Zarządzanie bezpieczeństwem informacji w świetle dyrektywy NIS2 – obowiązki, wyzwania prawne i organizacyjne przedsiębiorstw

Agnieszka Baran

Politechnika Białostocka, Wydział Inżynierii Zarządzania

e-mail: a.baran@pb.edu.pl

Klaudia Gierejko

Politechnika Białostocka, Wydział Inżynierii Zarządzania

e-mail: klaudiagierejko2@gmail.com

DOI: 10.65731/az-2026-0035

Streszczenie

Zagadnienie zarządzania bezpieczeństwem informacji w obliczu narastających cyberataków na świecie staje się niezwykle istotne dla każdej organizacji. Dane z różnego rodzaju raportów wskazują na coraz częstsze ataki na zasoby informacyjne nie tylko instytucji publicznych, ale również przedsiębiorstw z sektora MŚP. Unia Europejska w ramach prac nad nową legislacją w tym zakresie dąży do harmonizacji w podejściu do bezpieczeństwa informacji. Celem artykułu jest przegląd zmian wprowadzonych dyrektywą NIS2, ocena skutków prawnych i organizacyjnych dla przedsiębiorstw oraz wskazanie wyzwań w zakresie zarządzania bezpieczeństwem informacji. Obowiązki wynikające z nowej legislacji są wyzwaniem dla przedsiębiorców pod względem prawnym, ale i organizacyjnym. Najczęstsze wyzwania obecnie to problemy z interpretacją przepisów oraz nowych pojęć zawartych w dyrektywie, brak ekspertów w zakresie cyberbezpieczeństwa, ograniczona świadomość zagrożeń wśród kadry zarządzającej. Świadomość cyberataków pozostaje niska, co prowadzi do marginalizacji inwestycji w bezpieczeństwo i niewystarczającej liczby programów szkoleniowych dla pracowników.

Słowa kluczowe

Dyrektywa NIS2, Unia Europejska, system zarządzania bezpieczeństwem informacji

Wstęp

Według Eurostatu w 2023 r. około 22% przedsiębiorstw w UE odczuło różne konsekwencje z powodu incydentów związanych z bezpieczeństwem Technologii Informacyjno-Komunikacyjnych [Statistics Explained, 2026]. Nieustannie rośnie liczba ataków cybernetycznych zarówno na sektor prywatny, jak i administrację publiczną. Najczęściej są to ataki ransomware, ataki e-mailowe, w tym phishing. Ataki koncentrują się również na zakłócaniu łańcuchów dostaw, czemu sprzyjały pandemia w latach 2020-2023 oraz konflikt zbrojny na Ukrainie [Vandezande, 2024, s. 2]. Cyberprzestrzeń stała się przestrzenią komunikacyjną tworzoną przez system powiązań internetowych. „Jest obszarem zarówno kooperacji pozytywnej, prowadzącej do rozwoju w sferze edukacji, komunikacji społecznej czy gospodarki narodowej, jak i zjawisk negatywnych przybierających postać cybeprzestępczości czy cyberwojny" [Chałubińska-Jentkiewicz, 2019, s. 12]. W 2016 roku UE przyjęła dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych, której celem było narzucenie operatorom niektórych usług kluczowych i operatorom usług cyfrowych wspólnego poziomu cyberbezpieczeństwa w UE [Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148]. Dyrektywa NIS nałożyła na państwa członkowskie UE obowiązek przyjęcia krajowej strategii bezpieczeństwa sieci i systemów informatycznych. Dyrektywa NIS została wdrożona do prawa polskiego w drodze ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Dz.U. z 2026 r. poz. 20, 252]. Ponieważ państwa członkowskie UE implementowały dyrektywę NIS w odmienny sposób, doprowadziło to do znaczących różnic w podejściu do cyberbezpieczeństwa i niewystarczającego przygotowania podmiotów objętych przepisami prawa, w 2023 roku weszła w życie Dyrektywa NIS2 [Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555], która wprowadziła surowsze wymagania w zakresie cyberbezpieczeństwa. Dyrektywa NIS2 wymaga tworzenia krajowych strategii i wzmożonej współpracy transgranicznej w zakresie reagowania i egzekwowania jej przepisów.

Przy pisaniu artykułu zastosowano metody badawcze o charakterze jakościowym, ukierunkowane na analizę i ocenę aktualnego stanu wiedzy oraz obowiązującą regulację w obszarze zarządzania bezpieczeństwem informacji. Podstawową metodą badawczą była analiza literatury przedmiotu obejmująca opracowania naukowe odnoszące się do zagadnień zarządzania bezpieczeństwem informacji. Metoda formalno-dogmatyczna mająca na celu analizę aktów prawnych pozwoliła na ocenę spójności i efektywności rozwiązań normatywnych realizacji celów polityki Unii Europejskiej w zakresie cyberbezpieczeństwa.

Celem artykułu jest przegląd zmian wprowadzonych dyrektywą NIS2, ocena skutków prawnych i organizacyjnych dla przedsiębiorstw oraz wskazanie wyzwań w zakresie zarządzania bezpieczeństwem informacji.

1. Przegląd literatury

1.1. Zarządzanie bezpieczeństwem informacji

W literaturze przedmiotu pojęcie bezpieczeństwa informacyjnego definiowane jest zazwyczaj jako zbiór działań organizacyjnych, prawnych i technicznych mających na celu ochronę zasobów informacyjnych przed zagrożeniami. „Bezpieczeństwo informacyjne bardzo często rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania" [Liedel, 2006, s. 19]. Bezpieczeństwo informacji rozumiane jest również jako „ochrona przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych" [Pietras, 2016, s. 22]. Informację uznaje się za bezpieczną, gdy zagwarantowane są takie atrybuty jak: poufność, spójność, dostępność rozliczalność, autentyczność, niezaprzeczalność i niezawodność. Oznacza to przede wszystkim, że informacja nie jest udostępniana osobom nieuprawnionym, dane nie są zmieniane w sposób nieautoryzowany, zapewniona jest dokładność i kompletność aktywów, zaś dostęp do danych jest możliwy dla uprawnionych użytkowników i jest on łatwy, szybki i niczym nie zakłócony [Pietras, 2016, s. 23]. W literaturze wymienia się środki ochrony informacji i są to „środki organizacyjno-proceduralne, personalne, fizyczne czy techniczne. Zaś system ochrony obejmuje takie obszary funkcjonalne, jak: bezpieczeństwo fizyczne, zabezpieczenie procesu przetwarzania informacji, zabezpieczenie sprzętu, zabezpieczenie dostępu do systemu informatycznego, zabezpieczenie procesu wymiany informacji czy audyt bezpieczeństwa informacji" [Jarmoszko, 2016, s. 42]. Skala i zakres problemów, jakie obserwuje się, a które powstają w wyniku braku świadomości ryzyka wynikającego m.in. z utraty zasobów informacyjnych, generują istotne zagrożenie dla sprawności i efektywności funkcjonowania przedsiębiorstw. Utrzymanie bezpieczeństwa i podejmowanie działań w celu ochrony zasobów informacyjnych jest niezbędne w odniesieniu do każdej organizacji, dlatego tak istotne jest efektywne zarządzanie bezpieczeństwem informacyjnym.

Do kwestii bezpieczeństwa informacji odnosi się pakiet norm ISO/IEC 27000 dotyczący systemu zarządzania bezpieczeństwem informacji (SZBI, Information Security Management Systems, ISMS) (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC

27005). „Celem standardów jest między innymi zapewnienie bezpieczeństwa kluczowym zasobom, zarządzanie ryzykiem, stosowanie najlepszych praktyk, uniknięcie szkód dla marki, straty zysków i potencjalnych kar i rozwój systemów informacyjnych" [Wiśniewski, 2018, s. 132]. „Przewodnik dotyczący systemowego zarządzania bezpieczeństwem informacji ISO/IEC 27002 definiuje je jako zachowanie trzech cech informacji: poufności (confidentiality), spójności (integrity) oraz dostępności (availability)" [Łuczak, 2004]. Ryzyka w zakresie bezpieczeństwa informacji mogą zmieniać się w zależności od różnych okoliczności, dlatego podkreśla się wagę takich działań jak: monitorowanie i ocenianie skuteczności wdrożonych procedur bezpieczeństwa i procedur, identyfikację pojawiających się zagrożeń, które wymagają podjęcia działań, wybieranie, wdrażanie i doskonalenie odpowiednich zabezpieczeń. Aby skoordynować te działania organizacja musi zdefiniować własną politykę i cele bezpieczeństwa informacji, korzystając z systemu zarządzania bezpieczeństwem informacji [Górka-Chowaniec i Popek, 2024]. Ochrona informacji w organizacji wymaga strategii zarządzania, która zminimalizuje ryzyka związane z systemami informacyjnymi i infrastrukturą IT, ochroną danych osobowych i danych poufnych z zakresu własności intelektualnej. Dowodem na istotne znaczenie takiej strategii są duże korporacje z branży IT (Google, Microsoft czy IBM), gdzie w sposób naturalny zarządzanie bezpieczeństwem informacji jest traktowane jako kluczowy element długoterminowej strategii [Marynowicz, 2025, s. 94].

Obecnie zarządzanie bezpieczeństwem informacji stanowi podstawę skutecznego zarządzania przedsiębiorstwem. W erze dynamicznych zmian technologicznych, cyberzagrożeń i rosnącej liczby ataków na dane, system zarządzania bezpieczeństwem informacji (SZBI) nie tylko chroni przed nieuprawnionym dostępem, ale stanowi również integralną część strategii organizacyjnej [Marynowicz, 2025, s. 88]. Wielu autorów określa, iż SZBI jest „jednym z wielu podsystemów zarządzania funkcjonujących we współczesnych, dobrze zarządzanych organizacjach" [Ożarek, 2013, s. 52; Fleszer, 2018, s. 194]. Bezpieczeństwo informacji traktowane jest jako strategiczny zasób każdej organizacji, równie ważny jak zasoby finansowe, ludzkie czy technologiczne. Dlatego też właściwe zarządzanie tym zasobem warunkuje efektywność procesów decyzyjnych i strategicznych. Zgodnie z normą ISO/IEC 27000:2018 bezpieczeństwo informacji oznacza zachowanie poufności, integralności i dostępności informacji, a także – w niektórych kontekstach – zapewnienie autentyczności, rozliczalności i niezawodności systemów informacyjnych [International Organization for Standardization, 2018]. Norma ISO/IEC 27000:2018 prezentuje model zarządzania bezpieczeństwem informacji. Międzynarodowa Organizacja Normalizacyjna (ISO) opracowuje liczne rodziny norm dotyczących systemów zarządzania, stanowiących wyodrębnione obszary zarządzania organizacją, takie jak

system zarządzania jakością (QMS, Quality Management System) czy system zarządzania ciągłością działania (BCMS, Business Continuity Management). Standardy te opierają się na wspólnych zasadach, obejmujących podejście systemowe i procesowe, orientację na zarządzanie ryzykiem oraz koncepcję ciągłego doskonalenia. System Zarządzania Bezpieczeństwem Informacji (SZBI) należy do rodziny norm opracowywanych wspólnie przez ISO oraz Międzynarodową Komisję Elektrotechniczną (IEC). Standardy te tworzą spójne ramy dla projektowania, wdrażania i doskonalenia rozwiązań w zakresie ochrony informacji w organizacjach, stanowiąc element szerszego podejścia do zarządzania opartego na ustrukturyzowanych i międzynarodowo uznanych wymaganiach [Szmit, 2025, s. 11]. W ujęciu potocznym bezpieczeństwo utożsamiane jest ze stanem braku zagrożenia oraz poczuciem stabilności i spokoju. Dynamiczny rozwój technologii teleinformatycznych doprowadził jednak do wyodrębnienia szczególnego obszaru bezpieczeństwa, odnoszącego się do systemów teleinformatycznych oraz środowisk ich funkcjonowania. W tym kontekście bezpieczeństwo oznacza zapewnienie niezakłóconego, ciągłego i zgodnego z przeznaczeniem działania systemów, przy jednoczesnej ochronie przetwarzanych informacji oraz świadczonych usług. Obejmuje ono takie kształtowanie i nadzorowanie infrastruktury technicznej oraz organizacyjnej, aby realizacja zadań przypisanych systemom odbywała się w sposób stabilny i niezawodny, z uwzględnieniem interesu oraz dobra danej instytucji [Rychły-Lipińska i Kamiński, 2024, s. 106]. Natomiast w ujęciu funkcjonowania współczesnych organizacji, które w rosnącym stopniu opierają swoją działalność na rozwiązaniach cyfrowych bezpieczeństwo informacji stanowi fundamentalny element. Obejmuje ono działania ukierunkowane na zapewnienie poufności, integralności oraz dostępności danych, a także na ochronę zasobów informacyjnych przed nieautoryzowanym dostępem, nieuprawnioną modyfikacją oraz ich utratą [Rychły-Lipińska i Kamiński, 2014, s. 108]. Standardy ISO/IEC 27000 obejmują zestaw sformalizowanych zasad i zaleceń, które wspierają redukcję rosnącej liczby zagrożeń, umożliwiają eliminację zidentyfikowanych podatności oraz przyczyniają się do systematycznego doskonalenia poziomu bezpieczeństwa organizacji [Meriah i Ben Arfa Rabai, 2019, s. 86]. Norma ISO/IEC 27000, została opracowana w celu przedstawienia ogólnego przeglądu zagadnień związanych z systemem zarządzania bezpieczeństwem informacji oraz ujednolicenia terminologii stosowanej w tym obszarze. Dokument ten porządkuje podstawowe pojęcia i definicje, redukując ryzyko niejednoznaczności interpretacyjnych, które mogą negatywnie wpływać na rozumienie oraz wdrażanie zasad bezpieczeństwa informacji w procesach biznesowych. Istotnym elementem podejścia promowanego w ramach tej rodziny norm jest cykl ciągłego doskonalenia Plan-Do-Check-Act

(PDCA), stanowiący fundament systemowego zarządzania bezpieczeństwem. Z kolei norma ISO/IEC 27001, określa wymagania umożliwiające organizacjom wdrożenie oraz certyfikację systemu zarządzania bezpieczeństwem informacji. Jej zasadniczym celem jest ustanowienie, wdrożenie, utrzymanie i ciągłe doskonalenie SZBI poprzez zastosowanie adekwatnych mechanizmów kontrolnych, służących ochronie zasobów informacyjnych oraz minimalizacji ryzyka związanego z ich utratą, naruszeniem integralności lub poufności [Tamimi i in., 2019, s. 121]. Implementacja norm z serii ISO/IEC 27000 może przynieść organizacjom wielowymiarowe korzyści. Do najważniejszych zalicza się wzrost wiarygodności w relacjach z interesariuszami, ograniczenie ryzyka incydentów związanych z naruszeniem poufności danych, usprawnienie procesów operacyjnych oraz zwiększenie poziomu zgodności z obowiązującymi regulacjami prawnymi i wymaganiami branżowymi. Stosowanie tych standardów stanowi również wyraz świadomego i systemowego podejścia do ochrony informacji, sprzyjając zabezpieczeniu kluczowych zasobów organizacji [Metin i in., 2025, s. 8]. Zgodnie z normą ISO/IEC 27000 bezpieczeństwo informacji oznacza zachowanie poufności, integralności oraz dostępności informacji. W ujęciu rozszerzonym uwzględnia się również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność oraz niezawodność, które wspólnie determinują kompleksowy poziom ochrony zasobów informacyjnych [Szmit, 2025, s. 16]. Norma ISO/IEC 27001 stanowi międzynarodowy standard określający wymagania dotyczące systemów zarządzania bezpieczeństwem informacji. Dokument ten precyzuje zasady ustanawiania, wdrażania, utrzymywania oraz ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w organizacji. Ponadto norma formułuje wytyczne odnoszące się do identyfikacji, analizy oraz postępowania z ryzykiem w obszarze bezpieczeństwa informacji [Rychły-Lipińska i Kamiński, 2024, s. 110]. Nakłada na organizacje obowiązek systematycznej identyfikacji, analizy oraz postępowania z ryzykiem w obszarze bezpieczeństwa informacji, opierając się na zasadzie ciągłego doskonalenia. Uzupełnieniem tych wymagań jest norma ISO/IEC 27005, która dostarcza szczegółowych wytycznych dotyczących procesu zarządzania ryzykiem. Określa ona metodyczne podejście obejmujące identyfikację zagrożeń, analizę i ocenę ryzyka, dobór sposobów jego traktowania, a także monitorowanie i przegląd przyjętych rozwiązań. Zastosowanie tej normy wspiera organizacje w ustalaniu priorytetów działań oraz racjonalnym wykorzystaniu dostępnych zasobów w obszarze bezpieczeństwa informacji [Metin i in., 2025, s. 8]. Zgodnie ze stanowiskiem autorów, norma ISO/IEC 27001 stanowi narzędzie wspierające organizacje w realizacji wymogów prawnych i regulacyjnych odnoszących się do bezpieczeństwa informacji w warunkach pracy zdalnej poprzez zastosowanie kompleksowych mechanizmów systemowych, w szczególności: ustanowienie ramowego

standardu zgodności, umożliwiającego strukturalne podejście do spełniania wymogów regulacyjnych, systematyczne uwzględnianie obowiązujących przepisów prawa w procesach zarządzania bezpieczeństwem informacji, identyfikację oraz zarządzanie ryzykiem braku zgodności, w tym analizę potencjalnych konsekwencji prawnych i organizacyjnych, wdrażanie mechanizmów ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji, a także wzmacnianie wiarygodności organizacji oraz budowanie zaufania ze strony organów regulacyjnych i nadzorczych [Rychły-Lipińska i Kamiński, 2014, s. 111].

1.2. Prawne aspekty kształtowania systemów zarządzania bezpieczeństwem informacji

Unia Europejska na przestrzeni ostatnich lat aktywnie tworzy regulacje prawne w zakresie cyberbezpieczeństwa. Do tej pory nie było jednak kompleksowego aktu prawnego dotyczącego bezpieczeństwa cyfrowego sieci i systemów informatycznych. Funkcjonowały natomiast przepisy, które częściowo odnosiły się do bezpieczeństwa informacji, infrastruktury krytycznej i ochrony danych. Pierwszą dyrektywą regulującą kompleksowo kwestie cyberbezpieczeństwa była dyrektywa NIS (*Network and Information Security Directive*, Dyrektywa (UE) 2016/1148), która ustanowiła pierwszy wspólny poziom bezpieczeństwa sieci i systemów informatycznych w państwach członkowskich. Dyrektywa ta zobowiązała państwa członkowskie do stworzenia krajowych strategii cyberbezpieczeństwa, ustanowienia właściwych organów oraz punktów kontaktowych ds. bezpieczeństwa sieci i informacji. Głównym celem było ograniczenie ryzyka incydentów w kluczowych sektorach gospodarki i administracji publicznej. W 2022 roku weszła w życie dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, która zastąpiła poprzednią dyrektywę i znacząco zmieniła ramy cyberbezpieczeństwa w UE.

Dyrektywa NIS2 nakazuje wdrożenie środków organizacyjnych, technicznych i proceduralnych, co ma wpływ na konstrukcję systemu zarządzania bezpieczeństwem informacji. Dyrektywa NIS2 nakłada na państwa członkowskie obowiązek zwiększenia zdolności w zakresie cyberbezpieczeństwa. Wprowadza środki zarządzania ryzykiem i wymogi dotyczące sprawozdawczości dla podmiotów z różnych sektorów. Ustanawia zasady współpracy, wymiany informacji, nadzoru i egzekwowania środków cyberbezpieczeństwa. Celem dyrektywy NIS2 jest wyeliminowanie różnic w wymogach cyberbezpieczeństwa między państwami członkowskimi. Ma

to nastąpić poprzez ustanowienie minimalnych zasad skoordynowanych ram regulacyjnych. Dyrektywa ustanawia mechanizmy skutecznej współpracy między organami w różnych państwach członkowskich. Nowe przepisy rozszerzają katalog podmiotów kluczowych i ważnych. Są to przedsiębiorstwa, które działają w sektorach krytycznych, takich jak infrastruktura cyfrowa, usługi pocztowe, gospodarowanie odpadami, a także usługi rejestracji nazw domen i dostawców usług DNS (Domain Name System). Podmioty te muszą wprowadzić właściwe środki techniczne, operacyjne i organizacyjne w odniesieniu do zarządzania ryzykiem cyfrowym. Zobowiązane są również do przeprowadzania audytów bezpieczeństwa oraz zgłaszania incydentów do właściwych organów nadzorczych. Dyrektywa NIS2 wprowadza wiele istotnych obowiązków i wymogów wobec przedsiębiorców objętych zakresem regulacji, w tabeli poniżej ujęto tylko obowiązki o charakterze prawnym i organizacyjnym (Tab. 1).

Tab. 1. Obowiązki przedsiębiorstw wynikające z dyrektywy NIS2

Zakres regulacji	Obowiązki wynikające z NIS2	Wpływ obowiązku na przedsiębiorców	Charakter obowiązku
Zakres podmiotowy	rozszerzenie katalogu podmiotów objętych dyrektywą – podmioty kluczowe i ważne w wielu sektorach gospodarki	zwiększenie liczby przedsiębiorstw podlegających nowym przepisom	prawny
System zarządzania bezpieczeństwem informacji	wdrożenia systemu zarządzania bezpieczeństwem informacji (polityka bezpieczeństwa, procedury oraz zarządzanie ryzykiem)	stworzenie systemu zarządzania bezpieczeństwem informacji opartego na standardach	organizacyjny
Zarządzanie ryzykiem	systematyczna identyfikacja, analiza i ocena ryzyka w zakresie bezpieczeństwa sieci i systemów informacyjnych	obowiązek implementacji procedur analizy i szacowania ryzyka, planów ciągłości działania i odtwarzania po incydentach	organizacyjny
Zgłoszenia incydentów cyberbezpieczeństwa	zgłaszanie poważnych incydentów właściwym organom w ciągu 24 h (wczesne ostrzeżenie), 72 h (zgłoszenie incy-	obowiązek tworzenia procedur reagowania na incydenty oraz systemów monitorowania bezpieczeństwa, obowiązek zgłaszania	prawny / organizacyjny

Zakres regulacji	Obowiązki wynikające z NIS2	Wpływ obowiązku na przedsiębiorców	Charakter obowiązku
	dentu), raport końcowy po incydencie (do miesiąca po incydencie)	istotnych cyberzagrożeń	
Bezpieczeństwo łańcucha dostaw	uwzględnianie ryzyka związanego z dostawcami usług ICT i partnerami biznesowymi	ocena bezpieczeństwa dostawców oraz zarządzanie ryzykiem w łańcuchu dostaw	organizacyjny
Szkolenia i świadomość pracowników	realizacja szkoleń z zakresu cyberbezpieczeństwa dla pracowników	zwiększanie świadomości zagrożeń	organizacyjny
Dokumentacja i audyty	wymóg sporządzania dokumentacji dotyczącej środków bezpieczeństwa oraz audytów i kontroli	Udostępnianie dokumentacji do kontroli organów nadzorczych	prawny / organizacyjny
Odpowiedzialność zarządu	odpowiedzialność kierownictwa organizacji za nadzór nad zarządzaniem cyberbezpieczeństwem	Zwiększenie zakresu odpowiedzialności zarządczej i ładu korporacyjnego	prawny
Nadzór regulacyjny	organizacje objęte przepisami podlegają kontroli właściwych organów krajowych	utrzymywanie zgodności regulacyjnej	prawny
Sankcje za naruszenie przepisów	wysokie kary finansowe	zwiększenie znaczenia zarządzania zgodnością i ryzykiem regulacyjnym	prawny

Źródła: opracowanie własne na podstawie R. Moczulski, *Obowiązki przedsiębiorcy w zakresie cyberbezpieczeństwa – dyrektywa NIS2*, https://ttms.com/pl/obowiazki-przedsiebiorcy-w-zakresie-cyberbezpieczenstwa-dyrektywa-nis2/ [dostęp: 21.04.2026].

Dyrektywa NIS 2 wprowadza istotną regulację w postaci odpowiedzialności kadry kierowniczej, osoby zajmujące stanowiska zarządcze ponoszą formalną odpowiedzialność za decyzje związane z zapewnieniem cyberbezpieczeństwa. Obejmuje to w szczególności zatwierdzanie polityk i strategii w tym obszarze, przypisanie odpowiednich zasobów finansowych na środki ochrony oraz nadzór nad wdrażaniem zaleceń wynikających z kontroli. Ponadto regulacja ta ustanawia obowiązek systematycznego podnoszenia kompetencji kierownictwa poprzez szkolenia, których celem jest rozwijanie świadomości zagrożeń oraz zdolności do skutecznego zarządzania

ryzykiem [Grzybowska-Ganszczyk i Głowacki, 2025, s. 86-87]. Nowe przepisy wprowadzają dotkliwe kary dla kierownictwa za brak zatwierdzania środków bezpieczeństwa, są to m.in. czasowe zakazy pełnienia funkcji kierowniczych oraz odpowiedzialność cywilna. Jednocześnie organy nadzorcze mogą prowadzić kontrole i audyty, wydawać wiążące zalecenia oraz nakładać środki naprawcze i sankcje przewidziane w nowej regulacji [Glapiak, 2026, ifirma.pl]. Dyrektywa NIS 2 ustanawia wobec organizacji obowiązki obejmujące systematyczną ocenę ryzyka, implementację adekwatnych środków zabezpieczających oraz ciągłe monitorowanie poziomu bezpieczeństwa. Podmioty objęte regulacją zobowiązane są do wykazania posiadania zarówno zasobów technologicznych, jak i zdolności organizacyjnych, które umożliwiają efektywną i terminową reakcję na zagrożenia oraz incydenty bezpieczeństwa. Wymusza to konieczność wdrożenia mechanizmów kontroli dostępu, stosowania technik kryptograficznych w ochronie danych, prowadzenia stałego nadzoru nad infrastrukturą sieciową oraz wykorzystania zaawansowanych systemów detekcji i przeciwdziałania atakom. W porównaniu z wcześniejszą regulacją, dyrektywa NIS2 charakteryzuje się bardziej precyzyjnymi wymogami, nakładając na organizacje obowiązek posiadania zintegrowanej polityki zarządzania ryzykiem oraz sformalizowanego planu reagowania na incydenty [Mączka, 2024, s. 114]. Nowa dyrektywa przede wszystkim obejmuje więcej sektorów gospodarki, wprowadza surowsze obowiązki zarządzania ryzykiem cyberbezpieczeństwa oraz większą odpowiedzialność kadry zarządzającej za nieprzestrzeganie obowiązków w zakresie zarządzania ryzykiem cyberbezpieczeństwa. W porównaniu do dyrektywy NIS oprócz takich sektorów jak, energetyka, transport, opieka zdrowotna, finanse, gospodarka wodna i infrastruktura cyfrowa, nowe przepisy dotyczą również dostawców publicznej komunikacji elektronicznej, cyfrowych usług, gospodarki odpadami i ściekami, produkcji wyrobów o znaczeniu krytycznym, usług pocztowych i kurierskich oraz administracji publicznej na szczeblu centralnym i regionalnym, a także sektora kosmicznego. Dyrektywa NIS 2 wprowadza zasadę samookreślania podmiotów, w zakresie obowiązków znajduje się przeprowadzenie stosownych analiz oraz oceny, czy zgodnie z kryteriami tej dyrektywy stanowią one podmiot kluczowy lub ważny. Zasada samookreślania przewiduje jednak wyjątki. „W pewnych przypadkach państwa członkowskie są zmuszone dokonać identyfikacji podmiotów kluczowych stanowiących mikro lub małe przedsiębiorstwa, wobec których zaistnienie zakłóceń w świadczonych przez nie usługach mogłoby wywrzeć poważny wpływ na bezpieczeństwo i porządek publiczny czy też zdrowie publiczne” [Chronowska-Sioła, 2025, s. 25]. Zasada samookreślenia została wprowadzona ze względu na dużą liczbę przedsiębiorstw objętych dyrektywą NIS 2 i brakiem możliwości zidentyfikowania wszystkich podmiotów przez organy państwowe. Odpowiedzialność za wstępną kwalifika-

cję przeniesiono na przedsiębiorstwa, które muszą same ocenić, czy podlegają dyrektywie i jakie obowiązki cyberbezpieczeństwa je dotyczą. Natomiast jeżeli podmiot powinien dokonać kwalifikacji, ale tego nie zrobi, będzie ponosić odpowiedzialność administracyjną. Przedsiębiorstwa stosujące się do regulacji NIS2 mają możliwość zbudować reputację organizacji niezawodnej i bezpiecznej, wyznaczając wyższe standardy w branży. Szkody wizerunkowe mogą mieć znaczący wpływ na postrzeganie firmy i jej konkurencyjność na rynku. Istotną konsekwencją nowych przepisów jest konieczność inwestowania w technologie, procesy, szkolenia i audyty. W celu zapewnienia wykonalności nowych przepisów wprowadzono wysokie kary finansowe mogące sięgać nawet kilku milionów euro lub określonego procentu rocznego obrotu, co ma wymusić realne działania, a nie deklaracje.

Podsumowanie

Dyrektywa NIS2 jest odpowiedzią na zwiększające się zagrożenia naruszania cyberbezpieczeństwa w UE. Nowe przepisy zwiększają wymogi bezpieczeństwa w odniesieniu do przedsiębiorstw, szczególnie w kluczowych sektorach gospodarki. Z uwagi na zróżnicowane uwarunkowania prawne i organizacyjne państw członkowskich oraz niejednorodny charakter poszczególnych sektorów, proces wdrażania dyrektywy NIS2 może wiązać się z odmiennymi wyzwaniami w poszczególnych krajach członkowskich. Sam proces wdrażania przepisów w całej UE nie jest jeszcze ukończony co oznacza dużą niepewność dla podmiotów podlegających tej regulacji. Najczęstsze problemy jakie można obecnie zidentyfikować to m.in. problemy z interpretacją przepisów czy niejasność pojęć np. „istotny incydent" czy „odpowiedni poziom bezpieczeństwa". Ponieważ przedsiębiorcy muszą sami ustalić, czy podlegają nowej regulacji w tym kontekście również mogą mieć problemy interpretacyjne [Zalewski, 2025]. Kluczowym wyzwaniem dla sektora prywatnego pozostaje niedobór wykwalifikowanych specjalistów w obszarze cyberbezpieczeństwa. Dane rynkowe wskazują na znaczący deficyt kadrowy, sięgający kilkunastu tysięcy ekspertów, co w praktyce ogranicza zdolność przedsiębiorstw do tworzenia wewnętrznych struktur odpowiedzialnych za wdrażanie rozwiązań zgodnych z wymogami dyrektywy NIS2 [ISC2 Cybersecurity Workforce Study, 2023]. Sytuację tę dodatkowo komplikuje niski poziom dojrzałości organizacyjnej. Przejawia się to m.in. brakiem sformalizowanych polityk, procedur reagowania na incydenty oraz systemów raportowania, które zgodnie z regulacjami powinny być nie tylko wdrożone, lecz także systematycznie weryfikowane i dokumentowane. Istotną barierą pozostaje również ograniczona świadomość zagrożeń wśród kadry zarządzającej. Przekonanie, że cy-

berataki dotyczą głównie dużych organizacji, prowadzi do marginalizowania inwestycji w obszar bezpieczeństwa. W konsekwencji takie podejście może generować istotne ryzyko i narazić organizację na sankcje finansowe. Z tego względu wdrażanie wymogów powinno być postrzegane nie jako reakcja na presję regulacyjną, lecz jako integralny element długoterminowej strategii zarządzania ryzykiem operacyjnym [Majka, 2025]. Z zakresu problemów natury organizacyjnej, zazwyczaj jest brak odpowiednich struktur zarządzania cyberbezpieczeństwem, brak aktywności zarządu w nadzorze nad cyberbezpieczeństwem, brak integracji z systemami zarządzania ryzykiem i compliance [Chodyka, 2025, s. 158]. W wielu przedsiębiorstwach bezpieczeństwo IT nadal traktowane jest jako problem techniczny, a nie strategiczny element zarządzania. Istotnym problemem jest również koszt wdrażania dyrektywy NIS 2, szacuje się, że może on wynosić on około 31,2 mld euro rocznie, co odpowiada ok. 0,31% obrotów sektorów objętych regulacją [Leyden, 2024]. Dla wielu przedsiębiorców oznacza to konieczność modernizacji infrastruktury IT, wdrożenia systemów monitorowania incydentów, prowadzenia audytów bezpieczeństwa, wdrożenia procedur raportowania. Szczególnie dla sektora MŚP może to stanowić istotne obciążenie finansowe. Jednakże ze względu na fakt, iż bezpośrednią odpowiedzialność za nieprzestrzeganie przepisów ponosi kierownictwo organizacji, inwestycje w infrastrukturę IT powinny odgrywać kluczową rolę. Dyrektywa NIS2 nakłada również obowiązek kontrolowania bezpieczeństwa dostawców i partnerów biznesowych. W praktyce powoduje to takie trudności jak brak narzędzi do oceny bezpieczeństwa dostawców, brak standardów audytowania podwykonawców, duża liczba podmiotów w łańcuchu dostaw IT.

NIS2 ma na celu usprawnienie współpracy i wymiany informacji między państwami członkowskimi UE poprzez utworzenie specjalnych zespołów ds. badań i reagowania na zagrożenia. Wpłynie również na rozwijanie wspólnej wiedzy i praktycznych umiejętności (poprzez wymianę doświadczeń) w odniesieniu do różnych rodzajów incydentów, umożliwiając skuteczną alokację wysiłków w celu zapobiegania atakom na dużą skalę. Wczesne wykrywanie zagrożeń, które jest podstawą ochrony systemów i ostatecznie wzmocni bezpieczeństwo [Shamatonova, 2025, s. 48].

Należy podkreślić, iż nowa regulacja objęła zakresem zupełnie nowe rodzaje przedsiębiorstw, o ile takie sektory jak bankowość, energetyka czy telekomunikacja ma doświadczenie w realizacji procedur bezpieczeństwa informacji, to dla części podmiotów gospodarczych są to zupełnie nowe obowiązki. Organy regulacyjne nie miały obowiązku kontrolowania tych podmiotów w poprzedniej regulacji dyrektywy NIS, co jest dla nich zupełnie nowym zadaniem i wyzwaniem. Dlatego też w niektórych sektorach nadal jest niska świadomość zagrożenia cyberatakami, w wielu

przedsiębiorstwach występują braki w zakresie szkoleń pracowników, brakuje kultury cyberbezpieczeństwa oraz obserwuje się lekceważenie zagrożeń takich jak phishing czy ransomware.

ORCID iD

Agnieszka Baran: https://orcid.org/0000-0003-2068-019X

Literatura

1. Chałubińska-Jentkiewicz K. (2019), *Cyberbezpieczeństwo – zagadnienia definicyjne*, Cybersecurity and Law 2.
2. Chodyka M. (2025), *Bezpieczeństwo cyfrowe małych i średnich przedsiębiorstw a dyrektywa NIS 2*, Prawo i Bezpieczeństwo – Law & Security 2(5).
3. Chronowska -Sioła E. (2025), *Unijna dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych*, Cybersecurity and Law 2(14).
4. 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, Document 32016L1148.
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).
6. Fleszer D. (2018), *Wokół problematyki bezpieczeństwa informacji*, Roczniki Administracji i Prawa 18(1).
7. Glapiak A. (2026), *Dyrektywa NIS2 – jakie obowiązki wprowadza dla przedsiębiorców*, ifirma.pl, https://www.ifirma.pl/blog/dyrektywa-nis-2-jakie-obowiazki-wprowadza-dla-przedsiebiorcow/#za-co-groza-kary-i-sankcje-w-dyrektywie-nis2 [28.04.2026].
8. Górka-Chowaniec A., Popek A. (2024), *Attempt to use the deming cycle (PDCA) in the process of implementing an information security management system*, International Journal for Quality Research 19(2).
9. Grzybowska-Ganszczyk D. B., Głowacki B. (2025), *NIS 2 Directive as a tool for strengthening local and national security in the area of cyber threats*, dot.pl (I), s. 86-87.
10. ICT security in enterprises (2026), Statistics Explained, https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf [18.03.2026].

11. International Organization for Standardization, (2018), ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO, Geneva.
12. ISC2 Cybersecurity Workforce Study (2023) https://cybergovernancealliance.org/wp-content/uploads/2024/01/ISC2_Cybersecurity_Workforce_Study_2023-1.pdf, [21.04.2026].
13. Jarmoszko S. (2016), *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa*, w: Kubiak M. J., Białoskórski R. (red.), *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.
14. Leyden J. (2024), *EU's NIS2 Directive for cybersecurity resilience enters full enforcement*, CSO, https://www.csoonline.com/article/3568787/eus-nis2-directive-for-cybersecurity-resilience-enters-full-enforcement.html?utm_ [6.03.2026].
15. Liedel K. (2006), *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń, s. 19., cyt. za K. Pietras E. (2016), *Zagadnienia zarządzania bezpieczeństwem informacji w organizacji*, Zarządzanie Przedsiębiorstwem .
16. Łuczak J. (2004), *Zarządzanie bezpieczeństwem informacji*, w: Łańcucki J. (red.), *Znormalizowane systemy zarządzania*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.
17. Majka M. (2025), *NIS2 w praktyce: jak zmienia się krajobraz cyberbezpieczeństwa w Polsce*, Solutio Care, https://www.researchgate.net/publication/396913171_NIS2_w_praktyce_jak_zmienia_sie_krajobraz_cyberbezpieczenstwa_w_Polsce, [16.04.2026].
18. Marynowicz B. (2025), *Bezpieczeństwo informacji w perspektywie zarządzania strategicznego*, Management and Quality 7(1).
19. Mączka K. (2024), *Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji*, Civil and Cultural Heritage Protection 5.
20. Meriah I., Ben Arfa Rabai L. (2019), *Comparative Study of Ontologies Based ISO 27000 Series Security Standards*, Procedia Computer Science 160.
21. Metin B., Sevim S. B., Wynn M. (2025), *Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards*, Standards 5(4).
22. Moczulski R., *Obowiązki przedsiębiorcy w zakresie cyberbezpieczeństwa – dyrektywa NIS2*, https://ttms.com/pl/obowiazki-przedsiebiorcy-w-zakresie-cyberbezpieczenstwa-dyrektywa-nis2/ [21.04.2026].
23. Ożarek G. (2013), *System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie*, w: *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny, Warszawa.

24. Pietras E. (2016), *Zagadnienia zarządzania bezpieczeństwem informacji w organizacji*, Zarządzanie Przedsiębiorstwem 1.
25. Rychły-Lipińska A., Kamiński W. (2024), *Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001:2017*, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie 53.
26. Shamatonova D. (2025), *The importance of the NIS2 Directive and the potential challenges it entails*, Journal of Advance Research in Social Science and Humanities 11(1).
27. Szmit M. (2025), *Wybrane zagadnienia zarządzania cyfrową gotowością śledczą*, w: Baranowska M. (red.), *Systemy Zarządzania Bezpieczeństwem Informacji*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź.
28. Tamimi M., Alzahrani A., Aljohani R., Alshahrani M., Alharbi B. (2019), *Security Review based on ISO 27000/ ISO 27001/ ISO 27002 Standards: A Case Study Research*, International Journal of Management and Applied Science 5(8).
29. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r., poz. 20, 252).
30. Vandezande N. (2024), *Cybersecurity in the EU: How the NIS2 Directive stacks up against the NIS Directive*, Computer Law & Security Review 52.
31. Wiśniewski P. Sz. (2018), *Systemy zarządzania bezpieczeństwem informacji w przedsiębiorstwie*, Acta Universitatis Nicolai Copernici, Zarządzanie 45(2).
32. Zalewski T. (2025), *Włoska lekcja cyberbezpieczeństwa*, Rzeczpospolita, 03.12.2025, https://www.rp.pl/opinie-prawne/art43438621-tomasz-zalewski-wloska-lekcja-cyberbezpieczenstwa [06.03.2026].

Information Security Management in the Light of the NIS2 Directive – Obligations, Legal and Organizational Challenges for Enterprises

Abstract

The issue of information security management is becoming increasingly critical in the face of a global rise in cyberattacks. Data from various reports indicates a growing frequency of attacks on information resources, targeting not only public institutions but also small and medium-sized enterprises (SMEs). As part of its work on new regulations in this area, the European Union is striving to harmonize approaches to information security. The aim of this article is to review the changes introduced by the NIS2 directive, assess the legal and organizational consequences for enterprises and identify challenges in the field of information

security management. The obligations arising from the new legislation pose a challenge for businesses both legally and organizationally. The most familiar challenges currently include difficulties in interpreting the regulations and new concepts contained in the directive, a lack of cybersecurity experts, and limited awareness of threats among management. Awareness of cyberattacks remains low, leading to the marginalization of security investments and an insufficient number of employee training programs.

Key words

NIS2 Directive, European Union, Information Security Management System