych. Przypadek ten pokazuje, że odpowiednie procedury reagowania na incydenty, wykonywanie kopii zapasowych oraz współpraca z krajowymi zespołami reagowania stanowią podstawowe elementy skutecznego Systemu Zarządzania Bezpieczeństwem Informacji.

Atak WannaCry na brytyjską służbę zdrowia NHS (2017)

Jednym z najbardziej znanych incydentów cyberbezpieczeństwa był globalny atak ransomware WannaCry z maja 2017 roku, który objął ponad 200 tysięcy komputerów w ponad 150 państwach. Szczególnie dotkliwe skutki odnotowała brytyjska służba zdrowia (NHS), gdzie zablokowanie systemów informatycznych doprowadziło do odwołania zabiegów, utrudnień w dostępie do dokumentacji medycznej oraz zakłóceń w funkcjonowaniu placówek ochrony zdrowia. Analizy wykazały, że jedną z głównych przyczyn skuteczności ataku był brak instalacji wcześniej udostępnionych aktualizacji bezpieczeństwa systemów Windows. Przypadek WannaCry unaocznił znaczenie zarządzania podatnościami, regularnego aktualizowania oprogramowania, planów ciągłości działania oraz wdrażania standardów zarządzania bezpieczeństwem informacji, takich jak ISO/IEC 27001.

Zakończenie

Zarządzanie bezpieczeństwem informacji w instytucjach publicznych jest procesem złożonym i wielowymiarowym, który wymaga integracji działań na wielu płaszczyznach. Obejmuje ono zarówno tworzenie oraz stosowanie odpowiednich regulacji prawnych, wdrażanie rozwiązań technologicznych, jak i budowanie efektywnych struktur organizacyjnych odpowiedzialnych za ochronę danych. Szczególne znaczenie ma w tym kontekście System Zarządzania Bezpieczeństwem Informacji, który umożliwia systematyczne podejście do identyfikacji zagrożeń, analizy ryzyka oraz wdrażania adekwatnych środków ochrony. Niezwykle istotne jest także zapewnienie ciągłości działania instytucji poprzez odpowiednie przygotowanie na sytuacje kryzysowe oraz opracowanie i testowanie planów awaryjnych. Nie można jednak zapominać, że nawet najbardziej zaawansowane technologie nie są w stanie zagwarantować pełnego bezpieczeństwa bez udziału świadomych i odpowiednio przeszkolonych pracowników. Czynnik ludzki odgrywa kluczową rolę w całym systemie ochrony informacji, dlatego konieczne jest ciągłe podnoszenie kompetencji oraz budowanie kultury bezpieczeństwa w organizacjach publicznych. Tylko holistyczne podejście, łączące aspekty techniczne, organizacyjne i społeczne, pozwala na skuteczne przeciwdziałanie zagrożeniom oraz minimalizowanie skutków incydentów. W rezultacie właściwie zarządzane bezpieczeństwo informacji przyczynia się nie tylko do ochrony danych, lecz także do zwiększenia efektywności działania administracji oraz wzmacniania zaufania obywateli do instytucji publicznych.

Bibliografia

Bajor T., Krakowiak M. (2018), *Zarządzanie kryzysowe a bezpieczeństwo informacji*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa", t. 6, s. 649–659, https://doi.org/10.16926/tiib.2018.06.46

Co to jest Triada CIA i na czym polega? (2024), https://cyberthreat.pl/co-to-jest-triada-cia/ [dostęp: 13.04.2026].

Gerwatowski J. (2019), *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, „Studia Prawnoustrojowe", nr 44, s. 89–106, https://doi.org/10.31648/sp.4897

Incydenty bezpieczeństwa – definicja, przykłady i zarządzanie (2024), https://nafalinauki.pl/incydenty-bezpieczenstwa/ [dostęp: 15.04.2026].

ISO/IEC 27001:2022 (2022), *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, Geneva: International Organization for Standardization (ISO).

Jatkiewicz P. (2016), *Zarządzanie bezpieczeństwem w jednostkach samorządowych*, [w:] T. Szatkowski (red.), *Bezpieczeństwo danych w sektorze publicznym*, Warszawa: Polskie Towarzystwo Informatyczne, s. 57–77.

Kifner T. (2016), *Elementy kultury organizacji IT wspomagające wdrażanie systemu bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji*, [w:] T. Szatkowski (red.), *Bezpieczeństwo danych w sektorze publicznym*, Warszawa: Polskie Towarzystwo Informatyczne, s. 7–28.

Majchrzak D. (2018), *O zarządzaniu kryzysowym inaczej. Zarządzanie kryzysowe czy zarządzanie bezpieczeństwem?*, „Kwartalnik Bellona", nr 4, s. 39–61.

Narodowy Standard Cyberbezpieczeństwa NSC 800-12. Bezpieczeństwo informacji – wprowadzenie (2023), https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber [dostęp: 12.04.2026].

Olender A. (2020), *Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego*, „Wschód Europy. Studia humanistyczno-społeczne", vol. 6(2), s. 145–157, https://doi.org/10.17951/we.2020.6.2.145-157

Pietras E. (2016), *Zagadnienia zarządzania bezpieczeństwem informacji w organizacji*, „Zarządzanie Przedsiębiorstwem", vol. 19, nr 1, s. 22–28.

Rola czynnika ludzkiego w bezpieczeństwie informatycznym (b.r.), https://cybersec24.pl/2025/02/rola-czynnika-ludzkiego-w-bezpieczenstwie-informatycznym/ [dostęp: 12.04.2026].

Romaniuk P. (2014), *Zarządzanie systemami bezpieczeństwa informacji w administracji publicznej z wykorzystaniem instytucji audytu wewnętrznego*, [w:] M. Sitek, I. Niedziółka, A. Ukleja (red.), *Wymiary ochrony informacji i polityki bezpieczeństwa. Państwo – Prawo – Społeczeństwo*, Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, s. 7–22.

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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE z 2019 r., L 119/1).

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r., poz. 773).

Stallings W., Brown L. (2019), *Bezpieczeństwo systemów informatycznych. Zasady i praktyka*, t. 1, Gliwice: Helion.

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

Whitman M., Mattord H. (2021), *Principles of Information Security*, Boston: Cengage Learning.

Wiatrak L. (2016), *Zarządzanie ryzykiem wewnętrznym w organach administracji publicznej*, „Studia Ekonomiczne", vol. 298, s. 115–129.

Włodyka E.M. (2022), *Samorządowa administracja publiczna wobec cyberprzestrzeni: bezpieczeństwo informacji a praktyka zgłaszania w samorządzie terytorialnym osób do kontaktu z CSIRT NASK*, „Studia Gdańskie", t. XVIII, s. 301–314.

Wołowski F., Zawiła-Niedźwiecki J. (2012), *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Kraków: edu-Libri.

Zawiła-Niedźwiecki J., Rakoczy A. (2018), *Publiczne zarządzanie kryzysowe w działalności instytucji finansowych*, „Studia i Materiały", nr 1(26), s. 48–54, https://doi.org/10.7172/1733-9758.2018.26.4

O autorach

Gabriel Kagankiewicz – student drugiego roku studiów licencjackich na kierunku bezpieczeństwo wewnętrzne. Interesuje się zagadnieniami związanymi z cyberbezpieczeństwem oraz zarządzaniem systemami teleinformatycznymi w administracji publicznej. Jest członkiem Koła Naukowego „Jurysta".

Wiktoria Urbańska – studentka drugiego roku studiów licencjackich na kierunku bezpieczeństwo wewnętrzne. Interesuje się zagadnieniami związanymi z cyberbezpieczeństwem, kryminalistyką cyfrową oraz analizą incydentów. Jest członkinią Koła Naukowego „Jurysta".

About the Authors

Gabriel Kagankiewicz – a second-year undergraduate student in Internal Security. His interests include cybersecurity and the management of ICT systems in public administration. He is a member of the Research Club "Jurysta".

Wiktoria Urbańska – a second-year undergraduate student in Internal Security. Her interests include cybersecurity, digital forensics, and incident analysis. She is a member of the Research Club "Jurysta".

Ten utwór jest dostępny na licencji Creative Commons Uznanie autorstwa-Na tych samych warunkach 4.0 Międzynarodowe.

Open Access