

**Piotr Ładny Cyberbezpieczeństwo i cyberodporność
we współczesnym świecie
– Polska na tle Unii Europejskiej**

Cyberbezpieczeństwo i cyberodporność we współczesnym świecie
– Polska na tle Unii Europejskiej

Piotr Ładny

Cyberbezpieczeństwo i cyberodporność we współczesnym świecie – Polska na tle Unii Europejskiej

Rada Wydawnicza

Anna Cedro, Urszula Chęcińska, Katarzyna Jaworska-Biskup, Rafał Klóska,
Maciej Kowalewski, Ewa Mazur-Wierzbicka, Jarosław Nadobnik,
Grzegorz Wejman, Renata Ziemińska, Magdalena Zioło,
Andrzej Skrendo – przewodniczący Rady Wydawniczej,
Elżbieta Zarzycka – dyrektor Wydawnictwa Naukowego

Recenzent

dr hab. Łukasz Zakonnik

Redakcja i korekta językowa

Bernadeta Lekacz

Skład

Joanna Dubois-Mosora

Projekt okładki

Joanna Dubois-Mosora

Piotr Ładny ORCID 0000-0002-5744-0571



Ministerstwo Nauki
i Szkolnictwa Wyższego

Dofinansowano ze środków Ministra Nauki w ramach Programu
„Regionalna inicjatywa doskonałości”



Wersja elektroniczna publikacji dostępna na licencji CC BY-SA 4.0
po 12 miesiącach od daty wprowadzenia do obrotu

© Copyright by Uniwersytet Szczeciński, Szczecin 2025

DOI 10.18276/978-83-8419-046-3

ISBN 978-83-8419-046-3 (online)

ISBN 978-83-8419-045-6 (print)

ISSN 0860-2751

WYDAWNICTWO NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

Wydanie I | Ark. wyd. 12,0 | Ark. druk. 11,2 | Format 170/240

Spis treści

Wstęp	7
Rozdział 1	
Cyberbezpieczeństwo i cyberodporność – istota i zakres pojęciowy	9
1.1. Definicje i kluczowe pojęcia.....	9
1.2. Rodzaje i klasyfikacja zagrożeń.....	16
1.3. Cyberzagrożenia a ryzyko, incydenty i ataki	21
1.4. Cyberodporność	29
Rozdział 2	
Ramy regulacyjne i strategie cyberbezpieczeństwa – Polska na tle Unii Europejskiej	33
2.1. Regulacje na poziomie Unii Europejskiej	35
2.2. Regulacje w Polsce.....	49
2.3. Inne dokumenty kształtujące formalne ramy w zakresie cyberbezpieczeństwa	56
Rozdział 3	
Charakterystyka, ewolucja i metody ograniczania cyberzagrożeń	65
3.1. Charakterystyka najczęstszych zagrożeń i ataków w polskiej i europejskiej cyberprzestrzeni	67
3.2. Ewolucja zagrożeń spowodowana zmianami technologicznymi	90
3.3. Techniki i narzędzia ograniczania cyberzagrożeń	98
Rozdział 4	
Kompetencje i edukacja cyfrowa jako kluczowe elementy systemu cyberbezpieczeństwa w Polsce	107
4.1. Świadomość i kompetencje Polaków w zakresie cyberbezpieczeństwa – wyniki badań empirycznych	109
4.2. Znaczenie świadomości i edukacji dla budowy systemu cyberbezpieczeństwa w Polsce ...	121
4.3. Rekomendacje na rzecz rozwoju kompetencji cyberbezpieczeństwa w Polsce	137
Podsumowanie	153
Spis rysunków i tabel	157
Bibliografia	159
Załącznik 1. Formularz ankiety	173
Streszczenie	179
Abstract	180

Wstęp

Postępująca cyfryzacja, która przenika niemal wszystkie sfery życia społecznego i gospodarczego, niesie ze sobą zarówno znaczące korzyści, jak i nowe wyzwania. Dynamiczny rozwój technologii cyfrowych, takich jak sztuczna inteligencja, Internet Rzeczy czy technologie chmurowe i kwantowe, przyczynia się do wzrostu efektywności procesów, zwiększenia innowacyjności, podnoszenia jakości życia oraz poprawy dostępności usług publicznych. Jednocześnie rozwój ten generuje liczne zagrożenia związane z bezpieczeństwem informacji i integralnością systemów teleinformatycznych, co wymaga podejmowania skutecznych działań w zakresie podnoszenia poziomu cyfrowych zabezpieczeń oraz edukacji użytkowników. Konieczność zapewnienia efektywnej ochrony cyberprzestrzeni oraz podniesienia poziomu odporności na incydenty cybernetyczne staje się jednym z kluczowych wyzwań dla współczesnych społeczeństw i państw, wymagającym interdyscyplinarnego podejścia oraz współpracy podmiotów z różnych sektorów.

Głównym celem niniejszej monografii jest przeprowadzenie wieloaspektowej analizy zagadnień związanych z cyberbezpieczeństwem i cyberodpornością, ze szczególnym uwzględnieniem sytuacji Polski na tle innych państw Unii Europejskiej. Obok celu głównego sformułowano również takie cele szczegółowe, jak:

- a) identyfikacja kluczowych zagrożeń, które wpływają na funkcjonowanie państw, instytucji i obywateli w cyberprzestrzeni oraz technik i narzędzi umożliwiających podnoszenie poziomu cyberbezpieczeństwa;
- b) analiza ram prawnych, strategii krajowych i unijnych oraz działań instytucji publicznych w obszarze cyberbezpieczeństwa;
- c) ocena poziomu świadomości społecznej oraz kompetencji Polaków w zakresie cyberbezpieczeństwa i znaczenia tych czynników dla budowy systemu bezpieczeństwa cyfrowego w Polsce;
- d) opracowanie rekomendacji na rzecz podniesienia poziomu kompetencji cyfrowych i kompetencji cyberbezpieczeństwa w Polsce.

Opracowanie składa się z czterech rozdziałów. W rozdziale pierwszym przedstawiono definicje, podstawowe pojęcia oraz klasyfikacje cyberzagrożeń, a także omówiono różnicę pomiędzy cyberbezpieczeństwem i cyberodpornością.

Rozdział drugi koncentruje się na analizie regulacji prawnych oraz polityk strategicznych związanych z cyberbezpieczeństwem, obowiązujących na poziomie Unii

Europejskiej oraz w Polsce. W tej części monografii zaprezentowano przegląd najważniejszych dokumentów kształtujących formalne ramy w zakresie cyberbezpieczeństwa i wskazano powiązania, jakie występują między regulacjami kształtującymi bezpieczeństwo środowiska cyfrowego w Europie i w Polsce.

W rozdziale trzecim przedstawiono charakterystykę najczęstszych zagrożeń oraz ich ewolucję wynikającą ze zmian technologicznych. Omówiono również najczęściej stosowane techniki i narzędzia, które służą ograniczaniu tych zagrożeń.

Rozdział czwarty poświęcono analizie poziomu świadomości i kompetencji cyfrowych Polaków. W tej części opracowania przedstawiono wyniki autorskich badań empirycznych, które dotyczyły poziomu wiedzy i umiejętności Polaków w zakresie cyberbezpieczeństwa. Badanie zostało przeprowadzone metodą ankietową z wykorzystaniem kwestionariusza internetowego (CAWI) na ogólnopolskiej próbie 1108 Polaków w wieku 18–65 lat, o zróżnicowanych profilach demograficznych i zawodowych. Dotyczyło ono trzech kluczowych obszarów cyberbezpieczeństwa: poziomu świadomości, poziomu i źródeł wiedzy oraz umiejętności praktycznych respondentów. Zastosowane w badaniu metoda ilościowa i dobór próby umożliwiły uogólnienie wyników na całą populację dorosłych z błędem szacunku na poziomie $\pm 3\%$ (poziom ufności 95%). Wnioski z rozważań teoretycznych i badań empirycznych w powiązaniu z diagnozą w zakresie podejmowanych działań edukacyjnych i ich wpływu na ogólny poziom kompetencji cyfrowych i kompetencji związanych z cyberbezpieczeństwem pozwoliły na identyfikację obszarów wymagających intensyfikacji działań oraz przedstawienie szeregu rekomendacji mających na celu wzmocnienie kompetencji społeczeństwa i zwiększenie liczby specjalistów w dziedzinie cyberbezpieczeństwa w Polsce.

Obok metod ilościowych związanych z badaniem ankietowym autor wykorzystał badania wtórne, oparte na analizie literatury, dostępnych wyników badań oraz regulacji prawnych dotyczących cyberbezpieczeństwa.

Monografia ma charakter przede wszystkim naukowy, jednak zawarte w niej wyniki badań, analizy oraz rekomendacje mogą pozwolić na lepsze zrozumienie znaczenia cyberbezpieczeństwa i cyberodporności we współczesnym świecie, a tym samym stanowią wartościowe źródło wiedzy dla osób zajmujących się lub zainteresowanych tą problematyką.

Cyberbezpieczeństwo i cyberodporność – istota i zakres pojęciowy

1.1. Definicje i kluczowe pojęcia

Ludzkość od zawsze mierzyła się z wyzwaniami, jakie wiązały się z koniecznością pogodzenia korzyści związanych z postępem technologicznym oraz ryzykiem i wyzwaniami, jakie towarzyszą wszystkim innowacjom technologicznym. Ten dylemat staje się szczególnie widoczny w obszarze technologii cyfrowych i rozwoju transformacji cyfrowej, która w założeniu powinna się przyczynić do tworzenia innowacyjnych rozwiązań, poprawy komunikacji procesów, a w konsekwencji wzrostu wydajności i efektywności pracy¹. Transformacja cyfrowa oznacza jednak również, że coraz więcej danych przechowywanych jest w postaci cyfrowej, a rosnące uzależnienie biznesu i społeczeństwa od rozwiązań online sprawia, że nawet drobne luki w zabezpieczeniach mogą generować zupełnie nowe ryzyko i zagrożenia. Jednocześnie z rozwojem procesów gromadzenia i wymiany danych zwiększa się nasze uzależnienie od mediów cyfrowych, co sprawia, że monitorowanie i wywieranie wpływu na ludzi poprzez kształtowanie opinii i światopoglądów staje się coraz łatwiejsze². Wraz z rozwojem nowych zagrożeń pojawiła się konieczność zapewnienia cyberbezpieczeństwa, czyli ochrony przestrzeni cyfrowej oraz znajdujących się tam informacji i zasobów przed kradzieżą, zniszczeniem lub manipulacją.

Początków rozwoju pojęcia „cyberbezpieczeństwo” można doszukiwać się już w latach 40. XX wieku, czyli w czasach, kiedy powstały pierwsze komputery, a w ich pamięci zaczęto przechowywać informacje i tajemnice, które należało chronić przed kradzieżą lub podsłuchaniem. Ponieważ pierwsze komputery były ogromnymi urządzeniami zajmującymi całe pomieszczenia i nie istniały jeszcze sieci komputerowe, ochrona komputerów i przechowywanych tajemnic skupiała się początkowo na fizycznej ochronie

¹ G. Vial, *Understanding Digital Transformation: A Review and a Research Agenda*, „The Journal of Strategic Information Systems” 2019, no. 28(2), s. 118–144.

² R. Clarke, *Big Data, Big Risks*, „Information Systems Journal” 2016, no. 26(1), s. 77–90.

systemów komputerowych przed nieautoryzowanym dostępem. Celem było zapewnienie, że do przechowywanych danych nie uzyskają dostępu osoby niepowołane³.

Rozwój technologii przesyłania danych między komputerami, zapoczątkowany przez sieć ARPANET w latach 60. XX wieku, zwiększył znaczenie zagadnień dotyczących bezpieczeństwa cybernetycznego. ARPANET – eksperymentalna sieć komputerowa uznawana za poprzednika Internetu – umożliwiła przesyłanie danych między odległymi komputerami, ale również zainicjowała problemy związane z bezpieczeństwem sieciowym. Wraz z rosnącą liczbą podłączonych urządzeń pojawiły się pierwsze incydenty, takie jak przełamanie zabezpieczeń systemów komputerowych⁴ oraz powstanie pierwszych wirusów komputerowych⁵, np. wirusa Creeper na początku lat 70.⁶ W tym samym czasie firma IBM opracowała standard szyfrowania danych DES (ang. *Data Encryption Standard*) w celu bezpiecznej wymiany informacji w systemach komputerowych⁷.

W latach 80. rosnąca popularność komputerów osobistych stworzyła zupełnie nowy obszar dla zagrożeń cybernetycznych. W reakcji na wzrost liczby wirusów powstały pierwsze programy antywirusowe, a po incydencie związanym z zainfekowaniem ponad 6 tysięcy komputerów robakiem Morrisa (jednym z pierwszych robaków, które szeroko rozprzestrzeniły się w Internecie) na Uniwersytecie Carnegie Mellon w Pittsburghu utworzono pierwszy zespół reagowania na incydenty komputerowe (CERT – Computer Emergency Response Team)⁸.

Przełomowym momentem dla zagadnień związanych z bezpieczeństwem cyfrowym był rozwój Internetu w latach 90. i na początku XXI wieku, który zrewolucjonizował komunikację, ale też przyczynił się do rozwoju zagrożeń, takich jak złośliwe oprogramowanie, ataki na sieci korporacyjne, włamania do systemów rządowych. Rosnąca liczba incydentów związanych z nowymi technologiami sieciowymi doprowadziła do wzrostu społecznej świadomości w zakresie cyberbezpieczeństwa, co w konsekwencji

3 *History of Cybersecurity: An Overview*, <https://keepnetlabs.com/blog/cybersecurity-breaches-lessons-from-history> (17.11.2024).

4 W 1962 r. w reakcji na wprowadzenie haseł dostępu do komputerów MIT, które miały ograniczyć czas pracy na komputerach, jeden ze studentów opracował metodę wydobycia z komputera wszystkich haseł zapisanych w systemie i wykorzystał je, aby obejść ustalone limity i uzyskać więcej czasu przy komputerze. <https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches> (29.10.2024).

5 Wirus komputerowy (ang. *malware*) to szkodliwy program, który bez wiedzy użytkownika infekuje pliki lub obszary systemowe komputera, potrafi się samoistnie powielać i przenosić na inne urządzenia. Więcej na temat złośliwego oprogramowania i jego różnych odmian zob. w przewodniku NASK *O złośliwym oprogramowaniu*, <https://firmabezpiecznacyfrowo.pl/poradnik/cyberbezpieczenstwo-w-organizacji/malware/> (2.07.2025).

6 *Kiedy stworzono pierwszego wirusa komputerowego?*, <https://www.politykabezpieczenstwa.pl/pl/a/pierwszy-wirus-internetowy-na-swiecie> (2.07.2025).

7 *Wprowadzenie do bezpieczeństwa IT*, t. 1, red. M. Sajdak, Kraków 2023, s. 480–481.

8 *The Oxford Handbook of Cyber Security*, red. P. Cornish, Oxford 2021, s. 314–327.

przyspieszyło rozwój nowych technik i narzędzi zabezpieczających oraz zapoczątkowało rozwój branży bezpieczeństwa komputerowego⁹.

Chcąc scharakteryzować cyberbezpieczeństwo, należy podkreślić, że jest to zagadnienie wielowymiarowe, które ewoluowało wraz z rozwojem technologii informacyjno-komunikacyjnych i postępującą cyfryzacją społeczeństwa. Z uwagi na jego interdyscyplinarny charakter definicje cyberbezpieczeństwa różnią się w zależności od kontekstu, w którym są stosowane, oraz od specyfiki problematyki, jaką obejmują. W literaturze przedmiotu coraz częściej wskazuje się, że cyberbezpieczeństwo jest fundamentem funkcjonowania współczesnych społeczeństw, szczególnie w kontekście rozwoju globalnej gospodarki cyfrowej¹⁰, a samo pojęcie odnosi się do ochrony systemów informatycznych, sieci, danych oraz użytkowników przed nieuprawnionym dostępem, zakłóceniami, manipulacją czy zniszczeniem.

W licznych opracowaniach naukowych i popularnonaukowych termin ten opisuje się w różnym kontekście, podkreślając np. znaczenie rozwiązań technologicznych lub odnosząc się do zagadnień prawnych, organizacyjnych, ekonomicznych, społecznych, politycznych i innych, które są nierozdzielnie związane z tworzeniem systemów bezpieczeństwa informatycznego¹¹.

Część definicji charakteryzuje cyberbezpieczeństwo jako działania zmierzające do ochrony infrastruktury teleinformatycznej, wskazując, że pojęcie to obejmuje „ochronę sieci komputerowych i zawartych w nich informacji przed penetracją i złośliwym uszkodzeniem lub zakłóceniem”¹² lub „możliwość ochrony lub obrony zasobów cyberprzestrzeni przed cyberatakami”¹³ czy też „ochronę systemów komputerowych przed nieautoryzowanym dostępem lub uszkodzeniem”¹⁴. Amerykański Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST) definiuje cyberbezpieczeństwo jako „proces ochrony informacji poprzez zapobieganie atakom, ich wykrywanie i reagowanie na nie”¹⁵. Powyższe definicje podkreślają techniczny

⁹ J. Antczak, M. Kos, *Cybersecurity of ICT systems in the era of widespread digitization*, „Nowoczesne Systemy Zarządzania” 2022, nr 17(3), s. 81–98.

¹⁰ R. von Solms, J. Van Niekerk, *From information security to cyber security*, „Computers & Security” 2013, no. 38, s. 97–102.

¹¹ D. Craigen, N. Diakun-Thibault, R. Purse, *Defining Cybersecurity*, „Technology Innovation Management Review” 2014, no. 4(10), s. 13–16.

¹² J.A. Lewis, *Cybersecurity and Critical Infrastructure Protection*, Washington, D.C. 2006, <http://csis.org/publication/cybersecurity-and-criticalinfrastructure-protection> (22.11.2024).

¹³ National Information Assurance Glossary, Committee on National Security Systems (CNSS) Instruction No. 4009, 2010, https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf (3.12.2024).

¹⁴ R. von Solms, *Information security management (3): the Code of Practice for Information Security Management (BS 7799)*, „Information Management & Computer Security” 1998, vol. 6, no. 5, s. 224–225.

¹⁵ National Institute of Standards and Technology, *Framework for improving critical infrastructure cybersecurity: Version 1.0*, 2014, <https://www.nist.gov/document/cybersecurity-framework-021214pdf> (12.12.2024).

wymiar ochrony, koncentrując się głównie na ochronie systemów komputerowych i sieci przed nieautoryzowanym dostępem, wirusami oraz podstawowymi formami zagrożeń technicznych, traktując je w kategoriach czysto technologicznych. Współczesne definicje są znacznie szersze i obejmują aspekty organizacyjne, prawne, społeczne i psychologiczne, uwzględniając ochronę danych osobowych, integralność systemów krytycznych, zarządzanie ryzykiem oraz wpływ cyberzagrożeń na gospodarkę i społeczeństwo.

Agencja Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (Cybersecurity and Infrastructure Security Agency – CISA) w ramach inicjatywy, której celem jest wspieranie edukacji, rozwoju kariery i standaryzacji terminologii w dziedzinie cyberbezpieczeństwa (National Initiative for Cybersecurity Careers and Studies – NICCS), zdefiniowała cyberbezpieczeństwo jako „strategię, politykę i normy dotyczące zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej – elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej”¹⁶. Natomiast Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU) w Rekomendacji ITU-T X. 1205 definiuje cyberbezpieczeństwo jako „zbiór narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk, zapewnień i technologii, które mogą być wykorzystywane do ochrony środowiska cybernetycznego oraz organizację i zasoby użytkownika. Organizacja i zasoby użytkownika obejmują podłączone urządzenia komputerowe, personel, infrastrukturę, aplikacje, usługi, systemy telekomunikacyjne oraz całość przekazanych i/lub przechowywanych informacji w środowisku cybernetycznym. Cyberbezpieczeństwo dąży do zapewnienia osiągnięcia i utrzymania właściwości bezpieczeństwa organizacji i zasobów użytkownika względem odpowiednich zagrożeń bezpieczeństwa w środowisku cybernetycznym. Ogólne cele bezpieczeństwa obejmują dostępność, integralność oraz poufność”¹⁷.

Definicje cyberbezpieczeństwa można znaleźć również w oficjalnych dokumentach i aktach prawnych Unii Europejskiej. Rozporządzenie Parlamentu Europejskiego i Rady UE 2019/881 wskazuje, że termin ten oznacza „działania niezbędne do ochrony sieci

¹⁶ Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej” 2016, t. 3, nr 2(10), s. 103–128.

¹⁷ Recommendation X.1205 – Overview of cybersecurity, <https://www.itu.int/rec/t-rec-x.1205-200804-i> (9.12.2024).

i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”¹⁸.

Warto zauważyć, że w oficjalnych dokumentach Unii Europejskiej obok pojęcia „cyberbezpieczeństwo” przywoływany jest również termin „bezpieczeństwo sieci i systemów informatycznych”, które oznacza „odporność” sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych albo związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne¹⁹. Pojęcie to można uznać za element składowy będący częścią nadrzędnej koncepcji cyberbezpieczeństwa, który zamiast na bezpieczeństwie całej cyberprzestrzeni, koncentruje się na infrastrukturze sieciowej oraz na konkretnych systemach i aplikacjach. Podobną w swojej istocie definicję można znaleźć też w polskiej ustawie o krajowym systemie cyberbezpieczeństwa, zgodnie z którą cyberbezpieczeństwo oznacza „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”²⁰.

Przedstawiony przegląd definicji wskazuje, że cyberbezpieczeństwo to wieloaspektowa dziedzina obejmująca różne zagadnienia związane z ochroną systemów informatycznych, danych oraz infrastruktury przed zagrożeniami wynikającymi z działalności cyberprzestępców²¹, błędów ludzkich czy awarii technicznych. Chociaż same definicje cyberbezpieczeństwa różnią się w zależności od perspektywy, z której są formułowane, to jednak istnieje szereg wspólnych elementów, które pozwalają na wskazanie podstawowych cech i celów tej dziedziny.

Podobieństwa pomiędzy różnymi definicjami cyberbezpieczeństwa można dostrzec w nawiązaniu do tzw. triady CIA, czyli koncepcji w dziedzinie bezpieczeństwa informacji, która obejmuje trzy kluczowe elementy (filary) bezpieczeństwa komputerowego:

¹⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, 151 OJ L (2019). <http://data.europa.eu/eli/reg/2019/881/oj/pol>.

¹⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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, OJ L (2022). <http://data.europa.eu/eli/dir/2022/2555/oj/pol>.

²⁰ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2022, poz. 1863 ze zm.).

²¹ Zamiast określeń „cyberprzestępcy” czy „hakerzy” wielu autorów stosuje pojęcie „adwersarze” oznaczające osobę, grupę, organizację lub rząd, które prowadzą lub mają zamiar prowadzić szkodliwą działalność.

Poufność (ang. *confidentiality*) – oznacza ochronę danych przed nieuprawnionym dostępem. Tylko uprawnione osoby mogą uzyskać dostęp do określonych informacji, a wszelkie inne próby dostępu powinny być zablokowane²².

Integralność (ang. *integrity*) – oznacza, że dane powinny być chronione przed nieautoryzowanymi zmianami. W kontekście ochrony danych odnosi się ona do zapewnienia, że informacje pozostają niezmienione, a każda próba ich modyfikacji bez odpowiednich uprawnień zostanie wykryta. Integralność może też być rozumiana jako funkcjonowanie systemu w sposób niezakłócony i niezmanipulowany.

Dostępność (ang. *availability*) – oznacza, że dane muszą być dostępne dla uprawnionych użytkowników zawsze wtedy, kiedy są potrzebne. Nawet jeśli dane są bezpieczne i nienaruszone, brak dostępu do nich w kluczowych momentach może spowodować ogromne problemy dla właściciela lub użytkownika²³.

W kontekście rozwoju problematyki bezpieczeństwa wskazuje się często na dodatkowe własności, o jakie triada CIA powinna być uzupełniona. Są to²⁴:

Autentyczność (ang. *authenticity*) – oznacza zapewnienie, że tożsamość podmiotu lub osoby, która wykonuje określone operacje, jest zgodna z deklarowaną.

Rozliczalność (ang. *accountability*) – polega na możliwości ustalenia użytkowników, którzy w określonym czasie dokonywali określonych operacji na poszczególnych danych, czyli kto dokonał np. modyfikacji lub usunięcia zapisanych w systemach informatycznych danych. Ze względu na konieczność spełnienia wymagań prawnych dotyczących bezpieczeństwa rozliczalność może oznaczać, że organizacja dokumentuje i jest w stanie wykazać, w jaki sposób nałożone na nią obowiązki w zakresie cyberbezpieczeństwa spełnia.

Niezaprzeczalność (ang. *non-repudiation*) – oznacza brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów biorących udział w tej wymianie.

Niezawodność (ang. *reliability*) – to właściwość bezpieczeństwa informacji określająca czas bezawaryjnego działania systemów informatycznych procentowo.

Kompleksowe podejście do cyberbezpieczeństwa bazujące na rozbudowanej wersji filarów bezpieczeństwa komputerowego stosuje m.in. ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – kluczowa instytucja Unii Europejskiej zajmująca

²² Z poufnością bywa niekiedy utożsamiane pojęcie „prywatność”, jednak oba terminy mają odmienne znaczenie i pełnią różne funkcje w systemach ochrony informacji. Poufność dotyczy technicznych i organizacyjnych środków ochrony informacji, natomiast prywatność związana jest z zapewnieniem osobom prywatnym kontroli lub wpływu na to, jakie informacje na ich temat mogą być gromadzone i przechowywane, kto może je gromadzić oraz komu mogą być przekazywane. Prywatność ma więc wymiar prawny i etyczny, a nie tylko techniczny i organizacyjny.

²³ W. Stallings, L. Brown, *Computer security: Principles and practice*, Pearson 2018, s. 25–26.

²⁴ D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce: wybrane zagadnienia*, European Association for Security 2016, s. 32–33.

się bezpieczeństwem cybernetycznym w Europie. Natomiast w Polsce wszystkie sześć z przedstawionych filarów bezpieczeństwa informacji (poza dostępnością) zostało uwzględnionych w rozporządzeniu 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, które określa podstawowe wymagania i zalecenia dla nowych oraz istniejących publicznych systemów teleinformatycznych i rejestrów publicznych.

Z uwagi na multidyscyplinarność problematyki cyberbezpieczeństwa, która dotyczy technologii informacyjnych, prawa, zarządzania, socjologii i psychologii, oraz na zmiany, jakie w terminologii wywołuje postęp technologiczny, pojawianie się nowych zagrożeń oraz regulacje tego obszaru, w literaturze brak jest jednej, uniwersalnej definicji obejmującej wszystkie konteksty, w jakich termin ten jest stosowany. Pojęcie „cyberbezpieczeństwo” stale ewoluuje w odpowiedzi na zmieniający się krajobraz technologiczny i społeczny.

Nowe technologie, takie jak sztuczna inteligencja, *blockchain*²⁵ czy Internet Rzeczy, istotnie wpływają na rozszerzenie zakresu cyberbezpieczeństwa. Sztuczna inteligencja i uczenie maszynowe mogą pełnić podwójną rolę w obszarze cyberbezpieczeństwa. Z jednej strony stanowią skuteczne narzędzia ochrony np. w zakresie detekcji anomalii i wykrywania zagrożeń, z drugiej jednak strony mogą generować zupełnie nowe, trudne do przewidzenia zagrożenia²⁶. Z kolei Internet Rzeczy (*Internet of Things* – IoT) – koncepcja odnosząca się do sieci połączonych urządzeń i obiektów fizycznych, które mogą komunikować się ze sobą i wymieniać dane za pośrednictwem Internetu bez konieczności bezpośredniej ingerencji człowieka – zwiększa ryzyko związane ze stale rosnącą liczbą podłączonych urządzeń, co wymaga nowego podejścia do ich ochrony²⁷.

Definicja cyberbezpieczeństwa pozostaje dynamiczna i kontekstualna. Istotne jest uwzględnienie różnorodnych perspektyw, aby skutecznie adresować współczesne wyzwania w cyberprzestrzeni. Multidyscyplinarny charakter tego pojęcia podkreśla potrzebę współpracy pomiędzy ekspertami z różnych dziedzin, aby tworzyć zrównoważone i skuteczne strategie ochrony. Cyberbezpieczeństwo ewoluowało także w kontekście geopolitycznym. Pojawienie się cyberwojny i ataków sponsorowanych przez państwa,

²⁵ *Blockchain* to specjalny rodzaj cyfrowego rejestru, w którym informacje (np. o transakcjach) zapisywane są w kolejnych „blokach” połączonych ze sobą w łańcuch. Każdy blok zawiera dane oraz tzw. odcisk palca (*hash*) poprzedniego bloku, co sprawia, że całość jest odporna na nieautoryzowane zmiany oraz publicznie weryfikowalna. Technologia *blockchain* jest wykorzystywana m.in. do obsługi kryptowalut, cyfrowych tożsamości, zawierania cyfrowych umów czy śledzenia pochodzenia produktów.

²⁶ M. Aldhamer, *The Impact of Artificial Intelligence on the Future of Cybersecurity*, „Multi-Knowledge Electronic Comprehensive Journal for Education & Science Publications” 2024, no. 71.

²⁷ T.S. AlSalem, M.A. Almaiah, A. Lutfi, *Cybersecurity Risk Analysis in the IoT: A Systematic Review*, „Electronics” 2023, no. 12(18), 3958.

takich jak operacje Rosji przeciwko Ukrainie²⁸, ataki na instytucje publiczne czy ingerencje w procesy wyborcze²⁹, wymusiły nowe podejście do definiowania bezpieczeństwa w cyberprzestrzeni. Zmienia się również charakter samych zagrożeń, które stają się bardziej złożone i wielowektorowe, łączą różne metody i techniki ataku w celu zwiększenia skuteczności i trudności wykrycia. Wprowadzenie międzynarodowych standardów i regulacji (RODO i NIS2) miało na celu ujednolicenie podejścia do zarządzania bezpieczeństwem w cyberprzestrzeni. Regulacje te nie tylko uwzględniają techniczne aspekty ochrony, ale także wymagają budowania kultury bezpieczeństwa oraz wprowadzania mechanizmów raportowania incydentów. Współczesne definicje cyberbezpieczeństwa coraz częściej integrują też aspekty etyczne i społeczne, co jest wynikiem rosnącej świadomości wpływu technologii na życie codzienne. Problemy związane z prywatnością, etyką AI czy odpowiedzialnością za błędy technologiczne stają się integralnym elementem dyskusji o bezpieczeństwie w cyberprzestrzeni. Cyberbezpieczeństwo jako dziedzina naukowa również przechodzi ewolucję. Badania skupiają się nie tylko na technicznych aspektach ochrony, ale także na modelach zarządzania ryzykiem, psychologii użytkowników oraz wpływie regulacji na praktyki organizacyjne. Istotnym kierunkiem badań jest też analiza podatności w nowoczesnych technologiach, takich jak komputery kwantowe, które w niedługiej przyszłości mogą zrewolucjonizować zarówno ochronę, jak i zagrożenia w cyberprzestrzeni.

1.2. Rodzaje i klasyfikacja zagrożeń

Rozwój technologii informacyjno-komunikacyjnych oraz powszechna cyfryzacja społeczeństw przyczyniły się do wzrostu liczby i złożoności zagrożeń cyfrowych. Przez ostatnie dekady zagrożenia cyfrowe przechodziły dynamiczne przemiany, związane zarówno z postępującą cyfryzacją, rozwojem technologii, zmianami w motywacjach cyberprzestępców (wzrost znaczenia motywacji ekonomicznej i politycznej), czynnikami geopolitycznymi (ataki sponsorowane przez państwa i cyberwojny), jak i pandemią COVID-19, która przyczyniła się do wzrostu wykorzystania technologii zdalnych, zwiększyła zależność od systemów cyfrowych i uwypukliła luki technologiczne i kompetencyjne w obszarze technologii informacyjnych. Początkowo zagrożenia w cyberprzestrzeni związane były głównie z nieuprawnionym dostępem lub utratą danych oraz z działaniami destrukcyjnymi wykorzystującymi relatywnie proste mechanizmy w postaci np. wirusów komputerowych.

²⁸ K. Stoddart, *Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'*, „Applied Cybersecurity & Internet Governance” 2024, no. 3(1).

²⁹ *Understanding Cybersecurity Throughout the Electoral Process: A Reference Document an Overview of Cyber Threats and Vulnerabilities in Elections*, https://www.usaid.gov/sites/default/files/2023-01/Understanding-Cybersecurity-Throughout-the-Electoral-Process_1.pdf (11.01.2025).

Obecnie cyberzagrożenia obejmują bardzo szeroki wachlarz potencjalnych niebezpieczeństw – od awarii sprzętu, wycieków danych, poprzez kradzieże, celowe niszczenie danych lub infrastruktury, blokowanie usług, ataki phishingowe³⁰, kampanie dezinformacyjne, aż po skomplikowane operacje cyberwojenne. Nowe technologie, takie jak sztuczna inteligencja, uczenie maszynowe i automatyzacja, tworzą środowisko do rozwoju nieznanych wcześniej, coraz częściej hybrydowych technik i wektorów ataku³¹. Rozwój bezprzewodowej komunikacji, sieci społecznościowych, Internetu Rzeczy, chmury obliczeniowej czy elektronicznych usług publicznych znacząco poszerza obszar cyfrowej aktywności, a tym samym tworzy nowe zagrożenia dla bezpieczeństwa cyfrowego.

Ewolucja i rozwój czynników mających negatywny wpływ na bezpieczeństwa informacji niesie ze sobą konieczność ich zrozumienia oraz dokładnego opisu i charakterystyki. Dokładna klasyfikacja pozwalająca na precyzyjne określenie różnych rodzajów cyberzagrożeń umożliwia pełniejsze zrozumienie zagrożeń i źródeł ich pochodzenia, a także właściwe dopasowanie strategii obronnych. Obecnie stosowane klasyfikacje cyberzagrożeń opierają się na szeregu różnych kryteriów, wśród których można wymienić:

1. Źródła pochodzenia zagrożenia:
 - a) zewnętrzne – zlokalizowane są poza organizacją (np. ataki dokonywane przez cyberprzestępców, hacktywistów³², grupy terrorystyczne czy obce państwa);
 - b) wewnętrzne – wynikające z działań pracowników lub partnerów biznesowych, zarówno celowych (np. działania sabotażowe), jak i nieumyślnych (błędy ludzkie)³³.
2. Intencjonalność (umyślność) zagrożeń:
 - a) celowe – są wynikiem świadomych i zaplanowanych działań mających na celu wyrządzenie szkody organizacji lub osobie (np. szpiegostwo lub sabotaż komputerowy, kradzież danych czy dystrybucja nielegalnych treści);

³⁰ *Phishing* to rodzaj cyberprzestępstwa, w którym atakujący podszywa się pod zaufaną osobę, instytucję lub organizację w celu wyłudzenia poufnych informacji, takich jak dane logowania, numery kart kredytowych, dane osobowe czy kody autoryzacyjne.

³¹ Wektory ataków, definiowane jako sposoby, za pomocą których cyberprzestępcy uzyskują nieautoryzowany dostęp do systemów lub sieci, mogą obejmować różne techniki, np. wykorzystanie słabych lub skompromitowanych danych uwierzytelniających (m.in. upublicznionych w wyniku wycieków loginy i hasła), ataki socjotechniczne, zagrożenia wewnętrzne, niezaktualizowane oprogramowanie, brak szyfrowania oraz błędy w konfiguracji usług.

³² Hacktywizm (ang. *hacktivism*) to pojęcie stworzone poprzez połączenie słów *hacking* i *activism*, które oznacza użycie komputerów i sieci do promowania celów społecznych, politycznych lub religijnych, w tym szczególnie wolności słowa, praw człowieka i dostępu do informacji. Zob. P. Krapp. *Terror and Play, or What was Hacktivism?*, „Grey Room” 2015, no. 21, s. 70–93. Wśród najbardziej znanych grup kojarzonych z ideą hacktywizmu wymienia się np. Anonymous czy LulzSec.

³³ M. Jouini, L. Ben Arfa Rabai, A. Ben Aissa, L. Ben, *Classification of security threats in information systems*, „Procedia Computer Science” 2014, no. 32, s. 489–496.

- b) niecelowe – wynikają z niezamierzonych działań, często związanych z błędami ludzkimi, zaniedbaniami lub awariami technicznymi.
- 3. Charakter zagrożeń:
 - a) techniczne – zagrożenia związane z wykorzystaniem technologii informatycznych i luk w systemach IT;
 - b) nietechniczne – zagrożenia związane z czynnikami ludzkimi, organizacyjnymi lub proceduralnymi, np. ataki socjotechniczne³⁴ wykorzystujące ludzkie błędy i zaniedbania czy też nieprzestrzeganie ustalonych zasad bezpieczeństwa.
- 4. Czynniki generujące zagrożenia:
 - a) ludzie – zagrożenia spowodowane działaniami człowieka (osób z wnętrza organizacji lub hakerów), które powodują szkody lub zagrożenia dla systemów;
 - b) środowisko – klęski żywiołowe, np. trzęsienia ziemi, powodzie, pożary, czy zwieżręta, które mogą powodować poważne szkody w systemach informatycznych;
 - c) technologia – zagrożenia, których geneza wynika z wykorzystania takich środków technicznych, jak sprzęt (*hardware*) i oprogramowanie (*software*) oraz sieci i urządzenia służące do przesyłania informacji i zasilania energią elektryczną³⁵.
- 5. Rodzaj aktorów (podmiotów) stanowiących zagrożenie³⁶:
 - a) *script kiddies* – osoby o ograniczonych umiejętnościach technicznych, które wykorzystują gotowe narzędzia i skrypty do przeprowadzania ataków;
 - b) cyberprzestępcy (ang. *cybercriminals*) – grupy lub jednostki działające dla zysku finansowego, posiadające większe zasoby i wiedzę niż *script kiddies*;
 - c) hacktywiści (ang. *hacktivists*) – aktorzy motywowani ideologicznie, politycznie lub społecznie, którzy dysponują umiarkowanymi umiejętnościami i często współpracują w grupach;
 - d) zorganizowane grupy przestępcze (ang. *organized crime groups*) – „profesjonalne” grupy przestępcze działające na skalę międzynarodową, z zaawansowanymi narzędziami i strukturami;
 - e) sponsorowani przez państwa (ang. *state-sponsored actors*) – najbardziej zaawansowani aktorzy, posiadający ogromne zasoby finansowe, technologiczne i kadrowe, działający w interesie państw, np. grupy APT (ang. *Advanced Persistent Threat*)³⁷.

³⁴ W przeciwieństwie do ataków technicznych wykorzystujących techniki i narzędzia o charakterze informatycznym, ataki socjotechniczne wykorzystują ludzkie słabości, takie jak zaufanie, strach czy ciekawość.

³⁵ L. Ruf, A. Thorn, T. Christen, B. Gruber, R. Portmann, *Threat Modeling in Security Architecture – The Nature of Threats*, 2008, https://www.iss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf (5.11.2024).

³⁶ Bardziej rozbudowaną charakterystykę aktorów proponuje: A. Reza, *Cyber Threat Profiling: Understanding the Different Threat Actors*, <https://www.linkedin.com/pulse/cyber-threat-profiling-understanding-different-actors-reza-adineh> (5.02.2025).

³⁷ A. Lemay, J. Calvet, F. Menet, J.M. Fernandez, *Survey of publicly available reports on advanced persistent threat actors*, „Computers & Security” 2018, no. 72, s. 26–59.

6. Motywacja atakującego³⁸:
 - a) pieniądze – działania oparte na motywacji finansowej, prowadzące np. do kradzieży środków finansowych czy wymuszenia okupu;
 - b) ideologia – działania motywowane przekonaniem politycznymi lub ideologicznymi, np. hacktywizm czy szpiegostwo;
 - c) kompromitacja – dotyczy sytuacji, w których podstawą określonych działań lub zagrożeń jest wymuszenie oparte na groźbie lub szantażu;
 - d) ego – odnosi się do osobistych potrzeb psychologicznych lub emocjonalnych i może obejmować np. chęć uznania i podziwu, pragnienie pocucia ważności i wpływu, potrzebę zemsty czy też poszukiwanie emocji i podniecenia³⁹.
7. Rodzaj wykorzystywanych technik ataku (wektor ataku):
 - a) złośliwe oprogramowanie (*malware*) – wykorzystanie szkodliwych programów komputerowych, które mają na celu uszkodzenie, zakłócenie działania lub uzyskanie nieautoryzowanego dostępu do systemów komputerowych, sieci lub urządzeń;
 - b) ataki socjotechniczne – polegają na manipulacji psychologicznej ofiarą w celu nakłonienia jej do ujawnienia poufnych informacji lub podjęcia określonych działań;
 - c) wykorzystanie podatności (eksploatacja) – wykorzystanie luk i błędów w protokołach, systemach lub aplikacjach w celu uzyskania nieautoryzowanego dostępu lub wykonania szkodliwych działań w atakowanym systemie;
 - d) ataki na infrastrukturę sieciową – działania mające na celu zakłócenie, przejęcie kontroli, uszkodzenie lub wykorzystanie komponentów sieci komputerowych w celu osiągnięcia korzyści finansowych, szpiegostwa lub sabotażu; mogą obejmować zarówno działania wykorzystujące luki techniczne w urządzeniach i protokołach, jak i metody socjotechniczne;
 - e) wykorzystanie fizycznego dostępu – polega na bezpośrednim oddziaływaniu na infrastrukturę IT poprzez fizyczny kontakt z urządzeniami lub elementami sieci; tego typu zagrożenia wynikają z braku odpowiednich zabezpieczeń fizycznych, niekontrolowanego dostępu do pomieszczeń serwerowych, urządzeń końcowych, kabli sieciowych czy punktów dostępowych.
8. Cel ataku:
 - a) ataki na dane – celem jest kradzież, zniszczenie lub modyfikacja danych;

³⁸ Motywy cyberprzestępców określane są za pomocą akronimu MICE, którego rozwinięciem są słowa: *money, ideology, compromise, ego*. Warto jednak zauważyć, że wskazane motywy często występują w połączeniu i mogą tworzyć złożony obraz pobudek, jakimi kierują się cyberprzestępcy.

³⁹ F. Kaiser, M. Wiens, F. Schultmann, *Motivation-based Attacker Modelling for Cyber Risk Management: A Quantitative Content: Analysis and a Natural Experiment*, „Journal of Information Security and Cybercrimes Research” 2021, no. 4, s. 30–43.

- b) ataki na dostępność – zmierzają do zakłócenia lub uniemożliwienia działania usług czy urządzeń;
 - c) ataki na integralność – mają na celu zmianę treści informacji lub sposobu działania oprogramowania;
 - d) ataki na poufność – umożliwiają nieuprawniony dostęp do danych.
9. Skala i zasięg ataku:
- a) ukierunkowane (lokalne) – precyzyjne ataki na konkretną organizację, osobę, region lub kraj;
 - b) masowe (globalne) – ataki wymierzone w szerokie grono odbiorców, często realizowane w sposób zautomatyzowany; mogą obejmować wiele krajów, sektorów czy osób.
10. Fazy ataku:
- a) rozpoznanie (ang. *reconnaissance*) – początkowy etap, w którym dokonywany jest wybór celu i gromadzenie informacji o infrastrukturze IT, zabezpieczeniach oraz danych o pracownikach organizacji (np. poprzez biały wywiad – OSINT); pozwala to atakującemu na znalezienie słabych punktów, a nawet luk w zabezpieczeniach;
 - b) uzbrajanie (ang. *weaponization*) – etap obejmuje wykorzystanie informacji zdobytych w trakcie rekonesansu, aby przygotować złośliwe oprogramowanie oraz opracować sposoby wykorzystania słabych punktów atakowanego celu;
 - c) dostarczanie (ang. *delivery*) – w tej fazie cyberprzestępcy podejmują próbę dostarczenia przygotowanego złośliwego oprogramowania do systemów organizacji lub wykorzystania zidentyfikowanych słabych punktów; złośliwe oprogramowanie może być dostarczane za pomocą załączników przesyłanych wiadomości lub linków prowadzących do zainfekowanych stron internetowych;
 - d) przełamanie (ang. *exploitation*) – na tym etapie dochodzi do wykorzystania podatności systemu lub użytkownika, aby uzyskać nieautoryzowany dostęp do zasobów; przykładowe działania obejmują wykorzystanie podatności oprogramowania (np. niezłatanne luki w systemie operacyjnym) lub socjotechniki w celu wprowadzenia szkodliwego kodu;
 - e) instalacja (ang. *installation*) – po pomyślnym wykorzystaniu podatności następuje instalacja złośliwego oprogramowania, które umożliwia dalszą kontrolę nad systemem ofiary oraz zapewnia trwałość ataku;
 - f) dowodzenie i kontrola (ang. *command and control* – C2) – zainstalowane oprogramowanie komunikuje się z serwerem atakującego, umożliwiając mu sterowanie zainfekowanym systemem, w tym np. zdalne wykonywanie poleceń w celu utrzymania i rozwijania ataku;

- g) działania na celu (ang. *actions on objectives*) – ostatni etap, w którym atakujący realizuje swój cel, którym może być kradzież danych, zakłócenie działania systemów lub ich trwałe uszkodzenie⁴⁰.

1.3. Cyberzagrożenia a ryzyko, incydenty i ataki

Analizując różne podejścia do usystematyzowania cyberzagrożeń, należy zauważyć, że istniejące typologie zagrożeń cyfrowych różnią się nie tylko przyjętym kryterium podziału, ale też stosowaną terminologią. W obszarze cyberbezpieczeństwa często używane są takie pojęcia, jak cyberzagrożenia, ryzyko, incydenty czy ataki (cyberataki). Chociaż w sferze cyfrowego bezpieczeństwa terminy te często się zazębiają i przenikają, to w praktyce ich znaczenie i zakres zastosowania są różne.

Cyberzagrożenie to szerokie pojęcie obejmujące różnorodne zagrożenia występujące w przestrzeni cyfrowej, które mogą negatywnie wpływać na bezpieczeństwo systemów informatycznych, sieci, danych oraz użytkowników. Może być ono definiowane jako potencjalne naruszenie bezpieczeństwa, które występuje, gdy istnieje okoliczność, zdolność, działanie lub zdarzenie, które może naruszyć bezpieczeństwo i spowodować szkody⁴¹, lub też jako wszelkie okoliczności lub zdarzenia, które mogą mieć niekorzystny wpływ na działalność i aktywa organizacji, osób lub społeczeństwa za pośrednictwem systemu informatycznego – poprzez nieautoryzowany dostęp, zniszczenie, ujawnienie lub modyfikację informacji i/lub odmowę świadczenia usługi (ang. *denial of service*)⁴². Cyberzagrożenia mogą mieć charakter techniczny, np. złośliwe oprogramowanie, i nie-techniczny (społeczny), np. dezinformacja czy oszustwa internetowe. Źródłem cyfrowych zagrożeń mogą być zarówno świadome działania (np. kradzież danych czy uniemożliwienie dostępu do usług), jak i przypadkowe zdarzenia (np. awarie). Cyberzagrożenie to potencjalne niebezpieczeństwo lub zagrożenie dla systemów informatycznych, sieci, danych, organizacji lub osób, które może, ale nie musi się zmaterializować.

Incydent to rzeczywiste zdarzenie, które już nastąpiło i ma negatywny wpływ na bezpieczeństwo systemów informatycznych lub danych. Zgodnie z definicją z dyrektywy NIS2 oznacza on „zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem”. Jest to zatem zdarzenie, które ma wpływ na dane, usługi bądź sieci i systemy

⁴⁰ Podział łańcucha ataku na poszczególne fazy został opracowany przez badaczy z firmy Lockheed Martin w 2011 r. i jest znany jako Cyber Kill Chain.

⁴¹ R. Shirey, *Internet Security Glossary*, Internet Engineering Task Force 2000, <https://datatracker.ietf.org/doc/html/rfc2828> (9.03.2025).

⁴² *National Institute of Standards and Technology – glossary*, <https://csrc.nist.gov/glossary/term/threat> (14.01.2025).

teleinformatyczne, a które skutkuje zaburzeniem lub utratą jednego lub wielu atrybutów bezpieczeństwa: poufności, dostępności, integralności lub autentyczności⁴³. Z kolei według amerykańskiego Instytutu Standardów i Technologii incydent jest rozumiany jako „zdarzenie, które skutkuje rzeczywistym lub potencjalnym zagrożeniem dla poufności, integralności lub dostępności systemu informatycznego lub informacji, które system przetwarza, przechowuje lub przesyła, lub które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub dopuszczalnych zasady użytkowania”⁴⁴. Ogólnie pojęcie to można interpretować jako każde zdarzenie, które ma lub potencjalnie może mieć negatywny wpływ na cyfrowe bezpieczeństwo systemu, podmiotu lub osoby. Incydenty mogą być wynikiem celowych działań lub innych nieprzewidzianych zdarzeń.

Polska ustawa o krajowym systemie cyberbezpieczeństwa wyróżnia następujące rodzaje incydentów:

- a) incydent krytyczny – skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi;
- b) incydent poważny – powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej;
- c) incydent istotny – ma istotny wpływ na świadczenie usługi cyfrowej;
- d) incydent o podmiocie publicznym – powoduje lub może spowodować obniżenie jakości albo przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
- e) incydent zwykły – ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo; ten incydent nie podlega zgłoszeniu, ale też należy go obsługiwać.

Atak (cyberatak) jest pojęciem znacznie węższym od incydentu, bowiem obejmuje jedynie celowe działania w sferze technologii cyfrowych zmierzające do wyrządzenia szkody. Cyberataki mają na celu wyłączenie, zakłócenie, zniszczenie lub kontrolę systemów komputerowych bądź zmianę, zablokowanie, usunięcie, manipulowanie lub kradzież danych przechowywanych w tych systemach⁴⁵. Uznaje się je za jeden z rodzajów incydentów związanych z cyberbezpieczeństwem.

Ryzyko w kontekście cyberbezpieczeństwa odnosi się do potencjalnego wpływu i prawdopodobieństwa wystąpienia incydentu. Jest to kombinacja zagrożenia, podatności systemu oraz potencjalnych konsekwencji. Zgodnie z definicją zawartą w art. 6

⁴³ M. Pawlak, *Zarządzanie incydentami cyberbezpieczeństwa w praktyce*, PTI 2024, <https://pti.org.pl/zarządzanie-incydentami-cyberbezpieczenstwa-w-praktyce/> (5.04.2025).

⁴⁴ M. Nieves, K. Dempsey, V.Y. Pillitteri, *An introduction to information security*, NIST SP 800-12r1, National Institute of Standards and Technology 2017, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> (5.04.2025).

⁴⁵ *What is a cyber attack? How they work and how to stop them*, <https://www.techtarget.com/searchsecurity/definition/cyber-attack> (19.02.2025).

dyrektywy NIS2 „ryzyko oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydem, wyrażoną jako wypadkowa wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwa wystąpienia takiego incydemu”. Tak rozumiane ryzyko oznacza możliwości wystąpienia zdarzenia, które niesie ze sobą określone skutki (z założenia negatywne) oraz którego prawdopodobieństwo wystąpienia w przyszłości można oszacować.

Właściwe określenie ryzyka oraz oszacowanie jego prawdopodobieństwa jest podstawą zarządzania ryzykiem w organizacjach, czyli kompleksowych działań obejmujących:

- identyfikację potencjalnych zagrożeń,
- ocenę prawdopodobieństwa ich wystąpienia,
- analizę możliwych skutków,
- wdrażanie środków mających na celu minimalizację ryzyka.

W obliczu gwałtownego tempa zmian, jakim podlega cyfrowa przestrzeń, jednoznaczna klasyfikacja cyberzagrożeń staje się niezwykle trudna, ponieważ granice między poszczególnymi rodzajami zagrożeń coraz bardziej się zacierają, a ich charakterystyka ulega dynamicznym przeobrażeniom. W efekcie cyberzagrożenia, incydenty czy ataki są często w różny sposób opisywane i klasyfikowane, co powoduje zamieszanie, trudności w zrozumieniu ich istoty, a także uniemożliwia porównanie danych pozwalających na precyzyjne określenie skali poszczególnych zdarzeń.

W reakcji na rosnącą skalę i złożoność incydemów w cyberprzestrzeni wielokrotnie podejmowano próby stworzenia uniwersalnej klasyfikacji cyberzagrożeń. Analizy akademickie oraz opracowania organizacji zajmujących się cyberbezpieczeństwem starały się porządkować różne rodzaje ataków, metod i motywacji sprawców. Pomimo szeregu inicjatyw i koncepcji żadna z proponowanych klasyfikacji nie zyskała powszechnej akceptacji i w praktyce różne podmioty w zależności od potrzeb i specyfiki korzystają w różnym zakresie z różnych podejść i istniejących taksonomii.

Dynamiczny i złożony charakter środowiska cyberbezpieczeństwa powoduje, że wymienione wcześniej kryteria klasyfikacji cyberzagrożeń oraz ich podziały nie stanowią zamkniętego i niezmiennego katalogu. Wśród czynników, które wymuszają elastyczne podejście i regularne aktualizacje taksonomii cyberzagrożeń, można wymienić:

- a) nowe technologie i metody ataku, których ewolucja tworzy nowe rodzaje zagrożeń;
- b) zacieranie się granic między kategoriami – ataki coraz częściej łączą różne techniki i motywacje;
- c) pojawianie się nowych motywacji i grupy atakujących, co dynamicznie zmienia krajobraz zagrożeń;
- d) postępujący proces globalizacji i zmiany regulacji prawnych, które wymuszają adaptację istniejących klasyfikacji.

Z uwagi na złożoność i zmieniający się charakter cyberzagrożeń oraz zależność zagrożeń od kontekstu (charakter zagrożenia może się różnić w zależności od branży,

infrastruktury IT czy polityki bezpieczeństwa organizacji) klasyfikacje oparte na pojedynczym kryterium okazują się niewystarczające, gdyż nie oddają ich pełnego obrazu. Dlatego kompleksowe podejście do klasyfikacji cyberzagrożeń powinno uwzględniać wiele wymiarów, umożliwiając pełniejsze zrozumienie potencjalnych niebezpieczeństw i rzeczywistych incydentów oraz lepsze dopasowanie strategii obronnych.

W podejściu wielokryteriowym klasyfikacja cyfrowych zagrożeń może się opierać na zastosowaniu kombinacji kilku różnych kryteriów, np. źródła zagrożenia, motywacji atakującego, rodzaju wykorzystywanych technik ataku czy wpływu na organizację. Przykładem klasyfikacji wielokryteriowych jest taksonomia ataków opracowana przez Hansmana i Hunta⁴⁶, w której podział opiera się na czterech wymiarach:

- a) wektor ataku;
- b) cel ataku;
- c) rodzaj wykorzystanych podatności (luk)⁴⁷;
- d) rodzaj wykorzystanej zawartości (ang. *payload*) w postaci np. szkodliwego oprogramowania lub efekty ataku.

Dzięki zdefiniowaniu w obrębie każdego wymiaru dodatkowych, bardziej szczegółowych cech, w ramach stworzonej matrycy, ataki mogą być przyporządkowane do szczegółowo określonych kategorii i podkategorii. Pomimo wykorzystania kilku wymiarów w procesie systematyzacji zagrożeń oraz propozycji uzupełnienia klasyfikacji o dodatkowe elementy, takie jak: zakres szkód wyrządzonych atakiem, koszty przywrócenia systemu do stanu przed atakiem, czas propagacji (rozprzestrzeniania się ataku) czy rodzaj wykorzystanych metod obrony, opracowana hierarchia ma szereg słabości, które powodują, że możliwości jej stosowania ograniczone są głównie do ataków wykorzystujących szkodliwe oprogramowanie.

Innym przykładem wielokryteriowej charakterystyki ataków cyfrowych jest opracowany w 2009 roku model zagrożeń cyfrowych znany jako AVOIDIT⁴⁸. Nazwa pochodzi od pierwszych liter pięciu głównych aspektów ataków, które obejmuje model:

⁴⁶ S. Hansman, R. Hunt, *A taxonomy of network and computer attacks*, „Computers & Security” 2005, no. 24, s. 31–43.

⁴⁷ Do klasyfikacji podatności, jakie występują w sprzęcie lub oprogramowaniu, powszechnie wykorzystywany jest system katalogowania CVE (ang. *Common Vulnerabilities and Exposures*) stworzony w 1999 r. przez firmę MITRE Corporation w oparciu o zgłoszenia firm technologicznych, instytutów badawczych czy organizacji zajmujących się cyberbezpieczeństwem. Na 13 września 2024 r. w bazie CVE znajdowało się 240 830 wpisów. Uzupełnieniem bazy podatności CVE jest system oceny poziomu zagrożenia dla każdej podatności (ang. *Common Vulnerability Scoring System – CVSS*). W oparciu o rozbudowany algorytm oceny podatnościom wskazanym w systemie CVE przypisywany jest poziom krytyczności zagrożenia w skali od 0 do 10. <https://nfl.pl/baza-wiedzy/czym-jest-cve/#jaka-jest-relacja-miedzy-cve-a-cvss> (2.04.2025).

⁴⁸ C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, C. Wu, *AVOIDIT: A Cyber Attack Taxonomy. CTIT technical reports series*, 2009, https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy (22.03.2025).

- a) wektor ataku (ang. *attack vector*) – ataki charakteryzowane są ze względu na metodę lub ścieżkę, za pomocą której atakujący uzyskuje dostęp do systemu lub zasobu;
- b) wpływ operacyjny (ang. *operational impact*) – charakterystyka bazuje na ocenie skutków, jakie atak wywiera na działalność organizacji (np. przerwy w działaniu usług, zmniejszenie wydajności systemów, utrata zaufania klientów czy koszty naprawy szkód);
- c) mechanizmy obronne (ang. *defense*) – grupowanie ataków następuje w oparciu o strategię i mechanizmy obronne stosowane w celu zapobiegania, wykrywania oraz reagowania na ataki (np. systemy wykrywania i zapobiegania włamaniom, szyfrowanie danych oraz polityki bezpieczeństwa);
- d) wpływ na informacje (ang. *information impact*) – systematyka ataków w tym względzie opiera się na konsekwencjach związanych z bezpieczeństwem informacji (np. kradzież, nieuprawniony dostęp, manipulacja lub utrata danych);
- e) cel ataku (ang. *target*) – cyberataki różnicowane są z uwagi na docelowy system, infrastrukturę lub użytkownika będącego przedmiotem ataku (np. systemy krytyczne, dane osobowe użytkowników, sieci korporacyjne czy usługi publicznie).

Klasyfikacja ataków dokonywana w oparciu o model AVOIDIT dzieli je na 5 głównych kategorii (zgodnie z powyższym opisem), 29 podkategorii i 22 podpodkategorie. Model ten jest często wykorzystywany w analizach ryzyka i przy opracowywaniu strategii obronnych, ponieważ umożliwia kompleksowe spojrzenie na zagrożenia, uwzględniając zarówno aspekty techniczne, jak i operacyjne. W literaturze naukowej oraz praktyce działań związanych ze zwiększaniem bezpieczeństwa cyfrowego klasyfikacja AVOIDIT jest stosowana do osiągnięcia takich celów, jak:

- identyfikacja luk w zabezpieczeniach organizacji,
- modelowanie zagrożeń (ang. *Threat Modeling*),
- tworzenie planów reakcji na incydenty bezpieczeństwa,
- edukacja pracowników z zakresu cyberbezpieczeństwa.

W roku 2021 model AVOIDIT został znacząco rozwinięty przez zespół badaczy⁴⁹, którzy wprowadzili trzy dodatkowe aspekty pozwalające na bardziej szczegółową klasyfikację ataków. Zaproponowany w wyniku tych zmian model nazwano AVOIDITALS. Trzy kolejne jego cechy to:

- a) przeciwnicy (ang. *adversaries*) – umożliwia klasyfikację ataków z uwagi na rodzaj aktorów zagrożeń, którzy określani są często jako cyberprzeciwnicy lub adwersarze;

⁴⁹ M. Syafrizal, S.R. Selamat, N.A. Zakaria, *AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure*, „International Journal of Computer Science and Network Security” 2021, vol. 21, no. 8, s. 1–12.

- b) poziom automatyzacji (ang. *level of automation*) – umożliwia rozróżnienie ataków ze względu na zakres wykorzystania narzędzi automatyzujących działania cyberprzestępców;
- c) metody lokalizacji źródłowego adresu IP (ang. *source IP traceback*) – umożliwia rozróżnienie cyberataków ze względu na różne metody fałszowania prawdziwej lokalizacji agresora lub źródła ataku.

Taksonomia AVOIDITALS pozwala klasyfikować cyberataki według 8 głównych kategorii (5 z AVOIDIT i 3 dodatkowe, określone w AVOIDITALS), 105 podkategorii i 142 podpodkategorii, stanowiąc narzędzie klasyfikacji w oparciu o zdefiniowane wzorce cyberataków.

Spśród taksonomii, które znajdują szerokie zastosowanie w praktyce, na uwagę zasługuje systematyka incydentów komputerowych eCSIRT.net opracowana na potrzeby powołanej do życia w 2004 roku Europejskiej Agencji ds. Cyberbezpieczeństwa. Pierwotna wersja klasyfikacji została przygotowana przez europejską sieć zespołów reagowania na incydenty komputerowe (ang. *Computer Emergency Response Team* – CSIRT) w celu standaryzacji klasyfikacji incydentów bezpieczeństwa informatycznego. Aktualnie stosowana jest szósta wersja (oznaczona jako mkVI), stanowiąca adaptację i aktualizację oryginalnej taksonomii eCSIRT.net, uwzględniająca rozwój zagrożeń oraz potrzebę precyzyjniejszej klasyfikacji incydentów.

Taksonomia eCSIRT.net mkVI jest ważnym narzędziem umożliwiającym standaryzację klasyfikacji incydentów bezpieczeństwa w Europie, co ma kluczowe znaczenie dla efektywnej wymiany informacji w zakresie kategoryzacji i raportowania incydentów. Jej struktura umożliwia sprawną komunikację i współpracę między różnymi organizacjami zajmującymi się cyberbezpieczeństwem i jest szeroko stosowana przez CSIRT w Europie, w tym przez CERT Polska, do klasyfikacji i analizy incydentów bezpieczeństwa. Jest także wykorzystywana jako punkt wyjścia dla opracowywania innych taksonomii, takich jak np. zestandaryzowany system klasyfikacji incydentów cybernetycznych (ang. *Common Taxonomy for Law Enforcement and CSIRTs*), który powstał w celu ułatwienia współpracy między organami ścigania (np. policją, prokuraturą) a zespołami reagowania na incydenty komputerowe, umożliwiając skuteczniejszą wymianę informacji i koordynację działań w ramach zwalczania cyberprzestępczości.

Struktura taksonomii eCSIRT.net mkVI obejmuje dziesięć głównych kategorii incydentów:

- obraźliwe i nielegalne treści,
- szkodliwe oprogramowanie,
- gromadzenie informacji,
- próby włamań,
- włamania,
- dostępność zasobów,
- atak na bezpieczeństwo informacji,

- oszustwa komputerowe,
- podatne usługi,
- inne.

Każda z tych głównych kategorii obejmuje bardziej szczegółowe podkategorie, w których przedstawiono przykłady i wyjaśnienia (tabela 1)⁵⁰.

Tabela 1. Systematyka incydentów komputerowych eCSIRT.net mkVI

Klasyfikacja incydentu	Przykład incydentu	Opis
Obrażliwe i nielegalne treści	Spam	Niechciana poczta e-mail wysłana w sposób masowy bez zgody odbiorcy
	Mowa nienawiści	Dyskredytacja lub dyskryminacja, np. cyberstalking, rasizm
	Treści dziecięce/seksualne/przemoc	Pornografia dziecięca, gloryfikacja przemocy
Szkodliwe oprogramowanie	Wirus	Oprogramowanie wprowadzone do systemu w celu wyrządzenia szkody
	Robak	
	Koń trojański	
	Oprogramowanie szpiegowskie	
	Dialer	
	Rootkit	
Gromadzenie informacji	Skanowanie	Wysyłanie zapytań do systemu w celu identyfikacji słabych punktów (np. odpytywanie DNS, skanowanie portów)
	Podsłuch	Obserwacja i rejestrowanie ruchu sieciowego
	Inżynieria społeczna (socjotechnika)	Zdobywanie informacji dzięki wykorzystaniu manipulacji psychologicznej lub podstępów
Próby włamań	Wykorzystanie znanych luk systemowych	Próby wykorzystania znanych podatności systemu
	Próby logowania	Wielokrotne próby logowania np. z wykorzystaniem metody <i>brute force</i>
	Nowe sygnatury ataków	Wykorzystanie nowego, nieznanego exploita
Włamania	Naruszenie konta uprzywilejowanego	Udane naruszenie dostępu do konta, usługi lub aplikacji
	Naruszenie konta zwykłego	
	Naruszenie aplikacji	
	Bot	

⁵⁰ Incident Classification/Incident Taxonomy according to eCSIRT.net – adapted, <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf> (20.02.2025).

Klasyfikacja incydentu	Przykład incydentu	Opis
Dostępność zasobów	DoS	Wysyłanie do system ogromnych ilości danych (pakietów), co prowadzi do opóźnień lub przerwy w działaniu
	DDoS	
	Sabotaż	Celowe, złośliwe działanie mające na celu zakłócenie, zniszczenie lub uszkodzenie systemów komputerowych, sieci, danych lub usług organizacji
	Brak dostępności spowodowany czynnikami losowymi	Przerwy spowodowane awariami, działaniami sił wyższych lub błędami ludzkimi
Atak na bezpieczeństwo informacji	Nieuprawniony dostęp do informacji	Nieautoryzowany dostęp do danych
	Nieuprawniona modyfikacja informacji	
Oszustwa komputerowe	Nieautoryzowane wykorzystanie zasobów	Korzystanie z zasobów do nieautoryzowanych celów
	Naruszenie praw autorskich	Dystrybucja nielegalnego oprogramowania
	Kradzież tożsamości	Podszywanie się pod inną osobę w celu uzyskania korzyści
	<i>Phishing</i>	Podszywanie się pod inną osobę lub organizację w celu wyłudzenia danych
Atak z wykorzystaniem podatnych usług	Otwarte usługi podatne na nadużycia	Nieodpowiednio zabezpieczone lub niezaktualizowane urządzenia, np. serwery DNS, drukarki publiczne itp.
Inne	Wszystkie incydenty, które nie pasują do powyższych kategorii	Rosnąca liczba incydentów w tej kategorii wskazuje na potrzebę aktualizacji klasyfikacji

Źródło: opracowanie własne na podstawie: Reference Incident Classification Taxonomy, 2018, <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy> (12.02.2025).

Mimo że taksonomia została opracowana wiele lat temu (i przeszła szereg adaptacji), główne kategorie pozostają aktualne i można je nadal wykorzystywać. Tego samego nie można powiedzieć o podkategoriach, które mogą czasem prowadzić do problemów z klasyfikacją incydentu. Na przykład nie jest już szczególnie przydatne rozróżnianie między atakami DoS i atakami DDoS ani określanie, co jest „uprzywilejowanym naruszeniem konta”, „nieuprzywilejowanym naruszeniem konta” lub „naruszeniem aplikacji”. W praktyce podkategorie stały się częścią opisu, a nie konkretnym schematem klasyfikacji. Obecnie naprawdę trudno jest określić, czy konkretne złośliwe oprogramowanie jest wirusem, robakiem, trojanem, oprogramowaniem szpiegującym czy dialerem.

Przedstawione przykłady klasyfikacji cyberzagrożeń czy ataków to jedynie niewielka część taksonomii opracowanych przez naukowców i specjalistów z zakresu

cyberbezpieczeństwa⁵¹. W różnych krajach, w zależności od specyfiki organizacji, celów, jakim mają służyć, czy też z uwagi na specyficzny kontekst regulacyjny, spotkać można różne podejścia do systematyki.

Różnice mogą wynikać także z lokalnych priorytetów strategicznych i zagrożeń geopolitycznych, które kształtują podejście do cyberbezpieczeństwa. Na przykład kraje narażone na cyberataki ze strony podmiotów państwowych mogą się skupiać na zagrożeniach wywiadowczych i atakach na infrastrukturę krytyczną, podczas gdy inne państwa koncentrują się na zagrożeniach ekonomicznych, takich jak kradzież własności intelektualnej.

Nie bez znaczenia jest również dostępność zasobów i zdolności analitycznych poszczególnych organizacji, które determinują poziom szczegółowości stosowanych taksonomii. Duże organizacje międzynarodowe dysponujące zespołami analitycznymi mogą sobie pozwolić na wdrożenie bardziej złożonych systemów klasyfikacji, podczas gdy mniejsze podmioty wybierają uproszczone schematy dostosowane do ich możliwości operacyjnych. Cechą wspólną dla systematyk, które znajdują zastosowanie w praktyce, jest konieczność ich systematycznego przeglądu i uaktualniania w celu dostosowania do szybko zmieniającego się krajobrazu cyberzagrożeń.

1.4. Cyberodporność

Cyberbezpieczeństwo stanowi fundament ochrony systemów informatycznych, sieci oraz danych przed zagrożeniami wynikającymi z działalności cyberprzestępczej, błędów ludzkich czy awarii technicznych. Jednak w obliczu rosnącej liczby zaawansowanych ataków oraz dynamicznie zmieniającego się krajobrazu zagrożeń tradycyjne podejście do cyberbezpieczeństwa, skoncentrowane na prewencji i detekcji, okazuje się niewystarczające. W tym kontekście coraz większego znaczenia nabiera cyberodporność (ang. *cyber resilience*), która nie tylko uwzględnia mechanizmy ochronne, ale także kładzie nacisk na zdolność organizacji do szybkiego reagowania, adaptacji i odbudowy po incydencie cybernetycznym. Podejście to integruje elementy zarządzania ryzykiem, planowania ciągłości działania oraz odporności operacyjnej, umożliwiając organizacjom funkcjonowanie nawet w sytuacji wystąpienia cyberataków lub incydentów.

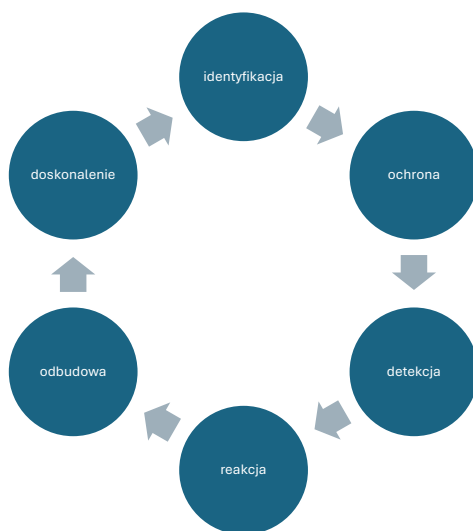
Cyberodporność jest złożonym podejściem, które rozszerza tradycyjne ramy cyberbezpieczeństwa, kładąc szczególny nacisk na zdolność organizacji do przetrwania i szybkiego powrotu do normalnego funkcjonowania po wystąpieniu incydentu cyfrowego. W odróżnieniu od klasycznych metod ochrony, które koncentrują się przede wszystkim

⁵¹ Znacznie szersze zestawienia i porównania taksonomii cyberzagrożeń można znaleźć m.in. w artykułach: G. Rabitti, A. Khorrami Chokami, P. Coyle, R.D. Cohen, *A taxonomy of cyber risk taxonomies*, „Risk Analysis” 2024; M. Syafrizal, S.R. Selamat, N.A. Zakaria, *AVOIDITALS: Enhanced*

na prewencji i detekcji zagrożeń, cyberodporność obejmuje pełne spektrum działań związanych z przygotowaniem na ataki, reagowaniem na nie oraz odbudową zdolności operacyjnych po ich wystąpieniu.

Główne założenie cyberodporności polega na akceptacji faktu, że nie wszystkich incydentów można uniknąć, a całkowite wyeliminowanie ryzyka jest niemożliwe. Zamiast tego cyberodporność zakłada, że organizacja będzie w stanie funkcjonować pomimo ataków lub zakłóceń, minimalizując ich negatywne skutki i przywracając kluczowe procesy w możliwie najkrótszym czasie. Według standardów NIST cyberodporność obejmuje nie tylko ochronę danych, ale też utrzymanie operacyjności systemów i zapewnienie ciągłości działania w warunkach zagrożeń oraz po wystąpieniu incydentu bezpieczeństwa⁵².

Cyberodporność składa się z kilku kluczowych elementów, które wspólnie tworzą zintegrowane podejście do zarządzania ryzykiem i incydentami⁵³, co przedstawiono na rysunku 1.



Rysunek 1. Filary cyberodporności

Źródło: opracowanie własne na podstawie: D. Eisenberg, K. Plourde, T. Seager, J. Allen, A. Kott, *Resilience metrics for cyber systems*, „Environment Systems and Decisions” 2013, no. 33.

⁵² R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, R. McQuaid, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, National Institute of Standards and Technology 2021.

⁵³ E. Vogel, Elisabeth, Z. Dyka, D. Klann, P. Langendörfer, *Resilience in the Cyberworld: Definitions, Features and Models*, „Future Internet” 2021, no. 13(11), s. 293.

Identyfikacja – pierwszym elementem jest dokładna identyfikacja zasobów krytycznych oraz potencjalnych zagrożeń. Obejmuje ona mapowanie systemów informatycznych, procesów biznesowych i zasobów ludzkich, które mogą być narażone na cyberataki. Dzięki temu organizacja może lepiej poznać swoje słabe punkty i określić priorytety w zakresie ochrony.

Ochrona (zapobieganie) – w ramach tego etapu wdrażane są środki mające na celu minimalizację ryzyka wystąpienia incydentu. Należą do nich m.in. zabezpieczenia techniczne (np. zapory sieciowe, systemy detekcji intruzów), polityki bezpieczeństwa, szkolenia pracowników oraz procedury ochrony danych.

Detekcja – kluczowym aspektem cyberodporności jest zdolność do szybkiego wykrywania nieautoryzowanych działań lub anomalii w systemach. Systemy monitorowania i analizy danych pozwalają na wczesne zidentyfikowanie potencjalnych zagrożeń oraz odpowiednie reagowanie w czasie rzeczywistym.

Reakcja – elementem cyberodporności jest też zdolność do skutecznego reagowania na zaistniałe incydenty. Organizacja powinna posiadać przygotowane plany reagowania na incydenty (ang. *incident response plans*), które określają, jakie kroki należy podjąć w razie ataku, aby ograniczyć jego skutki oraz zapobiec dalszemu rozprzestrzenianiu się zagrożenia.

Odbudowa i przywracanie – cyberodporność obejmuje także planowanie działań naprawczych i odbudowę systemów po incydencie. W tej fazie organizacja dąży do jak najszybszego przywrócenia normalnej operacyjności, odtwarzania utraconych danych oraz eliminacji luk w zabezpieczeniach, które mogły się przyczynić do ataku.

Ciągłe doskonalenie – procesy związane z cyberodpornością muszą być dynamiczne i elastyczne. Oznacza to, że organizacje muszą nieustannie analizować incydenty, aktualizować swoje strategie i procedury oraz adaptować się do nowych zagrożeń i technologii. Regularne testy, audyty bezpieczeństwa oraz analiza ryzyka są nieodzowne dla zapewnienia skuteczności całego systemu cyberodporności.

Szybki rozwój czynników ryzyka powoduje, że współczesne podejście do ochrony zasobów cyfrowych musi wykraczać poza klasyczne ramy cyberbezpieczeństwa, które tradycyjnie skupiały się na zapobieganiu i wykrywaniu zagrożeń. W obliczu coraz bardziej złożonych i dynamicznych ataków organizacje muszą przyjąć szerszą perspektywę, w której podejmowane działania obejmują nie tylko przeciwdziałanie incydentom, lecz również skuteczne reagowanie na nie i szybki powrót do stabilnego funkcjonowania. Wymaga to wieloaspektowego podejścia obejmującego zarówno warstwę techniczną, jak i organizacyjną.

Cyberodporność stanowi kompleksową strategię zarządzania zagrożeniami cyfrowymi, integrującą elementy klasycznego cyberbezpieczeństwa z zarządzaniem ciągłością działania, odpornością operacyjną i adaptacją do zmieniających się warunków. Jej celem nie jest całkowite wyeliminowanie ryzyka, lecz budowa zdolności do przetrwania ataku i kontynuacji krytycznych procesów nawet w warunkach zakłóceń. Cyberodporność

wskazywana jest jako kluczowy element strategii bezpieczeństwa informacji, umożliwiający organizacjom skuteczne funkcjonowanie w obliczu nieuchronnych zagrożeń i dynamicznie zmieniającego się krajobrazu cyberzagrożeń.

Państwa, przedsiębiorstwa i instytucje publiczne w obliczu niestabilnego środowiska geopolitycznego, rosnącej liczby zagrożeń i postępującej cyfryzacji muszą traktować cyberodporność jako strategiczny priorytet, równoważny z zapewnieniem cyberbezpieczeństwa rozumianego jako ochrona systemów i danych.

ROZDZIAŁ 2

Ramy regulacyjne i strategie cyberbezpieczeństwa – Polska na tle Unii Europejskiej

Współczesne społeczeństwo informacyjne jest w coraz większym stopniu uzależnione od technologii cyfrowych, co sprawia, że cyberbezpieczeństwo i cyberodporność stanowią kluczowe wyzwania dla państw i organizacji międzynarodowych. Dynamiczny rozwój technologii informacyjno-komunikacyjnych (ICT) sprawił, że państwa oraz organizacje ponadnarodowe muszą nieustannie dostosowywać swoje strategie i regulacje do zmieniającego się środowiska zagrożeń. W tym kontekście Unia Europejska oraz jej państwa członkowskie, w tym Polska, opracowują i implementują kompleksowe ramy regulacyjne oraz strategie mające na celu zapewnienie cyberbezpieczeństwa i cyberodporność, czyli zdolności do skutecznego reagowania i odbudowy po incydentach cybernetycznych. Odpowiednie wdrażanie tych przepisów jest kluczowe dla zapewnienia bezpieczeństwa cyfrowego na poziomie krajowym i międzynarodowym.

W krajach członkowskich Unii Europejskiej ramy regulacyjne w zakresie cyberbezpieczeństwa są kształtowane zarówno przez prawo krajowe, jak i przez unijne regulacje, które obejmują aspekty prawne, organizacyjne i techniczne w takich obszarach, jak:

- a) ochrona infrastruktury krytycznej – regulacje dotyczące zabezpieczenia sektorów uznanych za kluczowe dla funkcjonowania państwa i gospodarki (energetyka, transport, opieka zdrowotna, dostawy i zaopatrzenie w wodę i żywność, usługi finansowe, usługi cyfrowe i telekomunikacyjne);
- b) ochrona danych osobowych i prywatności – przepisy dotyczące ochrony danych osobowych określają obowiązki administratorów danych oraz podmiotów przetwarzających informacje cyfrowe;
- c) zarządzanie incydentami cyberbezpieczeństwa – wymagania dotyczące raportowania incydentów i naruszeń bezpieczeństwa przez podmioty zobowiązane, w tym operatorów usług kluczowych i dostawców usług cyfrowych;

- d) bezpieczeństwo produktów i usług cyfrowych – przepisy wprowadzające mechanizmy certyfikacji bezpieczeństwa produktów ICT (np. urządzeń IoT, oprogramowania, chmur obliczeniowych) oraz standardy dotyczące bezpieczeństwa łańcucha dostaw, w tym dla firm dostarczających technologie i usługi cyfrowe;
- e) bezpieczeństwo usług cyfrowych i telekomunikacyjnych – przepisy obejmujące ochronę infrastruktury telekomunikacyjnej i świadczenia usług elektronicznych oraz środki bezpieczeństwa dla dostawców chmury obliczeniowej, rejestratorów domen internetowych, platform internetowych i mediów społecznościowych;
- f) zwalczanie cyberprzestępczości – przepisy dotyczące przeciwdziałania przestępstwom z użyciem kryptowalut, praniu pieniędzy w sieci oraz ścigania sprawców ataków hakerskich, oszustw internetowych i wyłudzeń;
- g) bezpieczeństwo sztucznej inteligencji i nowych technologii – regulacje dotyczące odpowiedzialnego stosowania systemów sztucznej inteligencji, w tym ich zabezpieczenia przed manipulacjami i cyberatakami, oraz wymogi dotyczące cyberbezpieczeństwa w zakresie automatyzacji procesów oraz systemów autonomicznych;
- h) bezpieczeństwo obronne i militarne – strategiczne podejście do ochrony przed cyberatakami wymierzonymi w instytucje rządowe, systemy wojskowe i infrastrukturę krytyczną oraz współpraca międzynarodowa w ramach NATO i inicjatyw unijnych, np. Cyber Defence Policy Framework;
- i) edukacja i podnoszenie świadomości w zakresie cyberbezpieczeństwa – regulacje nakładające na podmioty obowiązek szkolenia pracowników w zakresie cyberhigieny oraz dotyczące programów wsparcia i finansowania inicjatyw na poziomie krajowym i europejskim (np. Digital Europe Programme).

Celem tych aktów prawnych jest ustanowienie jednolitych zasad w zakresie ochrony sieci i systemów informatycznych, a także zwiększenie odporności kluczowych sektorów gospodarki na cyberzagrożenia. Wdrażanie unijnych regulacji wymaga od Polski opracowania krajowych strategii i planów działania, które nie tylko spełniają wymogi prawne, ale także uwzględniają specyfikę krajowej infrastruktury cyfrowej i zagrożeń wynikających z lokalnego oraz globalnego kontekstu bezpieczeństwa.

Równocześnie na poziomie unijnym tworzone są instytucje i mechanizmy współpracy mające na celu harmonizację polityk cyberbezpieczeństwa oraz zwiększenie zdolności państw członkowskich do reagowania na incydenty cybernetyczne. Przykładem takiej inicjatywy jest ENISA, której zadaniem jest wspieranie państw Unii Europejskiej w budowie odporności na cyberzagrożenia oraz koordynacja działań w zakresie wymiany informacji i najlepszych praktyk.

2.1. Regulacje na poziomie Unii Europejskiej

Pierwszym aktem prawnym na poziomie Unii Europejskiej, który w sposób kompleksowy obejmował kwestie dotyczące cyberbezpieczeństwa, była przyjęta w 2016 roku **dyrektywa NIS** – dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (ang. Network and Information Security Directive – NIS Directive)¹.

Uchwalenie dyrektywy NIS jest uznawane za kamień milowy w działaniach zmierzających w kierunku ujednolicenia podejścia do bezpieczeństwa sieci na poziomie międzynarodowym. Jej geneza wynikała z kilku kluczowych czynników, w tym szczególnie z:

- a) dynamicznego rozwoju technologii i usług cyfrowych, który spowodował wzrost liczby i skali cyberzagrożeń, co w efekcie wymagało skoordynowanej odpowiedzi na poziomie Unii Europejskiej;
- b) potrzeby ujednolicenia systemu bezpieczeństwa w ramach Unii Europejskiej – przed wprowadzeniem dyrektywy NIS istniały znaczące różnice w podejściu do cyberbezpieczeństwa między państwami członkowskimi Unii, co tworzyło luki w ochronie na poziomie całej Unii;
- c) konieczności lepszej ochrony kluczowych sektorów gospodarki i społeczeństwa, takich jak energetyka, transport, bankowość czy opieka zdrowotna;
- d) wzmocnienia współpracy międzynarodowej w zakresie zwalczania cyberprzestępczości²;
- e) realizacji strategii cyberbezpieczeństwa Unii Europejskiej – dyrektywa NIS była elementem szerszej strategii Unii „Otwarta, bezpieczna i chroniona cyberprzestrzeń” z 2013 roku, która określała priorytety w zakresie cyberbezpieczeństwa³.

Treść dyrektywy NIS koncentrowała się na trzech filarach: instytucjach, które powinny powstać we wszystkich państwach członkowskich, współpracy na poziomie europejskim oraz zobowiązaniach w zakresie bezpieczeństwa sieci i informacji, a jej celem było podniesienie poziomu ochrony krajowych systemów cyberbezpieczeństwa w oparciu o zestaw wymagań dla operatorów oraz dostawców usług cyfrowych. Szczególne wymagania nałożono na dwie grupy podmiotów, które w dyrektywie zostały określone jako

¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, 194 OJ L § (2016). <http://data.europa.eu/eli/dir/2016/1148/oj/pol>.

² M. Górka, *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, „Przegląd Geopolityczny” 2018, nr 25, s. 86–103.

³ Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, 2013, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52013JC0001> (3.02.2025).

operatorzy usług kluczowych (ang. *Operators of Essential Services* – OES) oraz dostawcy usług cyfrowych (ang. *Digital Service Providers* – DSP).

Państwa członkowskie zostały zobligowane do wskazania operatorów usług kluczowych, czyli podmiotów, których systemy mają kluczowe znaczenie dla gospodarki i społeczeństwa. Do sektorów objętych tym obowiązkiem zaliczono m.in. energetykę, transport, rynki finansowe, opiekę zdrowotną, dostawy wody oraz infrastrukturę cyfrową. Operatorzy usług kluczowych zostali zobowiązani do stosowania odpowiednich środków bezpieczeństwa w celu zabezpieczenia swoich systemów informatycznych przed cyberzagrożeniami, wdrożenia systemów zarządzania ryzykiem i incydentami, współpracy z krajowymi organami ds. cyberbezpieczeństwa, przeprowadzania regularnych audytów i kontroli zgodności, opracowania procedur pozwalających na utrzymanie działalności w przypadku incydentu cybernetycznego, prowadzenia regularnych szkoleń dla personelu w zakresie cyberbezpieczeństwa i reagowania na incydenty oraz raportowania incydentów związanych z cyberbezpieczeństwem do właściwych organów nadzorczych.

Do kategorii dostawców usług cyfrowych zaliczono podmioty świadczące kluczowe usługi cyfrowe, które mają znaczenie dla gospodarki i bezpieczeństwa Unii Europejskiej. Wśród nich znajdują się:

- internetowe platformy handlowe (np. marketplace'y *e-commerce*),
- wyszukiwarki internetowe,
- usługi przetwarzania w chmurze.

W przeciwieństwie do operatorów usług kluczowych, dostawcy usług cyfrowych zostali objęci łagodniejszymi regulacjami w zakresie cyberbezpieczeństwa. Obowiązki nałożone na nich dotyczyły m.in. zarządzania ryzykiem, raportowania incydentów, utrzymania ciągłości działania i współpracy z organami nadzorczymi.

Poza nałożeniem szeregu obowiązków na dostawców usług, których uznano za istotnych z gospodarczego i społecznego punktu widzenia, dyrektywa NIS zawierała szereg regulacji, których celem było wzmocnienie zdolności państw członkowskich do przeciwdziałania zagrożeniom cyfrowym. Obejmowały one m.in.:

1. Obowiązek wdrożenia krajowych strategii cyberbezpieczeństwa – państwa członkowskie zostały zobowiązane do opracowania i przyjęcia krajowych strategii cyberbezpieczeństwa określających środki ochrony przed cyberzagrożeniami oraz mechanizmy reagowania na incydenty. Strategie miały obejmować zasady współpracy między sektorem publicznym i prywatnym oraz priorytety dotyczące zarządzania ryzykiem.
2. Tworzenie krajowych organów odpowiedzialnych za cyberbezpieczeństwo – wszystkie państwa członkowskie zostały zobowiązane do wyznaczenia właściwych organów ds. cyberbezpieczeństwa, odpowiedzialnych za wdrożenie i egzekwowanie przepisów dyrektywy.
3. Obowiązek utworzenia zespołów reagowania na incydenty komputerowe – na państwa członkowskie nałożony został obowiązek utworzenia CSIRT-ów na poziomie

krajowym i sektorowym, które miały odpowiadać za monitorowanie i reagowanie na incydenty cybernetyczne. Miały one też współpracować na poziomie unijnym oraz wymieniać informacje o zagrożeniach. Kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju bądź zbudować sieć CSIRT-ów sektorowych, obejmujących sektory rynkowe. Państwa ze słabiej rozwiniętymi zdolnościami w zakresie cyberbezpieczeństwa mogły się zwrócić o pomoc w rozwoju CSIRT do ENISA.

4. Zwiększenie zakresu współpracy między państwami członkowskimi w obszarze cyberbezpieczeństwa, w tym:
 - a) utworzenie Grupy Współpracy ds. Sieci i Systemów Informacyjnych NIS (ang. NIS Cooperation Group) mającej na celu wymianę informacji i dobrych praktyk w zakresie ochrony systemów informatycznych oraz wzmacnianie i budowanie współpracy między państwami członkowskimi na poziomie strategicznym; w jej skład wchodzi przedstawiciele państw członkowskich, Komisji Europejskiej i ENISA;
 - b) powołanie europejskiej sieci CSIRT (ang. *CSIRT network*) oraz stworzenie mechanizmów wymiany informacji pomiędzy CSIRT-ami w celu szybkiego reagowania na incydenty cybernetyczne o charakterze transgranicznym.

Postępująca cyfryzacja i ewolucja cyberzagrożeń spowodowały podjęcie przez Parlament Europejski prac zmierzających do nowelizacji przepisów dyrektywy NIS, których efektem było uchwalenie 14 grudnia 2022 roku dyrektywy zawierającej nowe przepisy dotyczące cyberbezpieczeństwa sieci i systemów informatycznych, określanej jako **dyrektywa NIS2**⁴. Nowe regulacje weszły w życie 16 stycznia 2023 roku, a 17 października 2024 roku wyznaczono jako termin implementacji zapisów dyrektywy do prawa krajów członkowskich.

W porównaniu z poprzednią wersją, dyrektywa NIS2 wprowadziła szereg istotnych zmian, w tym⁵:

1. Rozszerzenie zakresu regulacji do 18 sektorów krytycznych. Oprócz sektorów już objętych dyrektywą NIS, takich jak: energetyka, transport, opieka zdrowotna, finanse, gospodarka wodna i infrastruktura cyfrowa, przepisy te mają zastosowanie do dostawców publicznych usług łączności elektronicznej, większej liczby usług cyfrowych, takich jak platformy społecznościowe, gospodarowanie ściekami i odpadami, wytwarzanie produktów krytycznych, usługi pocztowe i kurierskie, administracja publiczna, zarówno na szczeblu centralnym, jak i regionalnym, oraz przestrzeń kosmiczna.

⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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, OJ L § (2022). <http://data.europa.eu/eli/dir/2022/2555/oj/pol>.

⁵ M. Wrzosek, *Dyrektywa NIS 2 – jakie zmiany w zakresie cyberbezpieczeństwa proponuje Komisja Europejska?*, 2020, <https://cyberpolicy.nask.pl/dyrektywa-nis-2-jakie-zmiany-w-zakresie-cyberbezpieczenstwa-proponuje-komisja-europejska/> (22.02.2025).

2. Wprowadzenie nowego podziału na podmioty kluczowe (ang. *essential entities*) i podmioty ważne (ang. *important entities*), zastępującego wcześniejszy podział na operatorów usług kluczowych i dostawców usług cyfrowych.
3. Zaostrzenie wymogów bezpieczeństwa dla objętych dyrektywą podmiotów, w tym:
 - a) obowiązek implementacji polityk bezpieczeństwa opartych na wszechstronnej analizie ryzyka;
 - b) wprowadzenie dynamicznej analizy ryzyka uwzględniającej zmiany techniczne, legislacyjne i nowe typy cyberzagrożeń;
 - c) wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z ISO 27001.
4. Bardziej rygorystyczne procedury zgłaszania incydentów, w tym wczesne ostrzeżenie i raportowanie w ustalonych terminach – w przypadku incydentów poważnych⁶ podmiotom wyznaczono maksymalny czas 24 godz. na przesłanie wczesnego ostrzeżenia oraz 72 godz. na zgłoszenie incydentu, a także zobligowano je do przekazywania raportów okresowych (na żądanie) i raportu końcowego z obsługi incydentu (po miesiącu od daty zgłoszenia incydentu lub w ciągu miesiąca od zakończenia obsługi incydentu)⁷.
5. Wprowadzenie surowszych kar finansowych za nieprzestrzeganie przepisów:
 - dla podmiotów kluczowych: co najmniej 10 mln euro lub 2% rocznego obrotu,
 - dla podmiotów ważnych: co najmniej 7 mln euro lub 1,4% rocznego obrotu,
6. Ustanowienie europejskiej sieci zarządzania kryzysowego w cyberprzestrzeni dla poprawy współpracy międzynarodowej.
7. Nałożenie na kierownictwo firm odpowiedzialności za zgodność ze środkami zarządzania ryzykiem w cyberbezpieczeństwie:
 - a) organy zarządzające podmiotów objętych dyrektywą są bezpośrednio odpowiedzialne za nadzór nad wdrażaniem środków zarządzania ryzykiem w cyberbezpieczeństwie;
 - b) wymagane jest, aby członkowie zarządu przechodzili regularne szkolenia z zakresu cyberbezpieczeństwa;
 - c) kierownictwo może ponosić osobistą odpowiedzialność za naruszenia przepisów dyrektywy.

⁶ Zgodnie z art. 23 pkt 3 dyrektywy NIS2 incydent uznaje się za poważny, jeżeli: 1) spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu; 2) wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.

⁷ A. Wachowska, K. Basaj, *Dyrektywa NIS 2 – obowiązki w zakresie zgłaszania incydentów*, 2024, <https://www.traple.pl/dyrektywa-nis-2-obowiazki-w-zakresie-zglaszania-incydentow/> (11.03.2025).

8. Objęcie regulacjami również małych i średnich przedsiębiorstw spełniających określone kryteria:
 - a) dyrektywa NIS2 rozszerza zakres na MŚP, które spełniają określone kryteria „kluczowości” dla gospodarki lub społeczeństwa;
 - b) wprowadza proporcjonalne wymagania dla MŚP, uwzględniając ich ograniczone zasoby;
 - c) państwa członkowskie mają zapewnić wsparcie i wytyczne dla MŚP w zakresie wdrażania wymogów cyberbezpieczeństwa.

Wprowadzenie minimalnych wymogów bezpieczeństwa dla wszystkich podmiotów objętych dyrektywą NIS2 ustanawia podstawowy zestaw środków bezpieczeństwa, które muszą być wdrożone przez wszystkie podmioty objęte dyrektywą. Obejmują one m.in.: polityki bezpieczeństwa danych, zarządzanie incydentami, ciągłość działania, bezpieczeństwo łańcucha dostaw, szyfrowanie i uwierzytelnianie wieloskładnikowe.

Zapisy dyrektywy nałożyły też na państwa członkowskie obowiązki dotyczące rozwoju krajowych strategii cyberbezpieczeństwa. Państwa członkowskie są zobowiązane do rozwijania własnych krajowych strategii i polityk w zakresie cyberbezpieczeństwa, które powinny być regularnie aktualizowane i dostosowywane do zmieniającego się krajobrazu zagrożeń. Dyrektywa promuje inwestycje w budowanie kompetencji i świadomości w zakresie cyberbezpieczeństwa, w tym poprzez szkolenia i kampanie edukacyjne skierowane zarówno do podmiotów publicznych, jak i prywatnych.

Kolejnym aktem prawnym, który obok dyrektywy NIS2 tworzy fundamenty europejskiego systemu cyberbezpieczeństwa, jest rozporządzenie Parlamentu Europejskiego i Rady z roku 2019, które określane jest jako **Akt o cyberbezpieczeństwie** (ang. Cybersecurity Act – CA)⁸. Został on opublikowany 7 czerwca 2019 roku jako część tzw. pakietu cyberbezpieczeństwa⁹ mającego na celu zwiększenia poziomu cyberbezpieczeństwa, cyberodporności i zaufania w Unii Europejskiej. Była to druga, po dyrektywie NIS, ogólnoeuropejska regulacja w dziedzinie cyberbezpieczeństwa. Jest podzielona na dwie części. Pierwsza z nich dotyczy działalności ENISA. Została ona powołana już w 2004 roku na mocy wcześniejszego rozporządzenia Parlamentu Europejskiego i Rady z roku

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, 151 OJ L § (2019). <http://data.europa.eu/eli/reg/2019/881/oj/pol>.

⁹ Unijny pakiet o cyberbezpieczeństwie to kompleksowy zestaw regulacji i strategii mających na celu wzmocnienie ochrony cyfrowej w państwach członkowskich Unii Europejskiej. Obejmuje on różne inicjatywy, które wspólnie tworzą spójne ramy prawne i operacyjne w zakresie cyberbezpieczeństwa. Pakiet o cyberbezpieczeństwie został opublikowany 16 grudnia 2020 r. przez Komisję Europejską. <https://cyberpolicy.nask.pl/aktualnosci/nowy-pakiet-cyberbezpieczenstwa-dla-ue/> (12.01.2025).

2004¹⁰, które stanowiło podstawę prawną dla funkcjonowania ENISA i określało jej cele i zadania. Rozwój zagrożeń w obszarze bezpieczeństwa informatycznego spowodował konieczność zwiększenia kompetencji ENISA, uszczegółowienia zakresu działania agencji, rozszerzenia obowiązków na nowe obszary, a także wzmocnienia jej roli poprzez nadanie jej stałego mandatu i zwiększenie zasobów. Do najważniejszych zadań agencji należy koordynacja działań w zakresie cyberbezpieczeństwa na poziomie europejskim, opracowywanie i promowanie najlepszych praktyk w dziedzinie cyberbezpieczeństwa, a także udzielanie wsparcia technicznego i doradczego państwom członkowskim Unii Europejskiej w zakresie ochrony przed cyberzagrożeniami.

Agencja swoimi działaniami wspiera proces tworzenia skutecznych rozwiązań z sferze cyberbezpieczeństwa państw członkowskich Unii Europejskiej i innych organów unijnych¹¹. Druga część CA tworzy ramy certyfikacji cyberbezpieczeństwa dla produktów i usług z obszaru technologii informacyjno-komunikacyjnych, takich jak np. urządzenia IoT, oprogramowanie, rozwiązania oparte na chmurze obliczeniowej. Rozporządzenie określa mechanizm tworzenia europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniają określone wymogi bezpieczeństwa. Celem jest zapewnienie, że na rynek trafiają urządzenia i rozwiązania, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa. Dzięki systemowi uznawania certyfikatów firmy nie muszą się ubiegać o certyfikat w każdym kraju, w którym chciałyby oferować swoje usługi bądź produkty.

W ramach prac związanych z wprowadzaniem w życie pakietu o cyberbezpieczeństwie w grudniu 2024 roku zostało opublikowane rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty, znane jako **Akt o cybersolidarności**¹². Weszło ono w życie 4 lutego 2025 roku, a jego celem było wzmocnienie zdolności Unii Europejskiej w zakresie wykrywania, przygotowania i reagowania na cyberzagrożenia oraz incydenty na dużą skalę. Akt o cybersolidarności stanowi odpowiedź na rosnące zagrożenia w cyberprzestrzeni, które mogą mieć poważne konsekwencje dla funkcjonowania społeczeństw i gospodarek państw członkowskich.

10 Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji Tekst mający znaczenie dla EOG, 01, 005 DD § (2004). <http://data.europa.eu/eli/reg/2004/460/oj/pol>.

11 K. Gawkowski, *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka Komisji Politologii i Stosunków Międzynarodowych” 2018, nr 2.

12 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (2024). <http://data.europa.eu/eli/reg/2025/38/oj/pol>.

Głównym celem rozporządzenia jest ustanowienie ram prawnych umożliwiających skoordynowane działania na poziomie Unii w zakresie:

- a) wczesnego wykrywania cyberzagrożeń – poprzez rozwój i integrację systemów monitorowania oraz wymiany informacji między państwami członkowskimi;
- b) zwiększenia gotowości na incydenty – poprzez wspieranie krajowych struktur odpowiedzialnych za cyberbezpieczeństwo oraz promowanie najlepszych praktyk;
- c) reagowania na incydenty na dużą skalę – poprzez ustanowienie mechanizmów solidarnościowych, które umożliwiają szybkie i skoordynowane działania w przypadku poważnych incydentów cybernetycznych.

Najważniejsze zapisy, jakie znalazły się w rozporządzeniu, objęły:

- d) utworzenie Europejskiej Rezerwy Cyberbezpieczeństwa – rozporządzenie przewiduje stworzenie rezerwy ekspertów i zasobów technicznych, które mogą być mobilizowane w przypadku poważnych incydentów cybernetycznych;
- e) wzmocnienie roli ENISA – agencja otrzymała rozszerzone kompetencje w zakresie koordynacji działań na poziomie Unii oraz wsparcia państw członkowskich w budowaniu zdolności w zakresie cyberbezpieczeństwa;
- f) mechanizmy finansowe – rozporządzenie wprowadza instrumenty finansowe wspierające państwa członkowskie w inwestycjach w infrastrukturę cyberbezpieczeństwa oraz w szkolenia dla specjalistów;
- g) współpracę publiczno-prywatną – zachęty do tworzenia partnerstw między sektorem publicznym a prywatnym w celu wymiany informacji o zagrożeniach oraz wspólnego reagowania na incydenty;
- h) zharmonizowane podejście do certyfikacji tzw. usług zarządzanych w zakresie bezpieczeństwa – rozporządzenie wprowadza ramy dla europejskich programów certyfikacji cyberbezpieczeństwa, które obejmują również usługi zarządzane w zakresie bezpieczeństwa, takie jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo.

Również w grudniu 2024 roku europejskie ramy regulacyjne dotyczące cyberbezpieczeństwa zostały uzupełnione o szereg przepisów, które wprowadziły obowiązkowe wymogi dotyczące cyberbezpieczeństwa dla produktów zawierających elementy cyfrowe. Zakres tych obowiązków został określony w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, które określono jako **Akt o odporności cyfrowej** (ang. Cyber Resilience Act – CRA)¹³. Jego celem jest podniesienie poziomu

¹³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Tekst mający znaczenie dla EOG) (2024). <http://data.europa.eu/eli/reg/2024/2847/oj/pol>.

cyberbezpieczeństwa produktów dostępnych na rynku Unii Europejskiej oraz zapewnienie, że sprzęt i oprogramowanie są projektowane, opracowywane i utrzymywane z uwzględnieniem wymogów cyberbezpieczeństwa przez cały cykl ich życia.

Regulacje określone w Akcie o odporności cyfrowej nakładają na producentów, importerów i dystrybutorów obowiązki dotyczące:

- a) projektowania i wytwarzania produktów zgodnie z zasadniczymi wymogami cyberbezpieczeństwa;
- b) zapewnienia bezpłatnych aktualizacji zabezpieczeń w okresie wsparcia produktu;
- c) przeprowadzania ocen ryzyka;
- d) powiadamiania ENISA o zidentyfikowanych lukach w produkcie lub usłudze w ciągu 24 godz.

Przepisy rozporządzenia obejmują szeroki zakres produktów cyfrowych, które mają możliwości komunikacyjne – zarówno sprzęt, jak i oprogramowanie, w tym np.:

- a) inteligentne urządzenia domowe (np. termostaty, zamki do drzwi, systemy oświetlenia);
- b) smartfony;
- c) urządzenia do monitorowania zdrowia i kondycji;
- d) przemysłowe urządzenia IoT wykorzystywane w produkcji i logistyce;
- e) zapory sieciowe i systemy wykrywania/zapobiegania włamaniom;
- f) systemy zarządzania tożsamością, w tym czytniki uwierzytelniania i kontroli dostępu;
- g) przeglądarki internetowe;
- h) menedżery haseł;
- i) VPN i systemy zarządzania siecią;
- j) oprogramowanie antywirusowe;
- k) systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM);
- l) infrastrukturę klucza publicznego i oprogramowanie do wydawania certyfikatów cyfrowych.

W obliczu dynamicznego rozwoju technologii cyfrowych, które doprowadziły do masowego przetwarzania informacji o użytkownikach bez ich pełnej kontroli, a także wzrostu liczby cyberataków, wycieków danych oraz zagrożenia ze strony inwazyjnych technologii śledzenia i profilowania, konieczne stało się wprowadzenie w krajach Unii Europejskiej regulacji, które zapewnią większą przejrzystość w przetwarzaniu danych (w tym szczególnie danych osobowych). Miały one pozwolić użytkownikom na uzyskanie realnej kontroli nad gromadzonymi na ich temat informacjami oraz nakreślić jednolite ramy prawne, które skutecznie ochronią prywatność w cyfrowym świecie.

W ramach podjętych w tym zakresie działań Parlament Europejski i Rada Unii Europejskiej 27 kwietnia 2016 roku wydały **Ogólne Rozporządzenie o Ochronie Danych**

(ang. General Data Protection Regulation – GDPR)¹⁴, które zastąpiło pochodzącą z 1995 roku dyrektywę w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych¹⁵. Przepisy GDPR weszły w życie 25 maja 2018 roku, unifikując i zastępując 28 dotychczasowych regulacji obowiązujących w poszczególnych państwach członkowskich.

Wprowadzenie GDPR stało się konieczne, ponieważ rozwój technologii cyfrowych (w tym pliki *cookie*, algorytmy śledzące i profilujące, *Big Data* itp.) spowodował, że wcześniejsze przepisy, oparte na dyrektywie 95/46/WE, zdeaktualizowały się, co w konsekwencji doprowadziło do różnic w interpretacji i stosowaniu zasad ochrony danych w poszczególnych krajach członkowskich.

GDPR uregulowało szereg kluczowych obszarów związanych z ochroną danych osobowych, w tym:

- a) zasady przetwarzania danych osobowych – określono podstawowe zasady, takie jak legalność, rzetelność, przejrzystość, minimalizacja danych, ograniczenie celu, integralność i poufność;
- b) podstawy prawne przetwarzania danych – ustalono sześć głównych podstaw legalnego przetwarzania danych, w tym zgodę użytkownika, wykonanie umowy, obowiązek prawny, ochronę żywotnych interesów, zadania realizowane w interesie publicznym i uzasadniony interes administratora;
- c) prawa osób, których dane dotyczą – wprowadzono nowe prawa dla obywateli Unii Europejskiej, w tym prawo dostępu do danych, prawo do sprostowania, prawo do usunięcia danych („prawo do bycia zapomnianym”), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych i prawo sprzeciwu wobec przetwarzania;
- d) obowiązki administratorów i podmiotów przetwarzających – administratorzy danych muszą wdrażać środki techniczne i organizacyjne zapewniające zgodność z GDPR, w tym prowadzić rejestr czynności przetwarzania, przeprowadzać ocenę skutków dla ochrony danych (proces mający na celu identyfikację ryzyka wynikającego z przetwarzania danych osobowych oraz minimalizację tego ryzyka w możliwie największym zakresie i na jak najwcześniejszym etapie) i stosować zasady *privacy by design* i *privacy by default*¹⁶;

¹⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Tekst mający znaczenie dla EOG), 119 OJ L § (2016). <http://data.europa.eu/eli/reg/2016/679/oj/pol>.

¹⁵ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, 13, 015 DD § (1995). <http://data.europa.eu/eli/dir/1995/46/oj/pol>.

¹⁶ Zasada *privacy by design* oznacza uwzględnienie zagadnień dotyczących ochrony danych już w fazie projektowania systemów, produktów lub usług, np. poprzez wdrożenie odpowiednich środków technicznych

- e) obowiązek zgłaszania naruszeń danych – wprowadzono wymóg zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu w ciągu 72 godz., a w niektórych przypadkach także poinformowania osób, których dane dotyczą;
- f) wyznaczenie Inspektora Ochrony Danych (IOD) – w niektórych przypadkach (np. przetwarzanie na dużą skalę, instytucje publiczne) organizacje muszą wyznaczyć Inspektora Ochrony Danych odpowiedzialnego za nadzorowanie zgodności z GDPR;
- g) zasady przekazywania danych poza Unię Europejską – wprowadzono rygorystyczne wymagania dotyczące przekazywania danych osobowych do krajów spoza Unii, wymagając odpowiedniego poziomu ochrony, np. poprzez standardowe klauzule umowne, mechanizmy certyfikacji czy decyzje Komisji Europejskiej o adekwatności ochrony;
- h) kary i sankcje – GDPR przewiduje surowe kary finansowe za nieprzestrzeganie przepisów – do 20 mln euro lub 4% rocznego globalnego obrotu przedsiębiorstwa, w zależności od tego, która kwota jest wyższa.

Przepisy GDPR muszą być stosowane przez wszystkie podmioty prowadzące swoją działalność na terenie Unii Europejskiej, niezależnie od kraju pochodzenia i miejsca, gdzie mają swoją siedzibę. Obok GDPR ważnym dokumentem, który określa ramy dotyczące przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, jest również **dyrektywa o prywatności i łączności elektronicznej** z 2002 roku (ang. ePrivacy Directive)¹⁷. Jej przepisy koncentrują się na prywatności w komunikacji elektronicznej (nawet jeśli dotyczy ona danych nieosobowych), w tym na takich kwestiach, jak marketing e-mailowy, pliki *cookie*, spam i poufność komunikacji, podczas gdy GDPR ma szerszy zakres i dotyczy ogólnej ochrony danych osobowych we wszystkich sektorach gospodarki.

Dyrektywa o prywatności i GDPR są ze sobą ściśle powiązane i wzajemnie się uzupełniają. W roku 2017 na wniosek Komisji Europejskiej zostały podjęte prace zmierzające do dostosowania regulacji zapisanych w dyrektywie o prywatności poprzez zastąpienie jej nowym aktem prawnym w postaci rozporządzenia (ang. ePrivacy Regulation). Prace w tym zakresie podjęto z kilku kluczowych powodów:

- a) dostosowanie do nowych technologii – obecna dyrektywa nie uwzględnia w pełni nowych technologii i usług cyfrowych, które pojawiły się od czasu jej uchwalenia w 2002 roku;

i organizacyjnych, takich jak pseudonimizacja. Zasada *privacy by default* opiera się na zapewnieniu, że domyślnie przetwarzane są wyłącznie dane niezbędne dla osiągnięcia konkretnego celu przetwarzania oraz ograniczenia ilości zbieranych danych, zakresu ich przetwarzania, okresu przechowywania i ich dostępności.

¹⁷ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), 13, 029 DD § (2002). <http://data.europa.eu/eli/dir/2002/58/oj/pol>.

- b) harmonizacja przepisów – rozporządzenie, w przeciwieństwie do dyrektywy, będzie bezpośrednio stosowane we wszystkich państwach członkowskich Unii Europejskiej, co zapewni jednolite podejście do ochrony prywatności w komunikacji elektronicznej;
- c) uzupełnienie GDPR – ePrivacy Regulation zawiera przepisy bardziej szczegółowe (ma działać jako *lex specialis*) w stosunku do GDPR, zapewniając dodatkowe gwarancje dla poufności i ochrony komunikacji elektronicznej;
- d) rozszerzenie zakresu – nowe rozporządzenie ma objąć szerszy zakres usług komunikacji elektronicznej, w tym np. komunikatory internetowe i usługi *over-the-top* (OTT), które polegają na oferowaniu usług multimedialnych przez operatorów, którzy jednak nie ingerują w nie i nie kontrolują przesyłanych treści.

Pierwotnie rozporządzenie miało wejść w życie razem z GDPR w 2018 roku, jednak proces legislacyjny okazał się bardziej skomplikowany, niż początkowo zakładano, co wynikało ze skomplikowanej natury regulowanych kwestii oraz konieczności uwzględnienia interesów różnych stron, a w części także opóźnień wywołanych pandemią COVID-19. Obecnie (kwiecień 2025 roku) prace nad rozporządzeniem nadal trwają, a ostateczna data jego przyjęcia i wejścia w życie nie jest jeszcze znana.

Z uwagi na fakt, że sektor finansowy jest coraz bardziej zależny od technologii i rozwiązań cyfrowych, a tym samym narażony na cyberataki, w listopadzie 2022 roku Parlament Europejski przyjął **rozporządzenie o operacyjnej odporności cyfrowej** (ang. The Digital Operational Resilience Act – DORA)¹⁸. Jego główne cele to:

1. Zwiększenie odporności operacyjnej sektora finansowego na cyberataki i zakłócenia technologiczne – na instytucje finansowe nałożono obowiązek wdrożenia zaawansowanych systemów zarządzania ryzykiem ICT, które pozwolą na szybkie wykrywanie, reagowanie i odzyskiwanie sprawności po incydentach cybernetycznych.
2. Harmonizacja praktyk w zakresie cyberbezpieczeństwa w całej Unii Europejskiej – przepisy rozporządzenia wprowadzają jednolite standardy i wymagania dla wszystkich instytucji finansowych działających na terenie Unii, co ma zapewnić spójne podejście do bezpieczeństwa cyfrowego.
3. Wzmocnienie nadzoru nad dostawcami usług ICT dla sektora finansowego – rozporządzenie znacząco rozszerza zakres obowiązków firm technologicznych obsługujących instytucje finansowe, uznając ich kluczową rolę w zapewnieniu ciągłości działania sektora.

¹⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, 333 OJ L § (2022). <http://data.europa.eu/eli/reg/2022/2554/oj/pol>.

4. Poprawa transparentności i raportowania incydentów związanych z ICT – DORA wprowadza rygorystyczne wymogi dotyczące zgłaszania poważnych incydentów cybernetycznych, co ma umożliwić szybszą reakcję na poziomie całego sektora.
5. Promowanie kultury cyberbezpieczeństwa w instytucjach finansowych – treść rozporządzenia kładzie nacisk na regularne szkolenia pracowników, testy odporności systemów oraz ciągle doskonalenie procesów związanych z bezpieczeństwem cyfrowym.

Nowe przepisy, których pełna implementacja do krajowych systemów prawnych nastąpiła 17 stycznia 2025 roku, dotyczą wszystkich firm świadczących usługi finansowe, w tym banków, dostawców usług płatniczych, instytucji pieniądza elektronicznego, firm inwestycyjnych, dostawców usług związanych z kryptowalutami, zakładów ubezpieczeń i zakładów reasekuracji, biegłych rewidentów i firm audytorskich, a także krytycznych zewnętrznych dostawców usług teleinformatycznych dla sektora finansowego. Najważniejsze zapisy DORA obejmują¹⁹:

- a) wymóg ustanowienia kompleksowych ram zarządzania ryzykiem ICT;
- b) obowiązek identyfikacji i wykrywania zagrożeń, ochrony zasobów, reagowania i odzyskiwania danych po incydentach;
- c) wprowadzenie ujednoliconych zasad zgłaszania poważnych incydentów związanych z ICT do właściwych organów nadzorczych;
- d) obowiązek regularnego testowania systemów i procesów ICT (co najmniej raz w roku), w tym przeprowadzania testów penetracyjnych czy oceny bezpieczeństwa sieci;
- e) ustanowienie wymogów dotyczących zarządzania ryzykiem związanym z zewnętrznymi dostawcami usług ICT, w tym obowiązek szczegółowej oceny ryzyka przed nawiązaniem współpracy z zewnętrznym dostawcą usług ICT oraz obowiązek monitorowania i okresowej weryfikacji ryzyka związanego z zewnętrznymi dostawcami;
- f) wprowadzenie bezpośredniego nadzoru nad krytycznymi zewnętrznymi dostawcami usług ICT dla sektora finansowego – ustanowienie Wspólnego Organu Nadzorczego złożonego z przedstawicieli europejskich organów nadzoru finansowego;
- g) wprowadzenie surowych kar finansowych za nieprzestrzeganie przepisów.

Obserwowany w ostatnich latach gwałtowny rozwój rozwiązań w obszarze sztucznej inteligencji (ang. *artificial intelligence* – AI) stanowi jeden z kluczowych czynników transformacji cyfrowej w Unii Europejskiej, jednak jego dynamiczny postęp niesie ze sobą istotne wyzwania w zakresie cyberbezpieczeństwa. AI może być wykorzystywana zarówno do wzmacniania systemów zabezpieczeń, jak i do prowadzenia działań cyberprzestępczych, takich jak zaawansowane ataki phishingowe, automatyzacja eksploatacji

¹⁹ Jakie zasady wprowadza DORA? – Kompletny przegląd regulacji, <https://nfllo.pl/baza-wiedzy/jakie-zasady-wprowadza-dora-kompletny-przeglad-regulacji/> (10.03.2025).

luk w systemach czy tworzenie nieprawdziwych treści i informacji. W odpowiedzi na te zagrożenia w lipcu 2024 roku opublikowane zostało rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji, czyli tzw. **Akt w sprawie sztucznej inteligencji** (ang. AI Act)²⁰, którego celem jest zapewnienie bezpiecznego i etycznego rozwoju tej technologii przy jednoczesnym zachowaniu równowagi między ochroną praw obywateli a wspieraniem innowacji w dziedzinie sztucznej inteligencji. AI Act dotyczy szerokiego kręgu podmiotów, w tym dostawców, importerów i podmiotów stosujących systemy oparte na sztucznej inteligencji, działających w Europejskim Obszarze Gospodarczym, a także podmiotów, które pochodzą spoza EOG, ale świadczą swoje usługi na tym obszarze. Regulacja ta klasyfikuje systemy AI według poziomu ryzyka (im wyższe ryzyko związane z systemem AI, tym bardziej rygorystyczne wymagania), nakładając na dostawców i użytkowników określone obowiązki w zakresie przejrzystości, monitorowania i zarządzania ryzykiem. W kontekście cyberbezpieczeństwa AI Act wprowadza szczególne wymagania dla systemów o wysokim ryzyku²¹, takich jak te wykorzystywane w infrastrukturach krytycznych, co ma na celu ograniczenie potencjalnych zagrożeń związanych z wykorzystaniem AI w atakach na systemy informatyczne. Szczególne wymagania, jakie muszą spełniać systemy AI klasyfikowane jako systemy wysokiego ryzyka, to m.in.:

- a) AI nie może podejmować decyzji całkowicie autonomicznie, a użytkownik powinien być informowany o jej działaniu;
- b) dane używane przez AI muszą być odpowiednio zabezpieczone przed manipulacją i nieuprawnionym dostępem;
- c) dostawcy systemów AI muszą zapewnić mechanizmy ciągłego monitorowania i raportowania potencjalnych zagrożeń.

Jednocześnie rozporządzenie ustanowiło zakaz stosowania określonych systemów AI (systemy o niedopuszczalnym ryzyku), wśród których znalazły się te:

- a) stosujące techniki podprogowe będące poza świadomością danej osoby, celowe techniki manipulacyjne lub wprowadzające w błąd;

²⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (2024). <http://data.europa.eu/eli/reg/2024/1689/oj/pol>.

²¹ Zgodnie z treścią AI Act systemy AI wysokiego ryzyka to te, które mają znaczący szkodliwy wpływ na zdrowie, bezpieczeństwo i prawa podstawowe jednostek. Obejmą one m.in. systemy używane do rekrutacji czy oceny pracowniczej lub systemy AI przeznaczone do zarządzania krytyczną infrastrukturą cyfrową. Systemami AI wysokiego ryzyka będą także te związane z bezpieczeństwem elementu produktu objętego prawodawstwem harmonizacyjnym (np. zabawki z elementami AI).

- b) wykorzystujące dowolne słabości danej osoby lub określonej grupy osób ze względu na ich wiek, niepełnosprawność, szczególną sytuację społeczną lub ekonomiczną;
- c) służące w odniesieniu do osób fizycznych do oceny ryzyka lub prawdopodobieństwa popełnienia przestępstwa wyłącznie na podstawie profilowania osoby fizycznej lub oceny jej cech osobowości i cech charakterystycznych;
- d) tworzące lub rozbudowujące bazy danych służące rozpoznawaniu twarzy poprzez pozyskiwanie wizerunków twarzy z Internetu lub z telewizji;
- e) wykorzystywane do wyciągania wniosków na temat emocji osoby w miejscu pracy lub instytucjach edukacyjnych;
- f) kategoryzujące osoby fizyczne w oparciu o dane biometryczne, aby wywnioskować informacje na temat ich rasy, poglądów politycznych, przynależności do związków zawodowych, przekonań religijnych lub filozoficznych, życia seksualnego lub orientacji;
- g) wykorzystywane do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw (z wyjątkami określonymi w rozporządzeniu).

Wdrożenie przepisów AI Act zaplanowane zostało w sposób etapowy: w lutym 2025 roku weszły w życie przepisy zakazujące stosowania w całej Unii szczególnie niebezpiecznych systemów AI, w sierpniu 2025 roku w życie wejdą przepisy kluczowe dla nadzoru nad sztuczną inteligencją, dotyczące m.in. określenia organu nadzoru rynku i organu notyfikującego, modeli AI ogólnego przeznaczenia, jak również kar za naruszenia AI Act, natomiast jako ostatnie zaczną obowiązywać przepisy, które odnoszą się do systemów AI wysokiego ryzyka oraz związanych z nimi obowiązków. Ich wejście w życie nastąpi w sierpniu 2026 roku oraz w przypadku niektórych systemów wysokiego ryzyka będących elementem produktów podlegających osobnym normom – w sierpniu 2027 roku.

Należy podkreślić, że przedstawione akty prawne to najważniejsze, ale nie wszystkie regulacje, które tworzą prawne ramy dla działań związanych z podnoszeniem poziomu bezpieczeństwa oraz zapobieganiem i zwalczaniem przestępczości w przestrzeni cyfrowej Unii Europejskiej. Na wspomnienie zasługują również regulacje, których proces implementacji na poziomie europejskim lub krajowym właśnie trwa lub rozpocznie się w bliskiej przyszłości:

1. Dyrektywa w sprawie odporności podmiotów krytycznych (ang. Directive on the Resilience of Critical Entities – CER Directive)²² – ma na celu zwiększenie odporności podmiotów krytycznych na zagrożenia, w tym cyberzagrożenia, w takich sektorach, jak energetyka, transport, zdrowie czy finanse. Zobowiązuje je do przeprowadzania

22 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG). <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/pol>.

ocen ryzyka i wdrażania środków ochronnych zapewniających ciągłość działania w obliczu zagrożeń. Weszła w życie 16 stycznia 2023 roku i miała być transponowana do prawa krajowego do 17 października 2024 roku, jednak wiele krajów członkowskich (w tym Polska) nie dotrzymało tego terminu.

2. Rozporządzenie UE w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania, określane jako Akt w sprawie danych (ang. Data Act)²³ – ma na celu regulację kwestii związanych z dostępem do danych, ich wykorzystaniem oraz podziałem korzyści wynikających z ich przetwarzania. Głównym jego celem jest zapewnienie sprawiedliwego dostępu do danych oraz ich użycia, stymulowanie innowacji i konkurencji, a także poprawa warunków działania na jednolitym rynku cyfrowym. Jego uzupełnieniem jest Akt w sprawie zarządzania danymi²⁴. Oba akty prawne wzajemnie się uzupełniają, przy czym Akt w sprawie zarządzania danymi koncentruje się na ramach prawnych, procesach i strukturach wspierających wymianę danych, a projekt Aktu w sprawie danych kładzie większy nacisk na wyjaśnienie, kto i na jakich warunkach ma prawo korzystać z danych. Akt w sprawie danych wszedł w życie 11 stycznia 2024 roku, a jego przepisy zaczną obowiązywać we wrześniu 2025 roku.

2.2. Regulacje w Polsce

Polska jako członek Unii Europejskiej aktywnie uczestniczy w procesie harmonizacji regulacji i wdrażania wspólnych standardów cyberbezpieczeństwa, podejmując działania na rzecz podnoszenia poziomu bezpieczeństwa sieci i systemów informacyjnych oraz wspierając przedsiębiorstwa i instytucje publiczne we wdrażaniu najlepszych praktyk oraz środków ochrony przed cyberatakami.

System cyberbezpieczeństwa w Polsce opiera się w dużym stopniu na implementacji regulacji unijnych (w tym NIS/NIS2, Aktu o cyberbezpieczeństwie, GDPR czy DORA). Jednocześnie krajowe rozwiązania są dostosowywane do realiów wynikających z krajowego systemu teleinformatycznego oraz struktury organizacyjnej podmiotów odpowiedzialnych za cyberbezpieczeństwo. Najważniejszym aktem prawnym, który określa ramy i zasady funkcjonowania krajowego systemu bezpieczeństwa cyfrowego, jest **ustawa**

²³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Tekst mający znaczenie dla EOG) (2023). <http://data.europa.eu/eli/reg/2023/2854/oj/pol>.

²⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Tekst mający znaczenie dla EOG), 152 OJ L § (2022). <http://data.europa.eu/eli/reg/2022/868/oj/pol>.

o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 roku (UoKSC)²⁵. Określa ona zasady funkcjonowania i organizacji systemu cyberbezpieczeństwa w Polsce, w tym role organów państwowych odpowiedzialnych za zapewnienie bezpieczeństwa w sieciach i systemach informatycznych, i jest pierwszym w Polsce aktem prawnym regulującym kwestie cyberbezpieczeństwa w sposób horyzontalny. Główne obszary, jakie zostały uregulowane w treści UoKSC, to:

1. Zasady organizacji krajowego systemu cyberbezpieczeństwa – ustawa definiuje podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa oraz ich obowiązki. Do kluczowych uczestników systemu należą operatorzy usług kluczowych, dostawcy usług cyfrowych, zespoły CSIRT oraz organy administracji publicznej.
2. Organizacja zespołów CSIRT – na mocy ustawy powołane zostały trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT-ów odpowiedzialny jest za wsparcie w zakresie cyberbezpieczeństwa oraz koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty:
 - a) CSIRT GOV (działa w strukturach Agencji Bezpieczeństwa Wewnętrznego) – wykrywanie zagrożeń i obsługa incydentów dotyczących systemów teleinformatycznych administracji publicznej oraz infrastruktury krytycznej;
 - b) CSIRT MON (działa w strukturach Ministerstwa Obrony Narodowej) – wykrywanie zagrożeń i obsługa incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym;
 - c) CSIRT NASK (działa w strukturach Państwowego Instytutu Badawczego Naukowa i Akademicka Sieć Komputerowa) – wykrywanie zagrożeń i obsługa incydentów zgłaszanych przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny oraz osoby fizyczne.
3. Obowiązki operatorów usług kluczowych – podmioty działające w sektorach strategicznych (energetyka, transport, ochrona zdrowia, infrastruktura finansowa, zaopatrzenie w wodę) muszą wdrażać odpowiednie środki techniczne i organizacyjne zapewniające odporność systemów na cyberzagrożenia. W przypadku incydentów muszą zgłaszać je odpowiednim organom (np. CSIRT GOV, CSIRT MON, CSIRT NASK).
4. Obowiązki dostawców usług cyfrowych – dostawcy usług cyfrowych (w tym m.in. platformy handlu internetowego, usługi przetwarzania w chmurze oraz wyszukiwarki internetowe) muszą stosować adekwatne środki bezpieczeństwa i raportować incydenty.

²⁵ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2022, poz. 1863 ze zm.). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560>.

5. Zarządzanie ryzykiem cyberbezpieczeństwa – operatorzy usług kluczowych muszą regularnie oceniać ryzyko i wdrażać plany postępowania na wypadek incydentów oraz prowadzić audyty i sporządzać raporty o stanie bezpieczeństwa.
6. Postępowanie w przypadku incydentów – podmioty objęte ustawą muszą niezwłocznie zgłaszać poważne incydenty zespołom CSIRT, które podejmują działania mające na celu ograniczenie skutków ataków i koordynację odpowiedzi.
7. Rola organów nadzorczych i regulacyjnych – nadzór nad każdym z kluczowych sektorów gospodarki sprawuje organ właściwy ds. cyberbezpieczeństwa, tj. ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym, np. sektorowym zespołom cyberbezpieczeństwa.
8. Współpraca międzynarodowa i wymiana informacji – określony został zakres i zasady współpracy z unijnymi strukturami w obszarze cyberbezpieczeństwa, takimi jak ENISA i sieć CSIRT-ów na poziomie Unii Europejskiej, oraz mechanizmy wymiany informacji o zagrożeniach.

Ustawa jest implementacją do porządku krajowego dyrektywy NIS. Ponieważ dyrektywa ta określała jedynie zestaw minimalnych wymagań, które mają zostać wprowadzone przez państwa członkowskie (harmonizacja minimalna), zakres podmiotów podlegających UoKSC został rozszerzony o administrację publiczną oraz sektor telekomunikacyjny.

Z uwagi na konieczność wdrożenia do polskiego systemu prawnego regulacji wprowadzonych dyrektywą NIS2 w Polsce trwają obecnie prace nad nowelizacją UoKSC dostosowujące jej treść do nowych wymogów w zakresie cyberbezpieczeństwa. Choć termin implementacji dyrektywy NIS2 upłynął w październiku 2024 roku, to biorąc pod uwagę stan zaawansowania prac nad projektem ustawy oraz czas potrzebny na realizację procesu legislacyjnego, można założyć, że znowelizowana UoKSC zacznie obowiązywać nie wcześniej niż w połowie 2025 roku.

Najważniejsze zmiany, jakie wymusza implementacja dyrektywy NIS2, dotyczą wprowadzenia nowych zadań dla państw członkowskich, rozszerzenia zakresu podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa oraz rozszerzenia kompetencji organów Unii Europejskiej. Przedstawiony w grudniu 2024 roku projekt nowelizacji UoKSC wskazuje, że najważniejsze zmiany, jakie zaplanowano w ustawie w związku z implementacją dyrektywy NIS2 oraz koniecznością dostosowania prawa do zmian zachodzących w obszarze zagrożeń cyfrowych, to²⁶:

1. Zmiana i rozszerzenie zakresu podmiotowego – dotychczasowy podział podmiotów objętych obowiązkami UoKSC na operatorów usług kluczowych i dostawców usług

²⁶ Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, <https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3> (19.01.2025).

cyfrowych został zastąpiony podziałem na podmioty kluczowe i ważne. Zmiana zakresu podmiotowego (w tym objęcie nowych sektorów gospodarki) oraz procedury kwalifikowania podmiotów do tych grup według szacunków Ministerstwa Cyfryzacji spowoduje, że liczba podmiotów objętych ustawą wzrośnie z około 400 do ponad 10 000²⁷.

2. Określenie obowiązków dla podmiotów kluczowych i ważnych:
 - a) wprowadzenie systemu zarządzania bezpieczeństwem informacji;
 - b) wdrożenie skutecznych zabezpieczeń, szacowania ryzyka związanego z cyberbezpieczeństwem;
 - c) przekazywanie informacji i raportowanie o poważnych incydentach;
 - d) przeprowadzanie audytów bezpieczeństwa systemów informacyjnych;
 - e) wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obsługę i zgłaszanie incydentów oraz udostępnianie wiedzy na temat cyberbezpieczeństwa.
3. Zmiany w strukturze i funkcjonowaniu KSC:
 - a) utworzenie sektorowych zespołów CSIRT, które będą wspierać podmioty kluczowe – przed nowelizacją tworzenie sektorowych CSIRT-ów nie było obowiązkowe i utworzono je jedynie dla dwóch sektorów: finansowego (CSIRT KNF) i ochrony zdrowia (Centrum e-Zdrowia);
 - b) wprowadzenie możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne do właściwych zespołów CSIRT-ów sektorowych i CSIRT-ów poziomu krajowego za pomocą systemu teleinformatycznego ministra właściwego ds. informatyzacji;
 - c) wzmocnienie kompetencji nadzorczych organów właściwych ds. cyberbezpieczeństwa;
 - d) rozszerzenie kompetencji ministra cyfryzacji w zakresie nadzoru nad cyberbezpieczeństwem.
4. Egzekwowanie przepisów:
 - a) wprowadzenie bardziej restrykcyjnych środków nadzoru i egzekwowania przepisów, takich jak możliwość okresowego zawieszenia prawa do prowadzenia działalności gospodarczej przez podmioty kluczowe w przypadku naruszeń;
 - b) wprowadzenie nowych administracyjnych kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe i podmioty ważne.
5. Uwzględnienie dostawców wysokiego ryzyka – projekt nowelizacji zawiera mechanizm uznania za dostawcę wysokiego ryzyka określonego dostawcy sprzętu lub oprogramowania dla ważnych podmiotów gospodarczych i społecznych w związku

²⁷ I. Makosz, *Jakie przedsiębiorstwa obejmie nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa*, 2025, <https://www.prawo.pl/podatki/jakie-przedsiębiorstwa-obejmie-nowelizacja-ustawy-o-krajowym-sys-temie-cyberbezpieczenstwa,531171.html> (19.03.2025).

z możliwym zagrożeniem bezpieczeństwa kluczowych podmiotów w Polsce, a przez to w konsekwencji także funkcjonowania państwa. Zapisy w tym zakresie wynikają z opublikowanego przez Komisję Europejską zestawu środków dotyczących minimalnej harmonizacji i standaryzacji na poziomie Unii Europejskiej rozwiązań cyberbezpieczeństwa sieci 5G²⁸.

6. Wprowadzeniu Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę – opracowywanego przez ministra właściwego ds. informatyzacji we współpracy z Pełnomocnikiem, Rządowym Centrum Bezpieczeństwa oraz innymi ministrami i właściwymi kierownikami urzędów centralnych. Dokument jest przyjmowany przez Radę Ministrów w drodze uchwały.

Obok fundamentalnej z punktu widzenia cyberbezpieczeństwa UoKSC niezwykle istotne były także dwie ustawy przyjęte w 2023 roku, które wprowadziły szereg mechanizmów związanych z ograniczaniem zagrożeń i ataków w środowisku cyfrowym:

7. Ustawa z dnia 28 lipca 2023 roku o zwalczaniu nadużyć w komunikacji elektronicznej²⁹, która wdrożyła szereg istotnych regulacji dotyczących cyberbezpieczeństwa:
 - a) wprowadzenie ustawowej listy ostrzeżeń dotyczących domen internetowych służących do wyłudzeń danych i środków finansowych z wykorzystaniem phishingu – lista pozwala dostawcom Internetu na blokowanie ruchu do stron phishingowych;
 - b) obowiązek blokowania przez przedsiębiorców telekomunikacyjnych wiadomości tekstowych (SMS) zawierających treści uznane za *smishing*³⁰ oraz połączeń telefonicznych wykorzystujących techniki fałszowania numeru nadawcy (ang. *spoofing*) w celu podszywania się pod inną osobę lub instytucję;
 - c) utworzenie wykazu numerów służących wyłącznie do odbierania połączeń głosowych, prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej (UKE), co ma ograniczyć możliwość podszywania się pod numery infolinii urzędów i innych podmiotów;

²⁸ Opublikowany w styczniu 2020 r. wspólny zestaw środków wzmacniających cyberbezpieczeństwo oraz ograniczających ryzyko w obszarze cyberbezpieczeństwa mobilnych sieci 5G w krajach Unii Europejskiej stanowi podstawę do podejmowania w krajach członkowskich Unii skoordynowanych działań nakierowanych na bezpieczeństwo nowoczesnych sieci komórkowych. Dokument ten określany jest jako 5G Toolbox. <https://www.gov.pl/web/cyfryzacja/unijny-zestaw-srodkow-dla-cyberbezpieczenstwa-sieci-5g---zatwierdzony> (25.01.2025).

²⁹ Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. 2023, poz. 1703). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001703>.

³⁰ *Smishing* to forma cyberoszustwa wykorzystująca wiadomości SMS do wyłudzenia poufnych informacji lub nakłaniania ofiar do szkodliwych działań. Nazwa pochodzi z połączenia słów SMS i *phishing*. W Polsce do blokowania smishingu wykorzystywane są wzorce dostarczane operatorom telekomunikacyjnym przez CSIRT NASK.

- d) obowiązek stosowania przez dostawców obsługujących co najmniej 500 tys. użytkowników i podmioty publiczne mechanizmów ograniczających możliwość fałszowania nazwy nadawcy poczty elektronicznej;
 - e) wprowadzenie kar dla osób dopuszczających się nadużyć w komunikacji elektronicznej;
 - f) utworzenie łatwego do zapamiętania numeru 8080 do zgłaszania podejrzanych wiadomości SMS;
 - g) stworzenie listy nadpisów³¹ wiadomości SMS zastrzeżonych dla instytucji publicznych;
 - h) określenie praw i obowiązków przedsiębiorców telekomunikacyjnych związanych z zapobieganiem i zwalczaniem nadużyć w komunikacji elektronicznej.
8. **Ustawa z 7 lipca 2023 roku o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości³²** – jej celem było ograniczenie skali wyłudzeń finansowych i innych nadużyć wynikających z kradzieży tożsamości oraz zwiększenie bezpieczeństwa obywateli w obszarze cyfrowym i finansowym. Najważniejsze regulacje wprowadzone na mocy ustawy to:
- a) utworzenie rejestru zastrzeżeń numerów PESEL – umożliwia on obywatelom nieodpłatne zastrzeżenie i cofnięcie zastrzeżenia numeru PESEL za pośrednictwem elektronicznych usług (aplikacja mObywatel i portal Gov.pl) lub osobiście w urzędzie gminy;
 - b) wprowadzenie obowiązku weryfikacji numeru PESEL w rejestrze zastrzeżeń przez firmy i instytucje finansowe, w tym banki i instytucje kredytowe (np. w związku z zawarciem umowy o kredyt, pożyczkę, zakup z płatnością ratalną czy leasing) oraz notariuszy (np. w związku z umową kupna lub sprzedaży nieruchomości);
 - c) wprowadzenie obowiązku weryfikacji numeru PESEL w rejestrze zastrzeżeń przez operatorów telekomunikacyjnych przy wydawaniu duplikatu karty SIM, co ma zapobiegać nadużyciom związanym z autoryzacją transakcji finansowych za pośrednictwem telefonów komórkowych.

Z punktu widzenia cyfrowego bezpieczeństwa podmiotów realizujących zadania publiczne, w tym szczególnie organów administracji rządowej i samorządowej, ochrony zdrowia czy wymiaru sprawiedliwości, na uwagę zasługują również przepisy zawarte w **ustawie z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów**

³¹ Nadpisy w wiadomościach SMS to alfanumeryczne ciągi znaków, które pojawiają się jako nadawca wiadomości na urządzeniu odbiorcy, zastępując standardowy numer telefonu, np. Alert RCB, Allegro czy Biedronka.

³² Ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz.U. 2023, poz. 1394). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001394>.

realizujących zadania publiczne³³. Za istotne z punktu widzenia cyberbezpieczeństwa regulacje zawarte w tej ustawie należy uznać:

- a) ustalanie minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych;
- b) ustalanie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi;
- c) ustanowienie Krajowych Ram Interoperacyjności systemów teleinformatycznych, gwarantujących neutralność technologiczną i jawność używanych standardów i specyfikacji;
- d) określenie zasad dostosowania systemów teleinformatycznych używanych do realizacji zadań publicznych do minimalnych wymagań i Krajowych Ram Interoperacyjności.

Zapisy ustawy odwołują się do Krajowych Ram Interoperacyjności (KRI)³⁴, które zawierają zbiór norm, standardów i wytycznych określających sposób funkcjonowania systemów teleinformatycznych w administracji publicznej, a także m.in. minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz standardy bezpieczeństwa informacji w systemach administracji publicznej, nakładając jednocześnie na podmioty publiczne objęte KRI obowiązki w zakresie regularnego przeprowadzania audytów bezpieczeństwa informacji (co najmniej raz w roku), utrzymywania aktualności sprzętu i oprogramowania oraz szkolenia pracowników w zakresie bezpieczeństwa informacji.

Poza wskazanymi ustawami i rozporządzeniami, które odnoszą się w sposób bezpośredni do problematyki cyberbezpieczeństwa, w wielu innych aktach prawnych znaleźć można zapisy, które pośrednio wpływają na bezpieczeństwo systemów informacyjnych, ochronę danych i obywateli. Przykładem mogą być przepisy Kodeksu karnego penalizujące nieuprawniony dostęp do systemów informatycznych, ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną określająca zasady odpowiedzialności dostawców usług internetowych za treści publikowane przez użytkowników czy ustawa z dnia 19 sierpnia 2011 roku o usługach płatniczych, która określa odpowiedzialność dostawców usług płatniczych za nieautoryzowane przez klientów transakcje. W efekcie system cyberbezpieczeństwa tworzą nie tylko akty prawne ściśle temu dedykowane, ale również inne regulacje, które poprzez swoje szczegółowe zapisy wpływają na ostateczny poziom cyfrowego bezpieczeństwa.

³³ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, nr 64, poz. 565). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20050640565>.

³⁴ 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. 2024, poz. 773). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240000773>.

Polski system prawny w zakresie cyberbezpieczeństwa jest uzupełniany przez akty prawa Unii Europejskiej, które określają wspólne standardy i obowiązki dla państw członkowskich. Niektóre z tych aktów, takie jak rozporządzenia unijne dotyczące bezpieczeństwa cyfrowego, mają bezpośrednie zastosowanie w Polsce i nie wymagają implementacji poprzez krajowe ustawy. Dotyczy to m.in. opisanych wcześniej rozporządzeń: Aktu o Cyberbezpieczeństwie, Aktu o odporności cyfrowej, Ogólnego Rozporządzenia o Ochronie Danych, rozporządzenia o operacyjnej odporności cyfrowej, Aktu w sprawie sztucznej inteligencji.

Wyjątkiem od tej zasady jest ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych³⁵. Z uwagi na fakt, że unijne GDPR jest stosowane bezpośrednio we wszystkich państwach członkowskich, polska ustawa jedynie uszczegóławia niektóre zagadnienia (np. procedury powoływania inspektora danych osobowych, zasady akredytacji i certyfikacji czy też kompetencje Prezesa Urzędu Ochrony Danych Osobowych).

2.3. Inne dokumenty kształtujące formalne ramy w zakresie cyberbezpieczeństwa

Cyberbezpieczeństwo jako kluczowy element funkcjonowania współczesnych społeczeństw i gospodarek wymaga nie tylko regulacji na poziomie ustaw i rozporządzeń, ale także kompleksowego podejścia obejmującego inne dokumenty normatywne i strategiczne. Dokumenty te, choć nie zawsze mają charakter wiążący, odgrywają istotną rolę w kształtowaniu standardów, praktyk oraz wytycznych, które uzupełniają formalne regulacje prawne. Określają one kierunki polityki państwa, wyznaczają ramy organizacyjne oraz wprowadzają zalecenia i normy techniczne, które wspierają instytucje publiczne, przedsiębiorstwa i obywateli w skutecznym zabezpieczaniu infrastruktury cyfrowej.

W kontekście polskiego i europejskiego systemu cyberbezpieczeństwa dokumenty te pełnią ważną funkcję w harmonizacji podejścia do zarządzania ryzykiem, reagowania na incydenty oraz współpracy międzynarodowej. Stanowią one także istotny element podnoszenia świadomości i budowania odporności na zagrożenia w cyberprzestrzeni oraz umożliwiając spójne wdrażanie mechanizmów ochrony na różnych poziomach. W efekcie choć nie mają one rangi ustawowej, ich wpływ na kształtowanie systemu cyberbezpieczeństwa jest znaczący, przyczyniając się do zwiększenia poziomu ochrony danych, systemów i usług cyfrowych.

Oprócz aktów prawnych stanowionych na poziomie Unii Europejskiej i krajów członkowskich ramy formalne i prawne w zakresie cyberbezpieczeństwa w Polsce i Unii tworzą również inne dokumenty, w tym:

³⁵ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>.

- strategię w zakresie cyberbezpieczeństwa,
- normy, rekomendacje i standardy techniczne,
- umowy międzynarodowe i porozumienia.

Strategie w zakresie cyberbezpieczeństwa

Strategie w zakresie cyberbezpieczeństwa uchwalane na poziomie Unii Europejskiej oraz państw członkowskich odgrywają kluczową rolę w kształtowaniu polityki ochrony systemów informacyjnych, infrastruktury krytycznej oraz prywatności obywateli i organizacji. Dokumenty te określają kierunki działań na rzecz zwiększenia odporności na cyberzagrożenia, harmonizacji przepisów oraz współpracy między państwami członkowskimi w celu przeciwdziałania cyberatakami. Na poziomie Unii Europejskiej strategię cyberbezpieczeństwa mają na celu ustanowienie wspólnych standardów, które zapewniają spójność działań we wszystkich krajach członkowskich. Przykładem jest Strategia Cyberbezpieczeństwa UE z 2020 roku, która zawiera propozycje inicjatyw regulacyjnych, inwestycyjnych i politycznych w trzech obszarach działań Unii: ochrona infrastruktury krytycznej i suwerenność technologiczna, rozwój zdolności do zapobiegania, odstraszania i reagowania na incydenty w cyberprzestrzeni oraz rozwój globalnej i otwartej cyberprzestrzeni poprzez zacieśnienie współpracy międzynarodowej³⁶. Wprowadzenie dyrektywy NIS2 stanowi jeden z kluczowych elementów tej strategii, obligując państwa członkowskie do wdrażania bardziej rygorystycznych wymogów w zakresie ochrony sieci i systemów informatycznych.

Na poziomie krajowym strategię cyberbezpieczeństwa stanowią fundament dla narodowych polityk i programów ochrony cyberprzestrzeni. Państwa członkowskie Unii Europejskiej opracowują własne strategię dostosowane do specyfiki lokalnych zagrożeń, infrastruktury technologicznej oraz priorytetów bezpieczeństwa narodowego. Warto zauważyć, że przyjęcie krajowych strategii cyberbezpieczeństwa jest nie tylko dobrą praktyką, ale również obowiązkiem wynikającym z prawa unijnego. Dyrektywa NIS2 wymaga, aby każde państwo członkowskie przyjęło krajową strategię cyberbezpieczeństwa, która określa cele strategiczne, niezbędne zasoby do ich osiągnięcia oraz odpowiednie środki polityczne i regulacyjne w celu osiągnięcia i utrzymania wysokiego poziomu cyberbezpieczeństwa na płaszczyźnie krajowej i ogólnoeuropejskiej. Od 2017 roku wszystkie kraje członkowskie opracowały i przyjęły krajowe strategię w zakresie cyberbezpieczeństwa, w tym część z krajów dokonała już aktualizacji swoich strategii w kolejnych latach³⁷.

³⁶ *The EU's Cybersecurity Strategy for the Digital Decade*, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> (3.03.2025).

³⁷ ENISA, *2024 Report on the State of the Cybersecurity in the Union*, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (12.03.2025).

Polska strategia cyberbezpieczeństwa określa najważniejsze cele i kierunki działań w zakresie ochrony cyberprzestrzeni państwa i obywateli. Aktualnie obowiązującą strategią jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024³⁸, która została przyjęta przez Radę Ministrów 22 października 2019 roku i weszła w życie 31 października 2019 roku, zastępując wcześniejsze Krajowe Ramy Polityki Cyberbezpieczeństwa na lata 2017–2022. W dokumencie określono pięć celów szczegółowych:

1. Rozwój krajowego systemu cyberbezpieczeństwa – obejmujący ewaluację i aktualizację przepisów prawa (w tym UoKSC), wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Cyberprzestrzeni RP oraz realizację działań związanych z rozwojem i budową odpornego na cyberzagrożenia systemu wymiany informacji.
2. Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty poprzez opracowanie Narodowych Standardów Cyberbezpieczeństwa (przykładem są już opracowane Standardy Cyberbezpieczeństwa Chmur Obliczeniowych), realizację przepisów tzw. Aktu o cyberbezpieczeństwie, z czym wiąże się utworzenie, utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa, oraz opracowanie wspólnej dla wszystkich sektorów metodyki audytów w zakresie cyberbezpieczeństwa.
3. Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa – finansowanie w ramach współpracy z Narodowym Centrum Badań i Rozwoju (Program CyberSecIdent – Cyberbezpieczeństwo i Tożsamość) badań naukowych, rozwoju nowoczesnych technologii i rozwiązań w cyberbezpieczeństwie oraz wzmocnienie współpracy z sektorem prywatnym i międzynarodowym poprzez realizację Programu Współpracy w Cyberbezpieczeństwie (PWCyber).
4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa – podniesienie kompetencji kadr nie tylko w podmiotach istotnych dla systemu cyberbezpieczeństwa RP, ale także pracowników administracji, przedsiębiorców i obywateli poprzez kampanie edukacyjne i szkolenia oraz promowanie dobrych praktyk w zakresie ochrony danych i systemów.
5. Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa – zaangażowanie w działania europejskich instytucji i zespołów działających w obszarze cyfrowego bezpieczeństwa oraz aktywne działania Polski w relacjach międzynarodowych (w tym regionalnych i globalnych w ramach systemu Narodów Zjednoczonych).

Aktualnie Ministerstwo Cyfryzacji prowadzi prace nad nową strategią cyberbezpieczeństwa dla Polski na kolejne lata. Projekt Strategii Cyberbezpieczeństwa

³⁸ Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037>.

Rzeczypospolitej Polskiej na lata 2025–2029 został przekazany do konsultacji z innymi resortami i instytucjami na poziomie krajowym.

Strategie cyberbezpieczeństwa stanowią podstawę do tworzenia aktów prawnych i norm technicznych, które regulują kwestie ochrony danych, reagowania na incydenty oraz współpracy międzynarodowej, a w konsekwencji przyczyniają się do zwiększenia odporności państw i organizacji na cyberzagrożenia. Mają one również wymiar ekonomiczny i technologiczny, ponieważ ich wdrażanie wspiera rozwój innowacyjnych rozwiązań oraz wzmacnia zdolność europejskich firm do konkurowania na globalnym rynku, co jest szczególnie istotne wobec dynamicznego rozwoju nowych technologii, takich jak sztuczna inteligencja i Internet Rzeczy.

Istotnym elementem strategii cyberbezpieczeństwa staje się w ostatnich latach aspekt obronny i geopolityczny. W obliczu rosnącej liczby ataków sponsorowanych przez państwa trzecie oraz działań dezinformacyjnych strategie umożliwiają skuteczną koordynację działań w zakresie cyberobrony, współpracę sojuszniczą oraz rozwój zdolności do odstraszania potencjalnych agresorów. Ponadto ich realizacja przyczynia się do wzmacniania pozycji państwa na arenie międzynarodowej, zwiększając jego zdolność do przeciwdziałania zagrożeniom hybrydowym i wpływom geopolitycznym poprzez cyberprzestrzeń.

Normy, rekomendacje i standardy techniczne

Obok regulacji prawnych i strategii cyberbezpieczeństwa, które wyznaczają ramy prawne i strategiczne dla ochrony systemów informatycznych, istnieje też szereg nieobowiązkowych narzędzi w postaci norm, rekomendacji i standardów technicznych. Choć ich stosowanie nie jest wymogiem prawnym, mają one istotny wpływ na poziom cyberbezpieczeństwa państw, instytucji oraz przedsiębiorstw, wspierając regulacje prawne i dostarczając konkretnych wytycznych dla organizacji. Normy, rekomendacje i standardy techniczne różnią się między sobą przede wszystkim zakresem, charakterem oraz sposobem ich stosowania. Podstawowe różnice pomiędzy tymi narzędziami przedstawiono w tabeli 2.

Tabela 2. Porównanie zakresu i charakteru różnych dokumentów tworzących formalne ramy cyberbezpieczeństwa

Rodzaj dokumentu	Charakter	Zakres obowiązywania	Przykłady
Regulacje prawne	Akty prawne regulujące bezpieczeństwo IT	Obowiązkowe	GDPR, NIS2, DORA, UoKSC
Normy	Zbiory wytycznych i najlepszych praktyk	Dobrowolne, ale szeroko stosowane	ISO/IEC 27001, ISO 15408 (Common Criteria)

Rodzaj dokumentu	Charakter	Zakres obowiązywania	Przykłady
Standardy techniczne	Specyfikacje technologiczne i metodyczne	Zależne od organizacji lub regulacji	ETSI EN 303 645, NIST SP 800-53
Rekomendacje	Wytyczne i dobre praktyki	Niewiążące, elastyczne	Rekomendacje ENISA czy KNF dla sektora finansowego

Źródło: opracowanie własne.

Normy to dokumenty opracowane przez uznane organizacje normalizacyjne, takie jak International Organization for Standardization (ISO), Polski Komitet Normalizacyjny (PKN) czy Europejski Komitet Normalizacyjny (CEN), które określają zasady, wytyczne lub specyfikacje techniczne dla produktów, procesów lub usług. Mają one zwykle charakter dobrowolny, ale mogą stać się obowiązkowe, jeśli zostaną powołane w przepisach prawnych lub umowach. Wdrażanie norm wynikać może z przepisów prawa, spełnienia wymogów partnerów, chęci uzyskania certyfikacji lub zwiększenia poziomu zaufania klientów. Przykładami norm w zakresie cyberbezpieczeństwa są:

1. ISO/IEC 27001 – międzynarodowa norma standaryzująca system zarządzania bezpieczeństwem informacji (SZBI). Określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu, który ma na celu ochronę poufności, integralności oraz dostępności informacji w organizacji. Pomaga identyfikować zagrożenia, zarządzać ryzykiem i wdrażać odpowiednie środki bezpieczeństwa³⁹.
2. ISO/IEC 15408 – międzynarodowa norma znana również jako Common Criteria for Information Technology Security Evaluation, określająca kryteria oceny bezpieczeństwa systemów teleinformatycznych. Wspiera proces projektowania, wdrażania oraz oceny produktów IT, takich jak oprogramowanie, sprzęt czy systemy komputerowe, pod kątem ich odporności na zagrożenia bezpieczeństwa.

Standardy techniczne to szczegółowe dokumenty określające wymagania techniczne dla produktów, procesów lub usług w celu zapewnienia ich jednolitości, kompatybilności i bezpieczeństwa. Często są one powiązane z normami i regulacjami prawnymi. Są przyjmowane przez organizacje techniczne, np. Europejski Instytut Norm Telekomunikacyjnych (European Telecommunications Standards Institute – ETSI), Instytut Inżynierów Elektryków i Elektroników (Institute of Electrical and Electronics Engineers – IEEE), Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST), i stanowią praktyczne wskazówki dotyczące wdrażania zabezpieczeń. Przykładami standardów w zakresie cyberbezpieczeństwa są:

³⁹ Norma ISO/IEC 27001 jest częścią zbioru norm ISO/IEC 27000, na który składają się również normy ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 czy ISO/IEC 27032.

1. ETSI EN 303 645 – globalny standard cyberbezpieczeństwa dla konsumenckich urządzeń Internetu Rzeczy opracowany przez Europejski Instytut Norm Telekomunikacyjnych we współpracy z producentami, środowiskiem naukowym i rządami państw;
2. NIST SP 800-53 – standard cyberbezpieczeństwa opracowany przez Narodowy Instytut Standardów i Technologii w Stanach Zjednoczonych, który określa wymagania dotyczące zabezpieczeń systemów informatycznych i organizacyjnych. Jest on jednym z najważniejszych dokumentów dotyczących zarządzania cyberbezpieczeństwem, szeroko stosowanym nie tylko w instytucjach rządowych USA, ale też przez organizacje na całym świecie, w tym w Europie.
3. IEC 62443 – międzynarodowy standard opracowany przez Międzynarodową Komisję Elektrotechniczną (IEC), dotyczący cyberbezpieczeństwa systemów automatyki i sterowania przemysłowego (ang. *Industrial Automation and Control Systems – IACS*). Jest on kluczowy dla ochrony infrastruktury krytycznej, takiej jak systemy energetyczne, wodociągi, zakłady chemiczne czy sieci transportowe.

Rekomendacje to niewiążące wytyczne opracowane przez instytucje publiczne lub prywatne w celu podniesienia poziomu cyberbezpieczeństwa. Są one bardziej elastyczne niż normy i standardy techniczne, a ich wdrożenie jest dobrowolne i zależy od decyzji organizacji. Ich celem jest promowanie najlepszych praktyk bez narzucania obowiązków. Przykłady rekomendacji w zakresie cyberbezpieczeństwa to m.in.:

1. Rekomendacje ENISA i CERT-EU w zakresie cyberbezpieczeństwa – wspólny zestaw dobrych praktyk pod nazwą „Boosting your Organization’s Cyber resilience – Joint Publication”⁴⁰, których powodem publikacji było rosnące zagrożenie *ransomware*⁴¹ i ponoszone z tego powodu straty.
2. Rekomendacje ENISA dotyczące bezpiecznego wdrażania usług chmurowych przez małe i średnie przedsiębiorstwa, opublikowane pod nazwą „Cloud Security Guide for SMEs”⁴².
3. Rekomendacje polskiej Komisji Nadzoru Finansowego dotyczące bezpieczeństwa ICT w sektorze finansowym (Rekomendacja D) – wytyczne dotyczące zarządzania ryzykiem związanym z systemami informatycznymi i telekomunikacyjnymi w bankach. Pierwsza wersja Rekomendacji D została opublikowana w 2002 roku, a następnie zaktualizowana w styczniu 2013 roku, aby dostosować ją do dynamicznego rozwoju technologii i rosnącego znaczenia IT w sektorze bankowym. Rekomendacja D obejmuje cztery główne obszary ryzyka środowiska teleinformatycznego: strategia

⁴⁰ Boosting your Organization’s Cyber resilience – Joint Publication, 2022, <https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience> (8.03.2025).

⁴¹ *Ransomware* to rodzaj ataku przeprowadzanego z wykorzystaniem złośliwego oprogramowania (*malware*), którego celem jest zaszyfrowanie danych ofiary lub zablokowanie dostępu do systemu komputerowego. Za odszyfrowanie lub odblokowanie dostępu przestępca żąda okupu (ang. *ransom*).

⁴² Cloud Security Guide for SMEs, 2015, <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes> (8.03.2025).

- i organizacja technologii informacyjnej i bezpieczeństwa, rozwój środowiska IT, utrzymanie i eksploatacja IT, zarządzanie bezpieczeństwem IT.
4. Rekomendacje polskiego Ministerstwa Cyfryzacji dla podmiotów sektora ochrony zdrowia – zawierają zestaw rekomendowanych minimalnych zaleceń bezpieczeństwa przeciwdziałających oraz ograniczających skutki incydentów cyberbezpieczeństwa. Dokument został przygotowany w celu szybkiego wdrożenia minimalnych zaleceń bezpieczeństwa z uwagi na sytuację związaną z pandemią COVID-19 i krytycznym znaczeniem zapewnienia niezakłóconego świadczenia usług przez placówki ochrony zdrowia.

Umowy międzynarodowe i porozumienia

Współczesne cyberzagrożenia coraz częściej mają charakter transgraniczny, co sprawia, że żadne państwo nie jest w stanie skutecznie zapewnić bezpieczeństwa wyłącznie na poziomie krajowym. Takie ataki, jak globalne kampanie *ransomware* czy operacje prowadzone przez grupy hakerskie sponsorowane przez państwa, pokazują, że cyberprzestępczość wymaga skoordynowanych działań międzynarodowych. Zmiany geopolityczne, np. nasilenie cyberataków w kontekście konfliktu rosyjsko-ukraińskiego, dodatkowo podkreślają konieczność współpracy państw w zakresie cyberobrony i przeciwdziałania zagrożeniom hybrydowym.

W przeciwieństwie do regulacji prawnych, takich jak RODO czy dyrektywa NIS2, które są wiążące dla państw członkowskich Unii Europejskiej, umowy i porozumienia międzynarodowe mają charakter dobrowolny i wymagają współpracy międzyrządowej w zakresie wdrażania ich postanowień. Jednym z ważniejszych przykładów współpracy międzynarodowej jest **Konwencja Rady Europy⁴³ o cyberprzestępczości** (Konwencja budapeszteńska)⁴⁴, która umożliwia państwom współpracę w zakresie ścigania cyberprzestępców oraz wymiany informacji o zagrożeniach. Powstała ona w związku z coraz powszechniejszym wykorzystaniem przestrzeni wirtualnej przez cyberprzestępców. Ze względu na globalny charakter Internetu skuteczne przeciwdziałanie temu zjawisku jest możliwe jedynie poprzez wdrożenie międzynarodowych mechanizmów współpracy. Głównym celem Konwencji jest umożliwienie efektywnej współpracy międzynarodowej w zakresie zwalczania przestępczości internetowej oraz penalizacja działań związanych z tworzeniem i rozpowszechnianiem w cyberprzestrzeni materiałów o charakterze rasistowskim i ksenofobicznym. Zapisy Konwencji określają katalog przestępstw

⁴³ Konwencja Rady Europy to międzynarodowy akt prawny o wysokiej randze, przyjmowany przez państwa członkowskie Rady Europy. Po ratyfikacji przez dane państwo konwencja staje się częścią krajowego porządku prawnego i jest wiążąca dla władz krajowych. Oznacza to, że państwa-strony konwencji są zobowiązane do przestrzegania jej postanowień i implementacji ich do swojego systemu prawnego.

⁴⁴ Konwencja Rady Europy o Cyberprzestępczości, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4656911> (15.03.2025).

popęlnianych z wykorzystaniem systemów informatycznych. Obejmuje on m.in. oszustwa i fałszerstwa komputerowe, przestępstwa związane z hackingiem (w tym nielegalny dostęp do systemów komputerowych oraz produkcję i sprzedaż tzw. narzędzi hackerskich), rozpowszechnianie i posiadanie pornografii dziecięcej, a także kopiowanie i dystrybucję utworów chronionych prawami własności intelektualnej.

Konwencja o cyberprzestępczości nakłada na państwa obowiązek wdrożenia odpowiednich procedur niezbędnych do prowadzenia postępowań karnych dotyczących przestępstw wymienionych w jej zapisach. Mają one na celu wsparcie krajowych organów ścigania w identyfikacji sprawców oraz gromadzeniu dowodów ich przestępczej działalności. Dokument reguluje m.in. zasady i gwarancje dotyczące przeszukiwania zasobów komputerowych, przekazywania, udostępniania i zabezpieczania danych informatycznych. Ponadto Konwencja zobowiązuje strony do podjęcia działań na rzecz wzmocnienia międzynarodowej współpracy w zakresie zwalczania cyberprzestępczości m.in. poprzez wzajemną pomoc prawną, wymianę informacji oraz ekstradycję sprawców.

Wśród innych przykładów międzynarodowych porozumień mających na celu wzmocnienie bezpieczeństwa i stabilność globalnej przestrzeni cyfrowej można wskazać:

1. Cyber Defence Pledge – porozumienie zawarte przez państwa członkowskie NATO podczas szczytu w Warszawie w 2016 roku. Jest to kluczowa inicjatywa Sojuszu Północnoatlantyckiego w zakresie cyberbezpieczeństwa, która ma na celu wzmocnienie cyberodporności państw członkowskich oraz zwiększenie ich zdolności do obrony przed zagrożeniami w cyberprzestrzeni. Stanowi ona ważny element strategii NATO w odpowiedzi na rosnące zagrożenia w cyberprzestrzeni i podkreśla znaczenie tej domeny dla bezpieczeństwa zbiorowego Sojuszu.
2. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) – międzynarodowe centrum badawczo-edukacyjne utworzone w 2008 roku w Tallinnie w wyniku porozumienia zawartego między państwami członkowskimi NATO. Jego głównym celem jest wspieranie państw członkowskich NATO oraz partnerów Sojuszu w obszarze cyberobrony poprzez edukację, badania, rozwój oraz wymianę doświadczeń i informacji. CCDCOE zostało utworzone po serii cyberataków na Estonię w 2007 roku. Ataki te uwiarydliły potrzebę zwiększenia zdolności NATO do reagowania na zagrożenia w cyberprzestrzeni.
3. Porozumienie o wymianie informacji między krajami Five Eyes (USA, Kanada, Wielka Brytania, Australia, Nowa Zelandia) – określa zasady współpracy wywiadowczej, której początki sięgają czasów II wojny światowej. Obecnie najważniejsze priorytety tej współpracy to zwalczanie cyberterroryzmu, cyberprzestępczości i innych zagrożeń cyfrowych.
4. Global Forum on Cyber Expertise (GFCE) – globalna platforma współpracy międzynarodowej, której celem jest wzmacnianie zdolności i ekspertyzy w zakresie cyberbezpieczeństwa na całym świecie. Powstała w 2015 roku podczas Global Conference

- on Cyber Space w Hadze z inicjatywy rządu Holandii oraz 41 innych uczestników, w tym przedstawicieli rządów, organizacji międzynarodowych i sektora prywatnego.
5. Porozumienie UE–NATO w zakresie cyberbezpieczeństwa – techniczne porozumienie zawarte w 2016 roku, które umożliwiło wymianę informacji oraz najlepszych praktyk między zespołami reagowania na cyberzagrożenia z NATO (NATO Cyber Security Centre – NCSC) oraz Unii Europejskiej (CERT-EU). Wśród siedmiu głównych obszarów wskazano m.in. zwiększenie zdolności do reagowania na zagrożenia hybrydowe, takie jak cyberataki i dezinformacja, a także podniesienie poziomu cyberbezpieczeństwa⁴⁵.

Międzynarodowe porozumienia zobowiązujące państwa członkowskie do wzmacniania swoich zdolności obronnych w cyberprzestrzeni czy umożliwiające szybszą wymianę informacji o zagrożeniach i incydentach cybernetycznych odgrywają kluczową rolę w globalnym systemie bezpieczeństwa. Ich znaczenie wykracza poza kwestie techniczne – poprzez wspólne działania wzmacniają one zaufanie między państwami i instytucjami, co jest szczególnie istotne w czasach rosnącej liczby cyberataków o podłożu geopolitycznym.

Porozumienia te przyczyniają się do budowy odporności na zagrożenia hybrydowe, w których cyberataki są wykorzystywane jako narzędzie destabilizacji politycznej, ekonomicznej i militarnej. Przykładem może być rosnąca liczba ataków na infrastrukturę krytyczną w Europie i USA, których celem jest zakłócenie funkcjonowania systemów energetycznych, finansowych czy transportowych. Współpraca międzynarodowa w ramach porozumień w zakresie cyberbezpieczeństwa pozwala na szybszą identyfikację sprawców ataków, skuteczniejsze reagowanie na incydenty oraz wzajemne wsparcie techniczne i operacyjne.

Ponadto w kontekście globalnej rywalizacji w cyberprzestrzeni międzynarodowe umowy i sojusze technologiczne stają się elementem strategii geopolitycznej. Porozumienia w zakresie cyberbezpieczeństwa i cyberobrony pokazują, że cyberbezpieczeństwo przestało być wyłącznie kwestią technologiczną, a jest kluczowym elementem strategii bezpieczeństwa narodowego. W obliczu dynamicznych zmian i rosnącej liczby zagrożeń rola porozumień w zapewnianiu stabilności i ochrony w cyberprzestrzeni będzie nadal rosła, stanowiąc fundament dla skutecznej walki z cyberprzestępczością i cyberwojną.

⁴⁵ Joint Declaration on EU-NATO Cooperation, https://www.nato.int/cps/en/natohq/official_texts_156626.htm (dostęp 16.03.2025 r.)

Charakterystyka, ewolucja i metody ograniczania cyberzagrożeń

Zagrożenia w cyberprzestrzeni mają z roku na rok coraz bardziej złożony i różnorodny charakter, stanowiąc wyzwanie zarówno dla firm, instytucji publicznych, jak i dla osób prywatnych. Szeroki wachlarz ataków – od prostych prób oszustwa po skomplikowane operacje wymierzone w infrastrukturę krytyczną – sprawia, że skuteczne zabezpieczenie zasobów cyfrowych staje się coraz trudniejsze. Cyberprzestrzeń stwarza obecnie nieograniczone możliwości zarówno dla użytkowników, jak i dla cyberprzestępców, którzy nieustannie opracowują nowe metody ataków.

Biorąc pod uwagę szerokie spektrum możliwości działania przestępców i innych podmiotów wywierających negatywny wpływ na środowisko cyfrowe, dokonanie pełnego przeglądu wszystkich wariantów zagrożeń, incydentów i ataków nie jest w niniejszym opracowaniu możliwe. Z tego względu dalsza analiza skoncentruje się wyłącznie na tych formach incydentów, które występują najczęściej i są najpoważniejsze w skutkach dla organizacji i osób prywatnych.

Analizy i raporty dotyczące cyberbezpieczeństwa wskazują, że w ostatnich latach na całym świecie, w tym również w krajach europejskich, lawinowo rośnie liczba cyfrowych zagrożeń i cyberataków. Wzrost ten dotyczy nie tylko liczby, wektorów i sposobów przeprowadzenia ataków czy obszarów, których dotyczą zagrożenia, ale też ich wpływu na użytkowników i systemy gospodarcze. Geopolityka i konflikty międzynarodowe powodują, że obserwuje się nasilenie ataków wspieranych przez rządy, w tym ataków kierowanych na krytyczne działy gospodarki. Coraz większym zagrożeniem staje się także dezinformacja rozpowszechniana za pomocą cyfrowych kanałów komunikacji (w tym poprzez media społecznościowe). Z analiz prowadzonych przez firmę Check Point Software Technologies wynika, że od kilku lat obserwowany jest znaczący rozwój globalnej cyberprzestępczości i wynikającej z tego liczby cyfrowych ataków i incydentów. Zebrane w tym zakresie dane wskazują, że w ciągu ostatnich 2 lat liczba cyberataków wzrosła o 30%, a tylko w 2024 roku nastąpił wzrost o 44% w porównaniu z rokiem 2023. Średnia liczba ataków przeprowadzanych na przeciętną organizację tygodniowo

osiągnęła w roku 2024 liczbę 1673¹. Jeszcze bardziej dostrzegalny jest wzrost liczby ataków w krajach europejskich. Według danych przedstawionych w raporcie opublikowanym przez DIGITAL SME liczba ataków skierowanych na zasoby i sieci firm europejskich wzrosła w ostatnim czasie o blisko 57%². Międzynarodowy Fundusz Walutowy szacuje, że liczba cyberataków na świecie w 2024 roku podwoiła się w porównaniu z okresem przed pandemią COVID-19³.

Zagrożenia dotyczą nie tylko dużych korporacji i operatorów infrastruktury krytycznej⁴. Według badania przeprowadzonego przez firmę Accenture w 2023 roku globalnie około 43% cyberataków skierowanych było nie na duże firmy, ale małe i średnie podmioty, z których jedynie 14% było przygotowanych na takie zdarzenia⁵. Małe i średnie przedsiębiorstwa stanowią atrakcyjne cele dla cyberprzestępców ze względu na ograniczenia zasobów finansowych przeznaczanych na zakup lub budowę rozwiązań w zakresie cyberbezpieczeństwa, a także deficyt wiedzy i świadomości, który sprawia, że właściciele MŚP często nie zdają sobie sprawy z zagrożeń, błędnie sądząc, że ich firmy nie są atrakcyjnymi celami dla cyberprzestępców⁶. Ograniczenia dotyczące wiedzy fachowej oraz środków finansowych sprawiają, że MŚP nie są w stanie zwalczać zagrożeń cyfrowych równie skutecznie jak duże podmioty, przez co są postrzegane przez przestępców jako łatwiejsze i w konsekwencji częściej wybierane cele⁷. W efekcie liczba ataków wykorzystujących np. mechanizmy socjotechniczne jest w przypadku firm zatrudniających mniej niż 100 pracowników aż o 350% większa niż w przypadku większych przedsiębiorstw⁸.

1 *The State of Cyber Security 2025 Report*, <https://www.checkpoint.com/security-report/> (25.02.2025).

2 <https://www.digitalsme.eu/57-surge-of-cyberattacks-in-europe-flagged-by-digital-sme-report/> (20.03.2025).

3 *The Global Financial Stability Report*, 2024, <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024> (18.02.2025).

4 Infrastruktura krytyczna to systemy i obiekty, które są niezbędne do funkcjonowania państwa i społeczeństwa, a ich zakłócenie lub zniszczenie mogłoby mieć poważne konsekwencje dla bezpieczeństwa i dobrobytu obywateli. Obejmuje ona zarówno fizyczne obiekty, jak i systemy cyfrowe. Według ustawy o zarządzaniu kryzysowym są to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców.

5 *Cyber Safety Tips for Small Business Owners*, <https://www.sba.gov/blog/2023/2023-09/cyber-safety-tips-small-business-owners> (12.02.2025).

6 D. Horváth, R.Z. Szabó, *Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?*, „Technological Forecasting and Social Change” 2019, no. 146, s. 119–132.

7 M.F. Arroyabe, C.F.A. Arranz, I. Fernandez de Arroyabe, J.C. Fernandez de Arroyabe, *The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges*, „Technological Forecasting and Social Change” 2024, no. 199.

8 *Spear Phishing – Top Threats and Trends*, <https://www.barracudamsp.com/resources/reports/spear-phishing-threats-and-trends> (8.04.2025).

Amerykańska Agencja ds. Rozwoju Międzynarodowego (US Agency for International Development – USAID) ocenia, że z punktu widzenia skutków finansowych cyberataki stają się jednym z najpoważniejszych zagrożeń dla przedsiębiorstw. Szacowany koszt, jaki poniosły przedsiębiorstwa na całym świecie w wyniku cyberprzestępczości, wyniósł w 2023 roku około 8 bln dolarów, a w 2027 roku ta kwota ma wzrosnąć trzykrotnie – do 24 bln dolarów⁹. Międzynarodowy Fundusz Walutowy ocenia¹⁰, że straty finansowe z powodu cyberincydentów wzrosły czterokrotnie od 2017 roku, zauważając jednocześnie, że faktyczne koszty cyberincydentów (bezpośrednie i pośrednie)¹¹ mogą być znacznie wyższe niż oficjalnie zgłaszane, a ich wysokość może stanowić od 1 do 10% światowego PKB¹². Dane dotyczące Polski wskazują, że tylko w sektorze handlu detalicznego straty spowodowane cyberatakami i wyciekami danych sięgnęły w 2024 roku prawie 90 mld złotych, a średnia suma szacowanych strat na jedną firmę wyniosła ponad 8 mln złotych¹³. Z kolei cyberoszustwa wykorzystujące techniki manipulacyjne (w tym np. techniki podszywania się pod inne osoby lub instytucje, oszustwa inwestycyjne czy fałszywe sklepy internetowe), których ofiarami padają zwykle osoby fizyczne, spowodowały w 2024 roku straty w wysokości około 500 mln złotych. Według danych gromadzonych przez Narodowy Bank Polski ofiarą oszustw mogło paść około 50 tys. osób, przy czym faktyczna liczba poszkodowanych może być większa, ponieważ nie wszystkie zgłaszają oszustwa.

3.1. Charakterystyka najczęstszych zagrożeń i ataków w polskiej i europejskiej cyberprzestrzeni

Analiza raportów oraz wyników badań prowadzonych w ostatnich latach w obszarze cyberbezpieczeństwa na świecie pozwala na określenie najważniejszych zagrożeń występujących aktualnie w cyberprzestrzeni. Przedstawione poniżej kategorie obejmują zagrożenia określone w oparciu o różne metody klasyfikacji i zostały wybrane na podstawie

⁹ USAID, *Economic Growth Briefer*, <https://www.usaid.gov/digital-development/cybersecurity/economic-growth-briefer> (5.09.2024).

¹⁰ *The Global Financial Stability Report*, 2024.

¹¹ Straty bezpośrednio obejmują najczęściej koszty związane z naprawą szkód, grzywny i kary nałożone przez organy regulacyjne w przypadku, gdy do incydentu doszło w wyniku zaniedbań ze strony zaatakowanego podmiotu, kwoty wymuszeń czy utracone dochody biznesowe spowodowane zakłóceniami operacyjnymi, natomiast straty pośrednie to m.in. utrata reputacji i zaufania klientów, zwiększone inwestycje w cyberbezpieczeństwo czy spadek efektywności pracy w firmie będący konsekwencją zakłóceń wywołanych cyberatakami.

¹² S. Kamiya, K. Jun-Koo, K. Jungmin, A. Milidonis, R.M. Stulz, *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms*, „Journal of Financial Economics” 2021, no. 139 (3), s. 719–749.

¹³ *Adyen Retail Report Poland 2024*, https://www.adyen.com/pl_PL/index-reports/retail (17.03.2025).

dostępnych informacji dotyczących ich częstości występowania i oceny skutków, jakie wywołują:

- a) zagrożenia dla dostępności systemów;
- b) zagrożenia związane z inżynierią społeczną;
- c) szkodliwe oprogramowanie i potencjalnie niepożądane aplikacje;
- d) cyberwymuszenia (z wykorzystaniem np. oprogramowania typu *ransomware*);
- e) wycieki i naruszenia związane z danymi przechowywanymi przez firmy i instytucje;
- f) ataki na przemysłowe systemy sterowania (w tym w obszarze infrastruktury krytycznej) oraz urządzenia Internetu Rzeczy;
- g) ataki na łańcuchy dostaw;
- h) kampanie dezinformacyjne;
- i) kradzieże tożsamości;
- j) zaawansowane ataki typu Advanced Persistent Threat (APT)¹⁴;
- k) luki i podatności w systemach informatycznych i oprogramowaniu.

Zagrożenia dla dostępności systemów

Kategoria zagrożeń dla dostępności systemów odwołuje się do pojęcia „dostępność” (ang. *availability*), które obok poufności i integralności jest jednym z kluczowych filarów bezpieczeństwa informacji. Termin ten oznacza, że systemy, usługi oraz dane są dostępne dla uprawnionych użytkowników w wymaganym czasie i zakresie. Zagrożenia dla dostępności systemów to wszelkie czynniki, które mogą prowadzić do zakłóceń w funkcjonowaniu systemów informatycznych, utraty dostępu do zasobów lub spowolnienia ich działania.

Zagrożenia dla dostępności można podzielić na kilka głównych kategorii. Pierwszą z nich są celowe ataki, takie jak ataki typu odmowa dostępu (ang. *Denial of Service* – DoS) czy rozproszona odmowa dostępu (ang. *Distributed Denial of Service* – DDoS), które polegają na generowaniu nadmiernego ruchu sieciowego w postaci ogromnej liczby żądań lub połączeń do atakowanego systemu (np. strony internetowej czy serwera, z którego udostępniana jest usługa), co prowadzi do przeciążenia systemu, a w konsekwencji niedostępności usług dla uprawnionych użytkowników. W przypadku ataków DDoS

¹⁴ *Advanced Persistent Threats* (APT) to skoordynowane i długotrwałe ataki cybernetyczne przeprowadzane przez wyspecjalizowane grupy przestępcze, często powiązane z państwami lub dużymi organizacjami. Celem APT jest systematyczna penetracja, eksploatacja i utrzymanie dostępu do celów strategicznych, takich jak systemy rządowe, infrastruktura krytyczna czy korporacje. APT charakteryzują się zaawansowanymi wektorami ataku, adaptacyjnym podejściem, długotrwałym ukryciem oraz zdolnością do konsekwentnego unikania wykrycia. Działania te wymagają znacznego nakładu zasobów, czasu oraz wyspecjalizowanej wiedzy, co odróżnia APT od standardowych cyberataków. <https://www.comcert.pl/sloownik/advanced-persistent-threats-apt/> (22.03.2025).

atakujący wykorzystuje sieć zainfekowanych komputerów lub urządzeń (*botnet*¹⁵) do zwielokrotnienia siły ataku. Celem ataków DoS/DDoS padają firmy na całym świecie, w tym również najwięksi dostawcy usług cyfrowych, np. Google, Microsoft czy Amazon¹⁶. W Polsce co roku obserwuje się wzrost liczby tego typu ataków, a szacunkowe dane wskazują, że tygodniowo może mieć miejsce nawet kilka tysięcy ataków DoS/DDoS skierowanych na polskie firmy i instytucje¹⁷. Tylko w 2024 roku celem serii ataków DDoS stały się polskie instytucje finansowe, strony internetowe komisji wyborczych oraz systemy związane z procesem wyborczym, sektor publiczny, w tym instytucje rządowe oraz podmioty zarządzające infrastrukturą krytyczną, taką jak wodociągi i systemy energetyczne. Wśród motywów, jakimi kierują się sprawcy, można wskazać chęć wymuszenia okupu w zamian za odstąpienie lub przerwanie ataku czy też wywołanie zakłóceń w funkcjonowaniu istotnych dla państwa lub gospodarki systemów informatycznych.

Drugą kategorią zagrożeń związanych z dostępnością systemów są awarie sprzętowe i infrastrukturalne, które mogą wynikać z naturalnego zużycia komponentów, błędów projektowych czy katastrof naturalnych, a trzecią – błędy ludzkie, które mogą prowadzić do niewłaściwej konfiguracji systemów czy przypadkowego uszkodzenia infrastruktury IT.

Zagrożenia związane z inżynierią społeczną

Inżynieria społeczna (ang. *social engineering*) to technika manipulacji psychologicznej, której celem jest skłonienie ofiary do ujawnienia poufnych informacji, podjęcia określonych działań lub naruszenia procedur bezpieczeństwa. W przeciwieństwie do klasycznych metod ataków polegających na przełamywaniu zabezpieczeń technicznych, metody socjotechniczne wykorzystują ludzkie słabości, chęć pomocy czy wpływ autorytetów, a także presję czasu i emocje i są często pierwszym krokiem w wieloetapowym procesie ataku, który może prowadzić do poważnych naruszeń bezpieczeństwa, wycieku danych osobowych lub finansowych, a nawet przejścia całych systemów organizacyjnych.

Zagrożenia bazujące na inżynierii społecznej obejmują niezwykle szerokie spektrum działań, które mogą być wymierzone zarówno w osoby indywidualne, jak i w duże przedsiębiorstwa, instytucje finansowe czy administrację publiczną. Wśród często stosowanych metod ataków wykorzystujących socjotechnikę można wskazać:

¹⁵ Botnety to sieci zainfekowanych komputerów lub urządzeń IoT zdalnie kontrolowane przez atakujących. Mogą one być wykorzystywane do przeprowadzania ataków typu DDoS, wysyłania spamu lub dalszego rozprzestrzeniania złośliwego oprogramowania. Atakujący wykorzystują botnety do wysyłania poleceń do zainfekowanych urządzeń i odbierania zebranych przez nie informacji.

¹⁶ *Ataki DDoS coraz groźniejsze*, 2021, <https://biznes.t-mobile.pl/pl/ataki-ddos-coraz-grozniesze> (17.03.2025).

¹⁷ *Rośnie liczba ataków na polskie firmy. W tym roku przeskoczy ważny próg*, 2024, <https://www.money.pl/gospodarka/co-grozi-firmom-w-cyberatakach-co-mozna-stracic-7075406726208352a.html> (17.03.2025).

1. **Phishing** – polega na wyludzaniu poufnych informacji poprzez podszywanie się pod zaufane podmioty. Atakujący wykorzystują e-maile, fałszywe strony internetowe lub komunikatory, aby nakłonić ofiary do udostępnienia danych logowania, informacji bankowych czy innych wrażliwych danych. Dodatkowo stosowane są techniki umożliwiające fałszowanie tożsamości nadawcy lub źródła komunikacji w celu wprowadzenia ofiary w błąd. Przykładem może być tzw. *e-mail spoofing* polegający na fałszowaniu pola „Od” w wiadomości e-mail, aby wyglądało, że pochodzi od zaufanej osoby lub instytucji, czy wykorzystanie technik homograficznych, w których dzięki użyciu znaków pochodzących z różnych alfabetów lub znaków wyglądających identycznie lub podobnie (np. litera l oraz cyfra 1) można rejestrować fałszywe domeny (adresy internetowe) i tworzyć linki prowadzące do stron wyglądających identycznie jak strony banków, korporacji, serwisów publicznych lub informacyjnych. Wykorzystanie zaawansowanych technik oraz możliwości technicznych (np. w zakresie automatycznego tłumaczenia treści w różnych językach) sprawia, że techniki phishingowe stają się coraz bardziej wyrafinowane, a fałszywe wiadomości coraz trudniejsze do odróżnienia od autentycznych. Do przeprowadzenia ataków mogą być wykorzystane różne odmiany phishingu, np.: *smishing* wykorzystujący wiadomości SMS zachęcające do kliknięcia złośliwych linków lub udostępnienia poufnych informacji czy *vishing* (*voice phishing*), w którym atakujący dzwonią do potencjalnych ofiar, podszywając się pod przedstawicieli banków, dostawców usług lub instytucji rządowych. Podobnie jak w przypadku e-maili, przestępcy mogą wykorzystać techniki fałszowania swojego identyfikatora – numeru telefonu (*Caller ID spoofing*), co umożliwia wyświetlenie na telefonie odbiorcy dowolnego numeru identyfikującego połączenie przychodzące. *Phishing* i jego odmiany mogą mieć charakter masowych kampanii skierowanych do szerokiego grona odbiorców (e-maile czy SMS-y rozsyłane do wielu odbiorców) lub ukierunkowanych ataków (tzw. *spear phishing*), których celem są konkretne osoby lub instytucje i które dla zwiększenia skuteczności często poprzedzone są zbieraniem szczegółowych informacji na temat celu ataku.
2. **Baiting** – polega na oferowaniu atrakcyjnie wyglądającej zachęty, aby nakłonić ofiary do podjęcia określonych działań. Przynętę może stanowić np. udostępnione w Internecie „darmowe” oprogramowanie, filmy, muzyka lub inna cyfrowa zawartość, która w rzeczywistości zawiera złośliwe oprogramowanie. Zachętą może być też fałszywy komunikat informujący o zagrożeniu, który wyświetla się użytkownikowi po wejściu na zainfekowaną stronę internetową lub profil w mediach społecznościowych zachęcający do pobrania np. fałszywego programu antywirusowego. Do zaatakowania konkretnego celu (np. firmy czy instytucji) przestępcy mogą również wykorzystać pozostawiony w miejscu publicznym dysk zewnętrzny (*pendrive*) zawierający szkodliwe oprogramowanie, licząc, że pracownik, który znajdzie taki dysk, podłączy go do firmowego urządzenia, infekując je i umożliwiając przejęcie nad nim kontroli i eskalację ataku.

3. *Pretexting* – zaawansowana forma inżynierii społecznej, w której cyberprzestępca przygotowuje szczegółową, wiarygodną historię w celu nakłonienia ofiary do ujawnienia prywatnych informacji lub podjęcia określonych działań (np. przekazania środków finansowych lub umożliwienia dostępu do konta bankowego). Metoda ta opiera się na psychologicznej manipulacji, której celem jest wywołanie u ofiary współczucia, strachu lub zaufania. W celu zwiększenia skuteczności atakujący może przeprowadzić wcześniej dokładne rozpoznanie, zbierając informacje o miejscu pracy ofiary, jej zainteresowaniach poprzez analizę mediów społecznościowych czy relacjach ze znajomymi na podstawie aktywności internetowej. Przykładem ataku opartego na pretextingu może być sytuacja, w której cyberprzestępca podaje się za pracownika banku i twierdzi, że wykrył podejrzaną aktywność na koncie ofiary. Wywołując poczucie zagrożenia, może przekonać ofiarę do podania hasła dostępowego i kodów autoryzacyjnych do przelewów lub zainstalowania złośliwego oprogramowania mającego rzekomo rozwiązać problem, a w rzeczywistości umożliwiającego dostęp do konta ofiary. W Polsce ta metoda manipulacji stała się w ostatnich latach niezwykle popularna, przybierając najróżniejsze formy, w których przestępcy podszycją się pod pracowników banków, operatorów telekomunikacyjnych, policjantów, znajomych lub bliskich ofiary (np. metoda „na wnuczka” czy też osoby szukające partnera/partnerki na portalach randkowych. W przypadku tego rodzaju oszustw przestępcy kierują się głównie motywacją finansową, jednak celem może być także skompromitowanie ofiary poprzez ujawnienie pozyskanych w trakcie ataku informacji. W okresie od stycznia 2021 roku do kwietnia 2022 roku członkowie jednej tylko grupy przestępczej, wykorzystując socjotechnikę, wyłudzili około 11 mln złotych od przedstawicieli trzech polskich gmin¹⁸.
4. *Wangiri* – oszustwo telefoniczne, w którym oszuści wykonują krótkie połączenia telefoniczne do potencjalnych ofiar, rozłączając się po jednym sygnale, zanim odbiorca zdąży odebrać telefon. Celem takiego działania jest sprowokowanie ofiary do oddzwonienia na nieznany numer (często są to numery o podwyższonej opłacie – zagraniczne lub premium), co skutkuje naliczeniem wysokich opłat za połączenie. Dodatkowo przestępcy mogą wykonywać połączenia z numerów, które sprawiają wrażenie, jakby były numerami należącymi do polskich operatorów (np. połączenia z Nigerii wyświetlają numer zaczynający się od +23, tak samo jak połączenia z numerów stacjonarnych z okolic Ciechanowa), oraz stosować techniki sztucznie wydłużające połączenie czy też wykonywać połączenia w nocy lub w godzinach pracy, kiedy trudniej jest odebrać telefon od razu. Oszustwo opiera się na motywacji finansowej,

¹⁸ Oszustwa na szkodę gmin. Akt oskarżenia trafił do sądu, 2024, https://www.rmfm24.pl/regiony/lodz/news-oszustwa-na-szkode-gmin-akt-oskarzenia-trafil-do-sadu,nId,7471466#crp_state=1 (18.03.2025).

bowiem wysokie opłaty, jakie ponosi osoba odzwaniająca, trafiają w całości lub w części (współpraca z lokalnymi operatorami telekomunikacyjnymi) do oszustów.

Szkodliwe oprogramowanie (*malware*) i potencjalnie niepożądane aplikacje

Szkodliwe oprogramowanie (ang. *malicious software* – *malware*) to ogólne określenie dla wszelkich programów komputerowych zaprojektowanych w celu wykonywania działań szkodliwych dla systemu, użytkownika lub organizacji. Może obejmować wirusy, robaki, trojany, *ransomware*, *spyware* i wiele innych rodzajów złośliwego kodu. Szkodliwe oprogramowanie działa na różnych poziomach systemów operacyjnych i aplikacji, w tym również na urządzeniach mobilnych, a jego głównymi celami mogą być:

- a) kradzież danych, np. haseł, informacji finansowych, danych osobowych (ang. *infostealer*);
- b) szpiegowanie użytkowników, np. poprzez rejestrację naciskanych klawiszy (ang. *keylogging*), przechwytywanie zrzutu ekranu lub obrazu z wbudowanej kamery;
- c) sabotaż systemów IT – uszkodzanie i kasowanie plików (ang. *wipers*), szyfrowanie danych (*ransomware*), blokowanie dostępu do usług lub systemów;
- d) uzyskanie nieautoryzowanego dostępu – tworzenie tylnych furtek (ang. *backdoors*) dla cyberprzestępców;
- e) rozprzestrzenianie się i infekowanie innych urządzeń.

Należy zauważyć, że w zależności od okoliczności i celu, w jakim instalowany jest dany program lub aplikacja, może on być uznany za *malware* (np. szpiegowanie nieświadomych użytkowników) lub oprogramowanie użytkowe (programy monitorujące działania wykonywane przez pracowników firm czy instytucji lub aplikacje służące kontroli rodzicielskiej). Analiza raportów dotyczących szkodliwego oprogramowania¹⁹ wskazuje na szybki rozwój nowych wariantów *malware* oraz znaczący ich wpływ na światowy poziom cyberbezpieczeństwa. W 2024 roku badacze zajmujący się analizą szkodliwego oprogramowania identyfikowali około 300 tys. nowych wariantów *malware* dziennie²⁰, a szacunki dotyczące cyberincydentów na świecie wskazują, że około 40% z nich wiązało się z jakąś formą złośliwego oprogramowania. Najgroźniejszym rodzajem szkodliwego oprogramowania pozostaje od kilku lat *ransomware* (złośliwe oprogramowanie, które szyfruje pliki lub całe urządzenia, uniemożliwiając dostęp do nich), które stanowiło 27% poważnych cyberincydentów w 2023 roku. Do najbardziej popularnych metod dostarczania szkodliwego oprogramowania do użytkowników należą linki internetowe i załączniki dołączane do wiadomości e-mail.

¹⁹ 100 Chilling Malware Statistics & Trends (2023–2025), <https://controld.com/blog/malware-statistics-trends/> (18.03.2025).

²⁰ Total amount of malware and PUA, <https://portal.av-atlas.org/malware> (18.03.2025).

Obok szkodliwego oprogramowania wyróżnia się też potencjalnie niepożądane aplikacje (ang. *Potentially Unwanted Applications* – PUA), czyli oprogramowanie, które użytkownik może nieświadomie zainstalować na swoim urządzeniu. Mogą one powodować takie działania, jak wyświetlanie reklam, instalowanie pasków narzędzi w przeglądarkach czy zmiana domyślnej strony głównej lub wyszukiwarki. Choć nie są zaprojektowane z myślą o wyrządzeniu bezpośredniej szkody, to mogą prowadzić do niepożądanych konsekwencji, takich jak spowolnienie działania komputera czy naruszenie prywatności.

Cyberwymuszenia

Cyberwymuszenia (ang. *Cyber extortion* – Cy-X) to forma cyberprzestępczości, w której bezpieczeństwo cyfrowych zasobów organizacji lub osób (poufność, integralność lub dostępność) zostaje naruszone i wykorzystane w celu wymuszenia zapłaty lub innych korzyści za pomocą gróźb lub szantażu. W przypadku organizacji przestępcy wykorzystują technologie informatyczne, aby zakłócić działanie systemów lub uzyskać dostęp do wartościowych zasobów, takich jak dane poufne, własność intelektualna czy krytyczne systemy infrastruktury. Po udanym ataku żądają okupu w zamian za zaprzestanie dalszych działań, odblokowanie systemów lub nieujawnianie skradzionych danych. W przypadku osób fizycznych przestępcy najczęściej szyfrują i wykradają dane, a następnie żądają zapłaty za odblokowanie dostępu do danych lub nieujawnianie skradzionych informacji.

Wśród najczęściej spotykanych metod stosowanych przy cyberwymuszeniach można wskazać oprogramowanie wymuszające okup (ang. *ransomware*) – po zaszyfrowaniu danych cyberprzestępcy żądają okupu w zamian za klucz deszyfrujący, który umożliwi odzyskanie dostępu do zaszyfrowanych zasobów. W ostatnim czasie obserwuje się wzrost liczby wielopoziomowych cyberwymuszeń (podwójnych lub potrójnych), w których przestępcy żądają okupu nie tylko za odszyfrowanie danych, ale także kolejnych za nieujawnienie wykradzionych danych (mogą zawierać poufne, wrażliwe lub kompromitujące informacje) czy też za odstąpienie od kolejnych ataków. Wzrasta również liczba incydentów związanych z wykorzystaniem *ransomware*. Z danych Check Point Software wynika, że w 2024 roku odnotowano łącznie 5414 ataków *ransomware* na organizacje na całym świecie, co stanowiło wzrost o 11% w porównaniu z rokiem poprzednim²¹. Z kolei firma Microsoft wskazała na jeszcze większą eskalację tego zjawiska, bowiem według *Digital Defense Report 2024* globalna liczba incydentów *ransomware* wzrosła o 175% w porównaniu z poprzednimi latami. W Europie *ransomware* odpowiadało za ponad

²¹ 2024 rokiem *ransomware*. Polskie instytucje na celowniku, <https://businessjournal.pl/2024-rokiem-ransomware-polskie-instytucje-na-celowniku/> (19.03.2025).

25% incydentów cyberbezpieczeństwa w latach 2023–2024, a Polska należy do trzech krajów (obok Ukrainy i Wielkiej Brytanii) najbardziej dotkniętych tego typu atakami²².

W raporcie *State of Ransomware 2024*²³ odnotowano, że 26% polskich firm straciło mniej niż 100 tys. złotych, 21% zanotowało straty w przedziale od 100 do 500 tys. złotych, a 13% poniosło straty od 500 tys. złotych do miliona. Straty powyżej miliona złotych zgłosiło 13% firm, z czego 8% straciło ponad 5 mln złotych.

Chociaż oprogramowanie wymuszające okup należy do najczęściej wskazywanych przykładów cyberwymuszeń, to należy podkreślić, że przestępcy szeroko wykorzystują też inne metody, takie jak np. opisane wcześniej ataki na dostępność (DoS/DDoS) czy szantaż oparty na informacjach dotyczących sfery intymnej i seksualnej (ang. *sextortion*). *Sextortion* polega na szantażowaniu ofiary groźbą opublikowania jej intymnych materiałów lub informacji dotyczących sfery seksualnej (np. zdjęć, nagrań wideo lub innych wrażliwych informacji pozyskanych w sposób nielegalny – w wyniku kradzieży czy wycieku lub też udostępnionych przez ofiarę) w celu wymuszenia określonych korzyści – zazwyczaj finansowych, ale także seksualnych lub innych. Według raportu Europejskiego Centrum ds. Cyberprzestępczości (EC3) liczba wymuszeń wykorzystujących materiały o charakterze seksualnym stale rośnie, jednak z uwagi na fakt, że wiele ofiar nie zgłasza tego typu przestępstw, skala zjawiska jest trudna do oszacowania. Szczególnie często ofiarami cyberprzestępstw o charakterze seksualnym padają nastolatki i młodzi dorośli z uwagi na brak doświadczenia i świadomości zagrożeń cyfrowych.

Wycieki i naruszenia związane z danymi przechowywanymi przez firmy i instytucje

Wycieki i naruszenia danych to incydenty, w wyniku których wrażliwe, chronione lub poufne informacje zostają ujawnione, przekazane lub udostępnione nieupoważnionym osobom lub podmiotom. O wycieku danych (ang. *data leak*) można mówić, kiedy dane zostają przypadkowo lub celowo udostępnione osobom nieuprawnionym bez naruszenia zabezpieczeń technicznych systemu lub bez bezpośredniego działania o charakterze przestępczym²⁴. Przyczyną wycieków są najczęściej zaniedbania, braki świadomości użytkowników lub błędy administracyjne. Przykładami mogą być takie sytuacje, jak pozostawienie dokumentów zawierających dane osobowe w miejscu publicznym czy błędne skonfigurowanie baz danych w chmurze umożliwiające publiczny dostęp.

²² Microsoft *Digital Defense Report 2024*, <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024> (19.03.2025).

²³ Sophos, *The State of Ransomware 2024*, <https://www.sophos.com/en-us/whitepaper/state-of-ransomware> (22.03.2025).

²⁴ K.L. Gwebu, J. Wang, L. Wang, *The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management*, „Journal of Management Information Systems” 2018, no. 35, s. 683–714.

Naruszenie danych (ang. *data breach*) jest pojęciem odnoszącym się do sytuacji, w której bezpieczeństwo danych zostaje naruszone w wyniku świadomych działań cyberprzestępców, których celem jest uzyskanie korzyści finansowych, politycznych lub społecznych. Podejście różnicujące oba przedstawione wyżej terminy nie zawsze jednak znajduje odzwierciedlenie w przepisach. Zgodnie z treścią art. 4 pkt 2 Ogólnego rozporządzenia o ochronie danych (RODO/GDPR) termin „naruszenie danych” oznacza „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”²⁵, co oznacza, że niezależnie od podjętych działań czy intencji każde ujawnienie danych osobowych jest traktowane jako naruszenie. Ponieważ jednak incydenty dotyczące cyberbezpieczeństwa mogą dotyczyć innych danych niż dane osobowe oraz z uwagi na fakt rozdzielania tych pojęć przez badaczy cyberbezpieczeństwa i w raportach dotyczących incydentów, w niniejszym opracowaniu wyciek i naruszenie danych będą traktowane jako odrębne pojęcia.

Z badania ankietowego Barometr Cyberbezpieczeństwa przeprowadzonego w 2024 roku przez KPMG wynika, że zagrożenia związane z wyciekami i naruszeniami danych są wskazywane jako najważniejsze ryzyko dla badanych organizacji. Najwyżej oceniane było ryzyko związane z takimi incydentami, jak: wyłudzenie danych uwierzytelniających (dane służące do logowania), naruszenia danych spowodowane złośliwym oprogramowaniem, kradzież danych przez pracowników i utrata danych w wyniku kradzieży lub zgubienia nośników czy urządzeń mobilnych. Spośród badanych firm 20% zarejestrowało incydenty związane z danymi osobowymi.

Problem związany z wyciekami i naruszeniami danych staje się coraz bardziej znaczący w kontekście rosnącego wolumenu danych, jakie gromadzą i przetwarzają podmioty na całym świecie, poziomu zaawansowania systemów informatycznych (w tym rozwiązań chmurowych) w połączeniu z niewystarczającymi często kwalifikacjami administratorów i użytkowników oraz wzrostu liczby ataków pośrednio lub bezpośrednio ukierunkowanych na pozyskanie danych – dla przestępców pozyskanie danych może być bezpośrednim celem (szpiegostwo) lub pośrednim (kiedy np. zaszyfrowanie danych służy osiągnięciu celu finansowego w postaci okupu).

²⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Tekst mający znaczenie dla EOG), 119 OJ L § (2016). <http://data.europa.eu/eli/reg/2016/679/oj/pol>.

Ataki na przemysłowe systemy sterowania (w tym w obszarze infrastruktury krytycznej) oraz urządzenia Internetu Rzeczy

Postępujące procesy cyfryzacji, automatyzacji oraz integracji infrastruktury przemysłowej (w tym krytycznej) z rozwiązaniami IT systematycznie zwiększają potencjalną powierzchnię cyberataków i znaczenie cyberbezpieczeństwa w obszarze związanym z wykorzystaniem przemysłowych systemów sterowania i nadzoru (ang. *Industrial Control Systems* – ICS) oraz urządzeniami Internetu Rzeczy. ICS obejmują szereg technologii, takich jak systemy SCADA (ang. *Supervisory Control and Data Acquisition*), DCS (ang. *Distributed Control Systems*), sterowniki PLC (ang. *Programmable Logic Controllers*), a także inne elementy automatyki przemysłowej, które są wykorzystywane do zarządzania procesami produkcyjnymi, transportowymi czy świadczeniem usług użyteczności publicznej (produkcja i dostawy energii elektrycznej, dostawy wody czy oczyszczanie ścieków). W praktyce ICS są odpowiedzialne np. za sterownie przepływem wody, zarządzanie pompami w procesach oczyszczania ścieków, sterowanie zwrotnicami, sygnalizacją kolejową oraz monitorowanie parametrów technicznych w sieci kolejowej czy utrzymywanie odpowiedniej temperatury w chłodniach, a także automatyczne dozowanie składników w zakładach produkujących żywność.

Urządzenia IoT to szersze pojęcie, które obejmuje nie tylko systemy przemysłowe, ale również urządzenia konsumenckie i rozwiązania wykorzystywane w projektach inteligentnych domów. Ich głównym celem jest zbieranie danych, komunikacja między urządzeniami w sieci i automatyzacja, a przykładem zastosowania są urządzenia (często bardzo proste, działające na zasadzie włącz/wyłącz), które dzięki wzajemnej komunikacji umożliwiają automatyczne sterowanie oświetleniem, ogrzewaniem, wentylacją, klimatyzacją, sprzętem RTV i AGD oraz systemami bezpieczeństwa (np. wyłączają urządzenia elektryczne i obniżają temperaturę po wyjściu mieszkańców z domu, uruchamiają podlewanie w oparciu o prognozę pogody lub czujniki wilgotności gleby czy też uruchamiają alarm i wysyłają powiadomienie po wykryciu ruchu na monitorowanym obszarze).

Ze względu na swoją specyfikę zarówno ICS, jak i IoT są podatne na różne formy cyberzagrożeń. Powodem jest coraz powszechniejsze ich wykorzystanie oraz rosnąca integracja z publiczną siecią internetową. Ponadto ICS są projektowane z myślą o długim cyklu życia (często kilkanaście lub więcej lat), co w praktyce oznacza, że wiele z aktualnie używanych systemów jest opartych na starych technologiach, zaprojektowanych bez uwzględnienia współczesnych mechanizmów bezpieczeństwa i często pozbawionych możliwości aktualizacji. W konsekwencji takie rozwiązania mogą mieć szereg luk i podatności umożliwiających np. przejęcie nad nimi zdalnej kontroli. Z kolei urządzenia będące częścią systemów IoT ze względu na masową skalę produkcji oraz obniżanie kosztów przez producentów (ogromna część takich urządzeń produkowana jest w Chinach) są pozbawione zaawansowanych mechanizmów bezpieczeństwa w postaci np. silnego szyfrowania, zaawansowanych metod kontroli dostępu, wsparcia producentów

i regularnych aktualizacji oprogramowania, co sprawia, że coraz częściej stają się celem cyberataków. Na uwagę zasługuje fakt, że ataki na urządzenia przemysłowe czy IoT mogą mieć na celu nie tylko przejęcie nad nimi kontroli, ale również wykorzystanie ich słabych zabezpieczeń do eskalacji ataków zmierzających do przejęcia całej infrastruktury informatycznej atakowanego podmiotu. Otwartość protokołów komunikacyjnych, z jakich korzystają urządzenia IoT, sprawia, że po przejęciu nad nimi kontroli przestępcy mogą wykorzystać je jako część rozbudowanej sieci botnetów używanych do przeprowadzania ataków DoS/DDoS. Na świecie i w Polsce obserwuje się rosnącą liczbę ataków na systemy ICS/IoT oraz coraz wyższy poziom wyrafinowania takich ataków. W roku 2024 w Polsce miało miejsce co najmniej kilka ataków na przemysłowe systemy sterowania²⁶, co można wiązać z sytuacją geopolityczną i znaczącą rolą, jaką w tych atakach ogrywają grupy sponsorowane przez państwa.

Ataki na łańcuchy dostaw

Atak na łańcuch dostaw (znany również jako atak na stronę trzecią, atak na łańcuch wartości lub atak przez tylne drzwi) to specyficzny rodzaj cyberataku, w którym przestępcy zamiast bezpośredniego atakowania organizacji wykorzystują podatności u zewnętrznych dostawców lub partnerów biznesowych, aby za ich pośrednictwem wprowadzić złośliwe oprogramowanie lub uzyskać nieautoryzowany dostęp do systemów docelowej organizacji. Naruszając bezpieczeństwo zewnętrznych partnerów (dostawców/pośredników), atakujący mogą uzyskać dostęp do większych sieci, co sprawia, że bezpieczeństwo łańcucha dostaw staje się kwestią kluczową również w kontekście cyberbezpieczeństwa. Złożoność nowoczesnych łańcuchów dostaw, często obejmujących wielu dostawców i usługodawców, istotnie zwiększa to ryzyko cyberincydentów.

Do najczęściej stosowanych strategii ataków można zaliczyć:

1. Atak na oprogramowanie – polega na modyfikacji oprogramowania, które następnie jest dystrybuowane do klientów. Przykładem może być modyfikacja kodu oprogramowania antywirusowego lub księgowego, które tworzone jest przez zewnętrznego dostawcę.
2. Atak na sprzęt – oznacza wprowadzenie fizycznych modyfikacji do urządzeń (na etapie produkcji lub dystrybucji), które następnie są instalowane u odbiorcy końcowego. Przykładem może być dodanie niezamówionych komponentów do sprzętu komputerowego lub sieciowego, co umożliwi zdalny i nieautoryzowany dostęp do systemów użytkownika tego sprzętu.

²⁶ *Cyberataki na infrastrukturę krytyczną w Polsce – zagrożenia dla systemów ICS/OT*, 2025, <https://aspolska.pl/ataki-i-cyberataki-na-infrastruktura-krytyczna-w-polsce-zagrozenia-dla-systemow-ics-ot/> (22.03.2025).

3. Atak na oprogramowanie układowe (*firmware*) – metoda zbliżona do ataku na sprzęt, z tą różnicą, że nielegalna modyfikacja nie dotyczy fizycznych komponentów, ale zapisanego trwale na urządzeniu oprogramowania, które steruje jego podstawowymi funkcjami. Przykładem może być wprowadzenie np. do *firmware* routerów modyfikacji, które umożliwią atakującym przejęcie kontroli lub ich zablokowanie.

Chociaż ataki na łańcuchy dostaw nie są zjawiskiem nowym, to ich liczba i poziom zaawansowania znacząco wzrosły od 2020 roku, co pozostaje z pewnością w związku z pandemią COVID-19, która przyczyniła się do rozwoju pracy zdalnej i zmian w relacjach biznesowych na całym świecie. Amerykańska organizacja Identity Theft Resource Center przedstawiła w raporcie dotyczącym naruszeń danych z 2023 roku informację, że liczba organizacji dotkniętych atakami w łańcuchu dostaw wzrosła o ponad 2600 p.p. tylko w ciągu ostatnich 5 lat²⁷. Z raportu opublikowanego przez ENISA, w którym przeanalizowano ataki na łańcuchy dostaw w latach 2020–2021, wynika, że liczba ataków zwiększyła się w 2021 roku czterokrotnie, około 58% ataków na łańcuch dostaw miało na celu uzyskanie dostępu do danych (głównie danych klientów, w tym danych osobowych i własności intelektualnej), a w przypadku 62% ataków na organizację przestępcy wykorzystali ich zaufane relacje z pośrednikami/dostawcami. W większości incydentów (ponad 60%) do przełamania zabezpieczeń wykorzystano złośliwe oprogramowania²⁸. W przypadku 66% analizowanych ataków sami dostawcy/pośrednicy nie wiedzieli lub nie zgłosili, w jaki sposób zostały naruszone ich systemy. Tak duży odsetek wskazuje, że pomimo często zaufanych relacji istnieje znacząca luka w zakresie kompetencji dotyczących cyberbezpieczeństwem i procedur zgłaszania incydentów między dostawcami/pośrednikami a korzystającymi z ich usług organizacjami.

Wśród najważniejszych powodów wzrostu skali cyberzagrożeń dla globalnych łańcuchów dostaw wskazuje się:

- a) rosnącą zależność od zewnętrznych dostawców – organizacje coraz częściej korzystają z usług i produktów dostarczanych przez zewnętrzne podmioty, co zwiększa powierzchnię ataku;
- b) skomplikowane łańcuchy dostaw – globalizacja i złożoność relacji biznesowych powodują, że łańcuchy dostaw stają się coraz trudniejsze do monitorowania i zabezpieczania, co tworzy luki wykorzystywane przez cyberprzestępców;
- c) niedostateczne zabezpieczenia u dostawców/pośredników – mniejsze firmy, będące częścią łańcucha dostaw, często nie dysponują odpowiednimi zasobami na

²⁷ ITRC, *2023 Annual Data Breach Report*, <https://www.idtheftcenter.org/publication/2023-data-breach-report/> (24.03.2025).

²⁸ ENISA, *Threat Landscape for Supply Chain Attacks*, 2021, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks> (24.03.2025).

wdrożenie zaawansowanych środków bezpieczeństwa, co czyni je łatwym celem dla przestępców;

- d) brak świadomości i procedur bezpieczeństwa – nie wszystkie organizacje weryfikują poziom zabezpieczeń swoich dostawców, co prowadzi do wzrostu ryzyka ataków.

Kampanie dezinformacyjne

Dezinformacja jest określana jako działanie, którego celem jest sfabrykowanie lub zakłócenie przekazu informacyjnego, aby osiągnąć określone korzyści polityczne, społeczne, finansowe czy militarne. Obejmuje ona sytuację, kiedy rozpowszechniane treści są całkowicie lub częściowo fałszywe, zmanipulowane lub wprowadzające w błąd, w tym szczególnie kiedy nieprawdziwe informacje dotyczą kwestii ważnej z punktu widzenia interesu publicznego (np. szczepionek, sieci 5G, energii jądrowej, klimatu, działań rządu), mają wywołać niepewność lub wrogość, doprowadzić do polaryzacji albo zakłócenia procesów demokratycznych. Przykładem mogą być nieprawdziwe, ale wiarygodnie wyglądające teorie, artykuły lub komentarze czy fałszywe lub zmanipulowane treści audio lub wideo (ang. *deep fake*), które z uwagi na rozwój technologiczny stają się dla większości odbiorców niezwykle trudne do rozpoznania. Obok celowo rozpowszechnianych fałszywych informacji (dezinformacja) rozróżnia się też takie pojęcia, jak *misinformation* (dezinformacja niezamierzona) – powielanie nieprawdziwych i niezweryfikowanych informacji przez użytkownika (w efekcie braku wiedzy, znajomości kontekstu itp.), który bezkrytycznie przekazuje zmanipulowane treści innym osobom, oraz *malinformation* (złośliwe lub szkodliwe wiadomości) – tworzenie i rozpowszechnianie treści opartych na prawdziwych danych i faktach, ale celowo przedstawianych w zmienionym kontekście w celu wprowadzenia w błąd, zaszkodzenia lub manipulacji²⁹.

Chociaż samo zjawisko jest znane od dawna, to z powodu rozwoju technologii cyfrowych i mediów społecznościowych jako kanałów komunikacji społeczno-politycznej zyskało nowy wymiar i skalę, która stanowi realne zagrożenie dla cyberbezpieczeństwa. Obecnie fałszywe treści są coraz częściej rozpowszechniane lub wzmacniane za pomocą mediów społecznościowych, sztucznej inteligencji oraz takich technik, jak zautomatyzowane konta (boty), *mikrotargeting*³⁰ czy trollowanie³¹. W kontekście mediów społeczno-

²⁹ E. Domańska, *Dezinformacja – czym jest i jak ją zweryfikować*, https://cyberprofilaktyka.pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html (24.03.2025).

³⁰ *Mikrotargeting* to technika marketingowa i komunikacyjna, która wykorzystuje dane demograficzne, behawioralne oraz preferencje użytkowników w celu precyzyjnego dopasowania treści do określonych grup odbiorców. W kontekście cyberbezpieczeństwa i dezinformacji *mikrotargeting* jest stosowany do manipulowania opinią publiczną, szczególnie w kampaniach politycznych i społecznych.

³¹ Trollowanie to celowe prowokowanie lub zakłócanie dyskusji w Internecie poprzez publikowanie kontrowersyjnych, obraźliwych lub fałszywych treści. Może mieć charakter indywidualny lub być częścią

ściowych zwraca się uwagę na to, że portale społecznościowe stanowią nie tylko platformę dystrybucji fałszywych lub zmanipulowanych informacji, ale również same aktywnie promują określone narracje, szczególnie te, które wywołują silne reakcje użytkowników. Dzieje się tak, ponieważ algorytmy odpowiedzialne za angażowanie użytkowników premiują treści kontrowersyjne i spolaryzowane, co w konsekwencji zwiększa zasięg fake newsów i teorii spiskowych.

Wraz z rosnącą polaryzacją na scenie międzynarodowej (wojna w Ukrainie, rosnące napięcia na linii USA–Chiny, eskalacja konfliktu na Bliskim Wschodzie) dezinformacja staje się coraz bardziej istotnym elementem współczesnych zagrożeń hybrydowych, które łączą w sobie elementy klasycznych ataków cyfrowych z operacjami wpływu. Jest szeroko wykorzystywana jako narzędzie wojny informacyjnej w celu manipulowania opinią publiczną, pogłębiania podziałów społecznych i podważania zaufania do instytucji państwowych. Szczególnie niebezpiecznym zjawiskiem staje się w tym kontekście wykorzystywanie dezinformacji do zakłócania procesów demokratycznych i wpływania na wyniki wyborów, co powoduje, że jej wykrywanie i blokowanie staje się kluczowym elementem strategii cyberbezpieczeństwa wielu państw³².

Według danych Eurostatu w 2021 roku 47% wszystkich osób w wieku 16–74 lat w Unii Europejskiej widziało nieprawdziwe lub wątpliwe informacje w witrynach informacyjnych lub mediach społecznościowych w ciągu 3 miesięcy poprzedzających badanie, jednak tylko 23% internautów wskazywało, że weryfikuje prawdziwość informacji lub treści. Polska znalazła się wśród trzech krajów z najniższym odsetkiem osób weryfikujących informacje pochodzące z internetowych serwisów informacyjnych lub mediów społecznościowych. Było ich jedynie 16%³³. Niski poziom kompetencji Polaków w zakresie weryfikacji informacji potwierdzają wyniki raportu *Dezinformacja oczami Polaków*³⁴, z których wynika, że pomimo świadomości zagrożeń, jakie są konsekwencją coraz powszechniejszych technik manipulacji, prawie 30% Polaków nie weryfikuje w żaden sposób wiarygodności informacji. Jedynie 20% deklaruje, że kiedykolwiek słyszało o instytucjach, które zajmują się sprawdzaniem faktów i weryfikacją informacji publikowanych w przestrzeni informacyjnej (ang. *fact-checking*), a zaledwie 4% respondentów wskazuje na serwisy takich instytucji jako swoje źródło informacji. Badanie wykazało,

zorganizowanych kampanii dezinformacyjnych prowadzonych przez masowo rejestrowane lub przejmowane konta użytkowników, tzw. farmy trolli.

32 NASK, *Dezinformacja, fake newsy i cyberzagrożenia – czy nasze wybory są bezpieczne?*, <https://nask.pl/aktualnosci/dezinformacja-fake-newsy-i-cyberzagrozenia-czy-nasze-wybory-sa-bezpieczne/> (26.03.2025).

33 Eurostat, *How many people verified online information in 2021?*, <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211216-3> (26.03.2025).

34 *Dezinformacja oczami Polaków*, 2024, <https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a32-02a26c324f18> (26.03.2025).

że aż 91% Polaków zdecydowanie zgodziło się przynajmniej z jedną z 30 fałszywych informacji przedstawionych respondentom w trakcie badania³⁵.

Kradzieże tożsamości

Kradzież tożsamości (ang. *identity theft*) to przestępstwo polegające na nieuprawnionym przejęciu i wykorzystaniu cudzych danych, takich jak imię i nazwisko, dane uwierzytelniające (login i hasło), adres zamieszkania, PESEL, numery i informacje zawarte w dokumentach (dowód osobisty, paszport, prawo jazdy) czy wizerunek, w celu osiągnięcia korzyści finansowych, uzyskania dostępu do poufnych informacji, obejścia procedur bezpieczeństwa lub popełnienia przestępstw w imieniu ofiary. Odmianą kradzieży tożsamości jest tworzenie tzw. syntetycznych tożsamości, czyli oszustwo polegające na łączeniu prawdziwych i fałszywych informacji w celu stworzenia całkiem nowej tożsamości. W przeciwieństwie do kradzieży tożsamości, w której przestępca podszywa się pod istniejącą osobę, syntetyczna tożsamość dotyczy postaci, która nie odpowiada żadnej rzeczywistej osobie.

W dobie postępującej cyfryzacji usług publicznych i komercyjnych (w tym usług cyfrowej tożsamości, np. polski mObywatel) oraz rosnącego wolumenu danych przechowywanych w postaci cyfrowej przestępcy coraz częściej wykorzystują skradzione lub fałszywe tożsamości do wyłudzenia kredytów, przejmowania kont bankowych, oszustw podatkowych, nadużyć w systemach opieki zdrowotnej, prania brudnych pieniędzy czy rozpowszechniania w sieci nieprawdziwych bądź nielegalnych treści.

Pozyskanie danych niezbędnych do stworzenia fałszywej tożsamości może obejmować wiele metod, np. fizyczną kradzież dokumentów lub nośników, kradzież danych z systemów informatycznych (np. w wyniku ataku), pozyskanie danych ujawnionych w wyciekach, wykorzystanie manipulacji (np. w trakcie rozmowy telefonicznej ofiary z osobą podszywającą się pod pracownika banku czy innej instytucji), biały wywiad (np. wykorzystanie informacji udostępnianych przez użytkowników w mediach społecznościowych). W tym kontekście coraz większego znaczenia nabiera świadomość wagi przestrzegania zasad cyberhigieny związanej z ochroną prywatności w sieci i ograniczaniem zakresu informacji osobistych, jakie upubliczniane są za pośrednictwem Internetu. Brak wiedzy w tym zakresie sprawia, że użytkownicy sami publikują w sieci informacje (w tym np. numer telefonu, adres, datę urodzenia czy zdjęcia kart płatniczych, dowodów osobistych i innych dokumentów), które mogą zostać wykorzystane do kradzieży tożsamości. Chociaż większość Polaków dostrzega zagrożenia związane z niewłaściwym wykorzystaniem informacji osobistych (79% Polaków obawia się kradzieży tożsamości),

³⁵ Fałszywe informacje dotyczyły obszarów związanych z energetyką, zdrowiem, klimatem, nowymi technologiami oraz polityką i zawierały twierdzenia, które były obecne w przestrzeni publicznej.

to jednocześnie chętnie te dane udostępnia, jeśli wiąże się to z uzyskaniem określonych korzyści. Ponad połowa jest skłonna udostępniać informacje o sobie w celu ułatwienia zakupów online (56%), otrzymania spersonalizowanych rekomendacji tańszych alternatyw (55%) czy rekomendacji nowych produktów (52%)³⁶.

Badanie przeprowadzone w 2022 roku na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów wykazało, że aż 11,5% ankietowanych Polaków przyznało się do opublikowania w Internecie zdjęcia swoich dokumentów. W grupie wiekowej 18–24 lata odsetek ten był jeszcze wyższy i wynosił 20%³⁷. Problem kradzieży tożsamości dotyka osoby i organizacje na całym świecie. Ocenia się, że tylko w Stanach Zjednoczonych do tego rodzaju przestępstw dochodzi co 22 sekundy³⁸, a 42% obywateli USA doświadczyło tego rodzaju oszustwa, tracąc w jego wyniku średnio 280 euro. W 2024 roku Federalna Komisja Handlu USA otrzymała 1,4 mln zgłoszeń dotyczących kradzieży tożsamości³⁹. W krajach europejskich, w których łącznie odnotowuje się 32% globalnych cyberincydentów związanych z kradzieżą tożsamości, koszty finansowe, jakie poniosły osoby poszkodowane w wyniku kradzieży tożsamości, oszacowano średnio na poziomie około 320 euro na osobę w Wielkiej Brytanii i 277 euro w Danii⁴⁰. W Polsce skalę problemu w sposób częściowy obrazują dane publikowane systematycznie przez Związek Banków Polskich w raportach InfoDok. Prezentują one informacje dotyczące wykrytych i udaremnionych prób wyłudzeń kredytów z wykorzystaniem skradzionej tożsamości. W 2024 roku odnotowano aż 12,3 tys. takich prób (wzrost o 27% w stosunku do roku 2023), co stanowi rekord od roku 2008⁴¹. Łączna kwota udaremnionych prób wyłudzeń kredytów wyniosła ponad 324 mln złotych.

Na podkreślenie zasługuje fakt, że konsekwencje kradzieży tożsamości obejmują nie tylko skutki finansowe, jakie ponoszą osoby fizyczne i organizacje. Ofiary doświadczają również szeregu negatywnych i długotrwałych skutków psychologicznych, społecznych i prawnych. Mogą one obejmować np. problemy związane z naprawą swojej reputacji, zdolności kredytowej czy poważne zaburzenia w życiu zawodowym i prywatnym.

³⁶ *EY Future Consumer Index 2023*, https://www.ey.com/pl_pl/newsroom/2023/07/ey-fci-bezpieczenstwo-danych (19.03.2025).

³⁷ UODO, *Jedno deklarujemy, drugie robimy. Jak nie chronić danych osobowych*, <https://uodo.gov.pl/pl/138/2558> (26.03.2025).

³⁸ *Veridas, Cybersecurity in 2025: Navigating the Identity Fraud Landscape*, <https://www.linkedin.com/pulse/cybersecurity-2025-navigating-identity-fraud-landscape-veridas-pbdhf> (27.03.2025).

³⁹ *2025 Identity Theft Facts and Statistics*, <https://identitytheft.org/statistics/> (27.03.2025).

⁴⁰ *Britain lands at the top of global identity theft*, <https://thepayers.com/payments-general/britain-lands-at-the-top-of-global-identity-theft--1265445> (2.02.2025).

⁴¹ *Raport o dokumentach infoDOK – IV kwartał 2024*, <https://dokumentyzastrzezone.pl/raport-infodok/> (5.02.2025).

Zaawansowane ataki typu Advanced Persistent Threat

Ataki typu *Advanced Persistent Threat* (zaawansowane trwałe zagrożenia) to zaawansowane i długotrwałe działania cyfrowe realizowane przez dobrze zorganizowane grupy, których celem jest pozyskanie poufnych informacji, zakłócenie działalności lub zdobycie długofalowego dostępu do zasobów organizacji i firm o kluczowym znaczeniu dla bezpieczeństwa narodowego, ekonomicznego lub technologicznego danego państwa. Początkowo pojęcie APT używane było do określenia działań kierowanych przeciwko organizacjom o charakterze militarnym, jednak obecnie ten rodzaj ataków nie ogranicza się do domeny wojskowej i staje się zagrożeniem dla instytucji państwowych, firm oraz infrastruktury krytycznej⁴². Ataki APT cechują się długotrwałością i metodycznością. Podczas gdy tradycyjne ataki dążą do natychmiastowego efektu (np. zaszyfrowanie danych), APT skupiają się na stopniowym pozyskiwaniu informacji i utrzymaniu kontroli nad systemami. Wyróżniającymi cechami APT są:

- a) konkretne i jasno określone cele realizowane przez atakujących;
- b) zaawansowana organizacja działań i wysokie kompetencje atakujących;
- c) długotrwała (wielomiesięczna lub nawet wieloletnia) obecność w atakowanych systemach⁴³;
- d) wykorzystanie technik utrudniających wykrycie i późniejszą analizę działań.

Określenie APT stosowane jest też w odniesieniu do grup, które odpowiadają za realizację tego typu ataków. Są one bardzo często powiązane bezpośrednio lub pośrednio z rządami i instytucjami państwowymi, które zapewniają im wsparcie finansowe, techniczne i operacyjne.

Przykładami znanych grup APT są m.in.:

- a) APT28 (Fancy Bear) – powiązana z rosyjskim wywiadem wojskowym GRU, przypisuje się jej ataki na takie cele, jak Bundestag, NATO, Biały Dom oraz Komitet Narodowy Partii Demokratycznej USA;
- b) APT29 (Cozy Bear) – powiązana z rosyjską Służbą Wywiadu Zagranicznego (SVR), znana z ataków na agencje rządowe, np. w USA, Norwegii i Holandii;
- c) (APT38) Lazarus Group – północnokoreańska grupa znana z ataków na firmę Sony Pictures w 2014 roku oraz kradzież 81 mln dolarów z Banku Bangladeszu w 2016 roku;
- d) APT10 (Stone Panda) – chińska grupa zajmująca się cyberszpiegostwem technologicznym i przemysłowym, jej głównym celem są organizacje rządowe, technologiczne oraz dostawcy usług chmurowych.

⁴² P. Chen, L. Desmet., C. Huygens, *A Study on Advanced Persistent Threats* [w:] *Communications and Multimedia Security*, red. B. De Decker, A. Zúquete, Berlin–Heidelberg 2014.

⁴³ B. Olszewski, A. Rot, *Advanced Persistent Threat attacks as a new cybersecurity threat*, „Informatyka Ekonomiczna – Business Informatics” 2016, nr 2(40), s. 84–94.

Według raportu Group-IB liczba ataków przeprowadzonych przez grupy APT wzrosła w 2024 roku o 58% w porównaniu z rokiem 2023, przy czym Europa stała się głównym celem (45,31% wszystkich incydentów), a Polskę wskazano wśród dwunastu najczęściej atakowanych państw na świecie⁴⁴. Do najbardziej narażonych na ataki APT zaliczono:

- instytucje administracji publicznej,
- branżę produkcyjną,
- podmioty finansowe,
- firmy z obszaru technologii informacyjnych,
- jednostki naukowe.

Luki i podatności w systemach informatycznych i oprogramowaniu

Podatność (ang. *vulnerability*), określana również jako luka bezpieczeństwa, to słabość, którą cyberprzestępcy mogą wykorzystać do uzyskania nieautoryzowanego dostępu do systemu komputerowego. Najczęściej pojęcie to odnosi się do słabych punktów w systemach informatycznych, w tym oprogramowaniu, sprzęcie lub konfiguracji, które mogą zostać wykorzystane przez atakujących do uzyskania nieautoryzowanego dostępu, kradzieży danych czy zakłócenia działania systemu. W szerszym ujęciu obejmuje ono nie tylko techniczne słabości, ale także braki w procesach, politykach czy szkoleniach personelu. W zależności od rodzaju miejsca ich występowania lub elementu infrastruktury, którego dotyczą, podatności można podzielić na:

- a) podatności oprogramowania i aplikacji – błędy programistyczne lub projektowe aplikacji, które umożliwiają atakującemu wykonanie nieautoryzowanych działań;
- b) podatności systemów operacyjnych – powstają w wyniku błędów implementacyjnych lub projektowych systemu operacyjnego umożliwiających dostęp do danych lub manipulację nimi;
- c) podatności sprzętowe – związane bezpośrednio z komponentami sprzętowymi, wynikają z błędów projektowych lub implementacyjnych sprzętu;
- d) podatności sieci i protokołów komunikacyjnych – dotyczą mechanizmów i protokołów wykorzystywanych do przesyłania danych w sieciach;
- e) podatności baz danych – dotyczą systemów bazodanowych, mogą prowadzić do nieautoryzowanego dostępu, manipulacji lub wycieku danych;
- f) podatności organizacyjne i proceduralne – są efektem niewłaściwych polityk bezpieczeństwa, procedur organizacyjnych czy niedostatecznej świadomości pracowników;

⁴⁴ Group-IB, *High-Tech Crime Trends Report 2025*, <https://www.group-ib.com/landing/high-tech-crime-trends-2025/> (22.03.2025).

- g) podatności środowisk chmurowych – dotyczą specyficznych zagrożeń w środowiskach chmurowych, wynikających z błędnej konfiguracji, niedostatecznego zabezpieczenia zasobów czy błędów popełnionych przez dostawców usług chmurowych;
- h) podatności urządzeń Internetu Rzeczy – są związane ze specyfiką urządzeń IoT, a wynikają m.in. z błędów lub niewystarczającego zabezpieczenia oprogramowania układowego (firmware'u) czy niskich standardów bezpieczeństwa.

Wraz z postępującą cyfryzacją, rozwojem technologii informacyjnych i komunikacyjnych oraz rosnącą liczbą urządzeń podłączanych do Internetu podatności stają się niezwykle atrakcyjnymi celami ataków dla cyberprzestępców. Podatności wykryte w powszechnie używanym oprogramowaniu lub sprzęcie mogą prowadzić do sytuacji, w której liczba zagrożonych użytkowników oraz organizacji jest niezwykle duża. Tym samym umożliwiają cyberprzestępcom automatyzację działań oraz przeprowadzanie jednoczesnych ataków na wiele celów. Szczególnie niebezpieczne są podatności typu *zero-day*⁴⁵, czyli luki w oprogramowaniu lub sprzęcie, które nie zostały jeszcze zidentyfikowane przez producentów i specjalistów ds. bezpieczeństwa, a przez to nie posiadają odpowiednich poprawek ani zabezpieczeń. Takie podatności mogą być przez długi czas skutecznie wykorzystywane przez cyberprzestępców, pozostając niewykryte i powodując poważne szkody dla użytkowników oraz organizacji.

W celu usystematyzowania informacji o wykrywanych podatnościach stworzono szereg systemów ich kategoryzacji, wśród których do najpopularniejszych należą⁴⁶:

1. CVE (ang. *Common Vulnerabilities and Exposures*) – międzynarodowy standard identyfikacji i katalogowania podatności w sprzęcie i oprogramowaniu. Został utworzony w 1999 roku przez MITRE Corporation przy wsparciu DARPA, aby uporządkować sposób komunikacji o zagrożeniach cybernetycznych. Według danych z 2024 roku baza CVE zawiera ponad 240 tys. unikalnych identyfikatorów podatności, tzw. CVE ID (zawiera przedrostek CVE, rok wykrycia podatności oraz jej numer – np. CVE-2017-0144), a tempo przyrostu nowych wpisów wynosi około 20 tys. rocznie.
2. CWE (ang. *Common Weakness Enumeration*) – lista luk bezpieczeństwa w sprzęcie i oprogramowaniu (*hardware & software*), która jest aktualizowana przez społeczność międzynarodową. Zawiera słabości, które mogą się pojawiać przy projektowaniu zarówno oprogramowania, jak i komponentów sprzętowych. W 2024 roku na liście widniały 933 pozycje.

⁴⁵ Określenie *zero-day* (*0-day*) oznacza, że od momentu wykrycia podatności przez cyberprzestępców minęło dokładnie zero dni, czyli luka jest całkowicie nieznana producentowi oprogramowania lub sprzętu. W konsekwencji nie ma jeszcze dostępnych żadnych aktualizacji zabezpieczających czy poprawek eliminujących tę podatność.

⁴⁶ Wprowadzenie do bezpieczeństwa IT, t. 1, red. M. Sajdak, Kraków 2023, s. 387–389.

3. CVSS (ang. *Common Vulnerability Scoring System*) – system umożliwiający ocenę poziomu zagrożenia wynikającego z danej podatności. Wynik CVSS przyznawany jest na podstawie kilku kryteriów, takich jak wpływ na poufność, integralność i dostępność danych oraz łatwość wykorzystania podatności. CVSS klasyfikuje zagrożenia wynikające z podatności w 5-stopniowej skali (krytyczne, wysokie, średnie, niskie, brak). Podatność krytyczna umożliwia przejęcie pełnej kontroli nad serwerem lub urządzeniem sieciowym. Podatności, które zostały oznaczone jako krytyczne, powinny być bezzwłocznie naprawione. Podatność o wysokim poziomie istotności pozwala na uzyskanie dostępu do wrażliwych informacji, jednak może wymagać spełnienia pewnych warunków. Powinna zostać naprawiona w bardzo krótkim czasie od jej zgłoszenia. Wykorzystanie podatności o średnim poziomie istotności może zależeć od różnych czynników. Zazwyczaj umożliwia ona dostęp do ograniczonej ilości danych lub do danych o mniejszej istotności. Naprawa tej podatności nie musi być zrealizowana od razu, jednak nie należy też z nią zwlekać. Wykorzystanie podatności o niskim poziomie istotności ma niewielki wpływ na bezpieczeństwo lub wymaga bardzo trudnych warunków do jego spełnienia. Naprawa tej podatności może się odbyć przy aktualizacji aplikacji o np. nową funkcjonalność.

Kompleksowe zestawienie podatności znaleźć można w prowadzonej przez NIST bazie danych NVD (ang. *National Vulnerability Database*), która gromadzi informacje o podatnościach, przypisanych do nich CVE-ID, ocenach CVSS oraz zalecenia dotyczące zarządzania podatnościami. Według danych opublikowanych przez ENISA⁴⁷ w okresie od czerwca 2023 roku do czerwca 2024 roku w bazie NVD zarejestrowano 33 524 podatności, co oznacza wzrost o 35,8% w stosunku do poprzedniego roku (24 690 zarejestrowanych podatności). Wśród zarejestrowanych podatności 9,3% sklasyfikowano jako posiadające krytyczny poziom istotności, a 21,8% – poziom wysoki.

Należy podkreślić, że dobór i kolejność przedstawionych kategorii zagrożeń należy traktować jedynie orientacyjnie, bowiem precyzyjna ocena skali, liczby i skutków ataków wykorzystujących różne kategorie cyberzagrożeń oraz wektory ataków stanowi obecnie istotne wyzwanie. Złożoność i dynamiczny charakter środowiska cyfrowego, a także różnorodność technik stosowanych przez cyberprzestępców oraz niepełny dostęp do informacji na temat cyberincydentów utrudniają dokładne oszacowanie tych parametrów. Przykładowo w przypadku cyberwymuszeń przestępcy wykorzystują zwykle szkodliwe oprogramowanie szyfrujące (*ransomware*), a metody, jakimi się posługują w celu jego umieszczenie w infrastrukturze ofiary, mogą obejmować luki i podatności w systemach informatycznych lub oprogramowaniu, ataki na niezabezpieczone urządzenia IoT czy inżynierię społeczną.

⁴⁷ ENISA *Threat Landscape 2024*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (15.03.2025).

Dodatkowo wiele organizacji nie zgłasza incydentów bezpieczeństwa z obawy przed utratą reputacji lub konsekwencjami prawnymi i finansowymi. W przypadku osób fizycznych powodem braku zgłoszeń może być niewielka wartość poniesionych strat, wstyd, niezajomość lub skomplikowanie procedur związanych ze zgłaszaniem cyberprzestępstw, a także brak wiary w skuteczność zgłoszenia, co w konsekwencji prowadzi do niedoszacowania rzeczywistej liczby ataków. Ponadto zaawansowane techniki maskowania stosowane przez atakujących mogą powodować, że niektóre incydenty pozostają niewykryte przez dłuższy czas.

Również skutki ataków mogą być bardzo różne i zależne od wielu czynników, takich jak rodzaj ataku, wartość zaatakowanych zasobów czy efektywność zastosowanych środków ochrony. Przykładowo ataki typu *ransomware* stanowią jedno z ważniejszych zagrożeń dla sektora ochrony zdrowia, prowadząc do poważnych i często długotrwałych zakłóceń w funkcjonowaniu placówek medycznych. Konsekwencje ataków i incydentów cyfrowych obejmują m.in. skutki finansowe (np. koszty odzyskiwania zaszyfrowanych danych czy koszty rozwoju systemów zabezpieczeń), operacyjne (np. skutki przerw w działalności), prawne i regulacyjne (np. kary i odszkodowania dla partnerów i klientów) czy w końcu strategiczne i geopolityczne (np. wpływ na bezpieczeństwo narodowe i zakłócenia w działalności sektorów istotnych dla gospodarki). Należy też zauważyć, że nie wszystkie skutki ataków są łatwo mierzalne, zwłaszcza te związane z utratą zaufania klientów, długoterminowymi konsekwencjami finansowymi w przypadku firm i instytucji czy społeczne i psychologiczne w odniesieniu do osób prywatnych.

Oficjalne informacje dotyczące skali i rodzajów cyberataków na poziomie krajów członkowskich Unii Europejskiej pochodzą głównie z corocznych raportów publikowanych przez Europejską Agencję ds. Cyberbezpieczeństwa oraz krajowych agencji i organów zajmujących się cyberbezpieczeństwem, np. we Francji – Narodowej Agencji Bezpieczeństwa Systemów Informacyjnych (Agence nationale de la sécurité des systèmes d'information – ANSSI), w Niemczech – Federalnego Urzędu ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik – BSI), a w Polsce – CERT Polska.

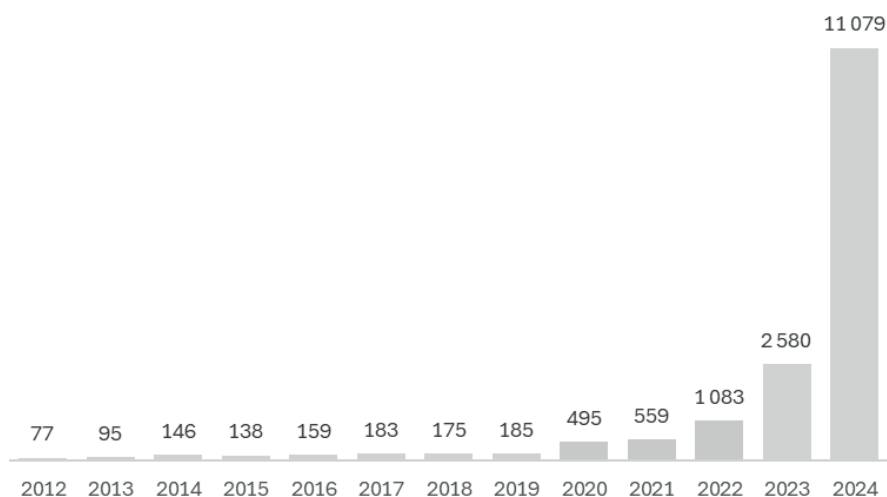
W raporcie *ENISA Threat Landscape 2024*⁴⁸ wśród najczęściej występujących rodzajów zagrożeń wskazano: zagrożenia dostępności usług – w tym ataki DoS/DDoS (41% zgłoszonych incydentów), *ransomware* (25,8%); zagrożenia dotyczące danych – w tym ataki i wycieki danych (19%); zagrożenia wykorzystujące manipulację społeczną (6%), *malware* (5,2%); zagrożenia związane z dezinformacją (1%) oraz ataki na łańcuchy dostaw (1%). Uwzględniając liczbę zgłoszonych ataków i incydentów, do najbardziej narażonych sektorów w Europie należą:

- administracja publiczna/rząd (19% zgłoszonych incydentów),

⁴⁸ *Ibidem*.

- transport (11%),
- finanse/bankowość (9%),
- usługi dla biznesu (8%),
- infrastruktura cyfrowa (8%),
- ogół społeczeństwa (8%),
- przemysł (6%).

Łączną liczbę incydentów zarejestrowanych przez ENISA w latach 2012–2024 przedstawiono na rysunku 2.



Rysunek 2. Liczba incydentów zarejestrowanych przez ENISA w latach 2012–2024

Źródło: opracowanie własne na podstawie raportów ENISA.

Nieco inny krajobraz zagrożeń prezentuje raport opublikowany przez CERT Polska⁴⁹, według którego w 2024 roku najczęściej zgłaszane były oszustwa komputerowe (55,9% zarejestrowanych incydentów), obejmujące m.in. fałszywe sklepy internetowe, oszustwa finansowe, inwestycyjne (w których przestępcy poprzez elektroniczne środki komunikacji namawiają swoje ofiary do inwestycji w nieistniejące przedsięwzięcia bądź zakupu takich walorów, jak kryptowaluty, złoto, dzieła sztuki), a także wyłudzenia środków finansowych od osób prywatnych i instytucji (np. wykorzystując mechanizmy umożliwiające fałszowanie tożsamości). Drugim rodzajem incydentów pod względem liczby zgłoszeń były próby wyłudzenia poufnych danych, np. loginu i hasła do poczty,

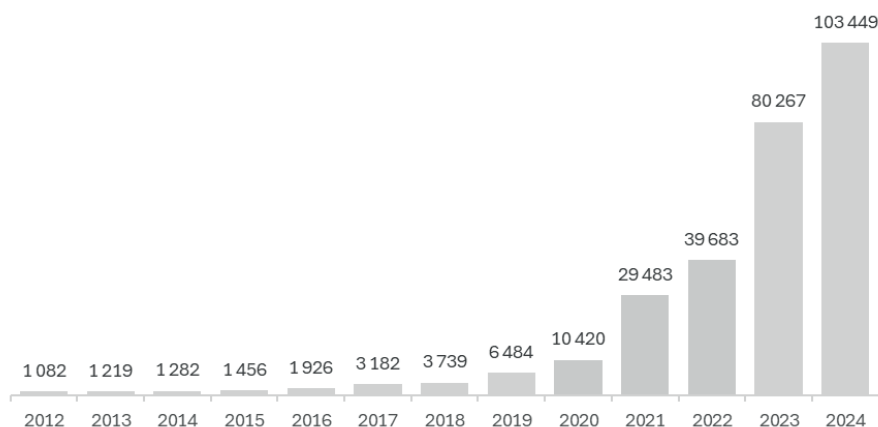
⁴⁹ *Krajobraz bezpieczeństwa polskiego Internetu w 2024 roku*, 2025, https://cert.pl/uploads/docs/Raport_CP_2024.pdf (25.04.2025).

strony banku, portalu społecznościowego czy innej usługi online (*phishing*), które stanowiły 38,8% zarejestrowanych unikalnych incydentów⁵⁰. Kolejne miejsca w rankingu liczby zarejestrowanych incydentów w 2024 roku przypadły: szkodliwemu oprogramowaniu (1,8%), podatnościom wykrytym w usługach cyfrowych (1,6%) oraz publikacji obraźliwych i nielegalnych treści (0,7%). Łączna liczba incydentów w 2024 roku wzrosła w porównaniu z 2023 rokiem o 29%.

Biorąc pod uwagę liczbę incydentów zarejestrowanych w poszczególnych sektorach gospodarki, w Polsce najbardziej narażone były:

- infrastruktura rynków finansowych (42,6%),
- handel hurtowy i detaliczny (17,7%),
- media (12,9%),
- poczta i usługi kurierskie (5%),
- energetyka (4,5%),
- infrastruktura cyfrowa (3,9%),
- osoby fizyczne (2,6%),
- bankowość (2,5%).

Łączną liczbę incydentów zarejestrowanych przez CERT Polska w latach 2012–2024 przedstawiono na rysunku 3.



Rysunek 3. Liczba incydentów zarejestrowanych przez CERT Polska w latach 2012–2024

Źródło: opracowanie własne na podstawie raportów CERT Polska.

⁵⁰ W 2024 r. do CERT Polska wpłynęło 600 990 zgłoszeń, które zostały przeanalizowane. Na ich podstawie zarejestrowano 103 449 unikalnych incydentów bezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na cyberbezpieczeństwo.

Przedstawione na rysunkach 2 i 3 dane obrazują gwałtowny wzrost liczby incydentów bezpieczeństwa, jaki widoczny jest w Polsce i Europie od 2020 roku. Należy jednak podkreślić, że z uwagi na różnice w taksonomii incydentów stosowanej przez ENISA i CERT Polska, metodologii wykorzystywanej do zbierania danych oraz tworzenia corocznych raportów, a także różnice w zakresie podmiotów objętych obowiązkiem zgłaszania incydentów dane dotyczące liczby incydentów nie mogą być bezpośrednio ze sobą porównywane.

3.2. Ewolucja zagrożeń spowodowana zmianami technologicznymi

Ewolucja zagrożeń cyfrowych jest ściśle związana z dynamicznym rozwojem technologicznym, który obejmuje niemal wszystkie sfery życia społecznego, gospodarczego oraz działalności administracji publicznej. Zmiany w tym obszarze istotnie wpływają zarówno na funkcjonowanie współczesnych społeczeństw, jak i na metody i narzędzia wykorzystywane przez cyberprzestępców. Wraz z upowszechnieniem się nowych rozwiązań technologicznych pojawiają się zupełnie nowe produkty i usługi, które z jednej strony tworzą nowe możliwości dla producentów i użytkowników, ale jednocześnie zwiększają powierzchnię ataków, otwierają nowe drogi i wektory ataków oraz umożliwiają cyberprzestępcom tworzenie coraz skuteczniejszych narzędzi służących przełamaniu zabezpieczeń.

Tempo zmian, jakie obserwuje się w obszarze nowych technologii, można określić jako bezprecedensowe, a wśród najważniejszych trendów, jakie obecnie i w najbliższej przyszłości będą wpływać na krajobraz cyberzagrożeń, można bez wątpienia zaliczyć rozwój sztucznej inteligencji i uczenia maszynowego, Internetu Rzeczy, technologii chmurowych oraz kwantowych.

Sztuczna inteligencja i uczenie maszynowe

Rozwój sztucznej inteligencji (AI) oraz uczenia maszynowego (ML) znacząco zmienia charakter współczesnych cyberzagrożeń, umożliwiając cyberprzestępcom tworzenie bardziej zaawansowanych narzędzi, automatyzację i personalizację ataków oraz wyszukiwanie podatności i skuteczniejsze omijanie zabezpieczeń. Chociaż rozwiązania wykorzystujące sztuczną inteligencję i uczenie maszynowe są rozwijane z myślą o usprawnieniu procesów analitycznych i automatyzacji złożonych zadań, zostały szybko zaadaptowane

przez osoby i grupy działające w celach przestępczych. W konsekwencji wpływają na wzrost liczby i skuteczności ataków, a także ich złożoność oraz trudność wykrycia⁵¹.

Jednym z obszarów, w których AI jest wykorzystywana przez cyberprzestępców, jest tworzenie realistycznych treści z wykorzystaniem modeli językowych oraz narzędzi generujących obrazy i filmy. Dzięki modelom generatywnej sztucznej inteligencji możliwe jest tworzenie sfałszowanych nagrań audio i wideo (ang. *deep fake*), które mogą być wykorzystywane do szantażu, dezinformacji czy działań podważających zaufanie do instytucji publicznych i procesów demokratycznych.

Realistyczne i przekonujące treści wytworzone z wykorzystaniem narzędzi AI pozwalają szybko i niewielkim kosztem tworzyć trudne do rozpoznania fałszywe wiadomości e-mail (omijające filtry antyspamowe) lub strony internetowe wykorzystywane w spersonalizowanych kampaniach phishingowych. Sztucznie wygenerowane treści wzmacniają skuteczność inżynierii społecznej, przez co ataki socjotechniczne stają się trudniejsze do wykrycia i znacznie bardziej skuteczne.

Z kolei wykorzystanie algorytmów uczenia maszynowego pozwala analizować ogromne ilości danych pochodzących z różnych źródeł (w tym np. mediów społecznościowych czy informacji publikowanych na stronach internetowych), aby identyfikować wzorce zachowań, preferencje i słabe punkty potencjalnych ofiar lub tworzyć złośliwe oprogramowanie zdolne do modyfikacji własnego działania na podstawie wcześniejszych niepowodzeń.

Wśród możliwości wykorzystania AI przez cyberprzestępców wskazuje się również na jej potencjał związany z automatyzacją procesów wyszukiwania wrażliwych danych i luk w systemach zabezpieczeń. Algorytmy są w stanie szybko skanować sieci i oprogramowanie w poszukiwaniu słabych punktów, a następnie koordynować skomplikowane ataki, dostosowując się przy tym dynamicznie do zidentyfikowanych mechanizmów obronnych. Ocenia się, że dzięki wykorzystaniu narzędzi AI/ML szybkość prowadzenia ataków może wzrosnąć nawet 100-krotnie. W 2021 roku średni czas potrzebny do kradzieży danych z organizacji wynosił 9 dni. W 2023 roku były to już zaledwie 2 dni. W 2025 roku czas potrzebny do kradzieży danych może spaść do zaledwie 25 minut⁵².

Wykorzystanie algorytmów i narzędzi AI przyczynia się także do obniżenia barier wejścia dla cyberprzestępców, umożliwiając osobom o niskich kompetencjach technicznych lub nawet nieposiadającym żadnych kompetencji (ang. *script kiddies*) tworzenie

⁵¹ M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitsoff, B. Filar, H. Roff, G. Allen, J. Steinhardt, C. Flynn, S. O'Heigeartaigh, S. Beard, H. Belfield, S. Farquhar, D. Amodei, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018.

⁵² *Najważniejsze cyberzagrożenia na 2025 r. Wyzwaniem komputery kwantowe*, <https://businessinsider.com.pl/technologie/nowe-technologie/najwazniejsze-cyberzagrozenia-na-2025-r-wyzwaniem-komputery-quantowe/ph05lhe> (12.04.2025).

narzędzi, wyszukiwanie podatności i prowadzenie skutecznych ataków na systemy informatyczne.

Potencjalnie negatywne skutki dla poziomu cyberbezpieczeństwa mogą mieć też ułatwienia, jakie oferują modele generatywne w obszarze programowania. Coraz większe możliwości, jakie mają duże modele językowe (np. ChatGPT, DeepSeek czy Claude) oraz dedykowane narzędzia wykorzystujące AI w zakresie kodowania, umożliwiają osobom bez specjalistycznej wiedzy technicznej tworzenie aplikacji, stron internetowych, usług chmurowych czy rozwiązań informatycznych automatyzujących zadania. Stworzone w ten sposób rozwiązania ze względu na błędy popełnione przez AI oraz brak odpowiedniej wiedzy i doświadczenia użytkownika mogą charakteryzować się niskim poziomem bezpieczeństwa i być podatne na ataki.

W kontekście rosnącego wykorzystania algorytmów AI oraz ML w autonomicznych pojazdach i różnego rodzaju urządzeniach podkreślić należy również ryzyko, jakie może wynikać z błędów w działaniu tych systemów, a także z bezprawnej ingerencji czy celowej manipulacji algorytmami. Konsekwencje incydentów w tym obszarze mogą obejmować zagrożenia bezpieczeństwa użytkowników i osób postronnych, zakłócenie działania infrastruktury krytycznej, naruszenia prywatności, a w skrajnych przypadkach nawet katastrofy z udziałem ludzi.

Zagrożenia dla cyberbezpieczeństwa wynikające z rozwoju sztucznej inteligencji nie ograniczają się jedynie do zakłócenia działania czy możliwości jej użycia przez atakujących, ale obejmują również ryzyko związane z samym procesem jej rozwoju i zastosowania. Wskazuje się w tym zakresie np. na problemy dotyczące bezprawnego wykorzystania zbiorów danych w procesie trenowania (naruszenie praw autorskich) czy też wykorzystanie danych o niskiej jakości, zawierających treści nieprawdziwe, niepełne lub obciążone stereotypami i uprzedzeniami (np. dotyczącymi pochodzenia, orientacji seksualnej czy ról społecznych). Zagrożenie stanowi też brak przejrzystości w zakresie pozyskiwania i przetwarzania (w tym w celu dalszego trenowania modeli) danych użytkowników korzystających z AI oraz potencjalne konsekwencje wycieku tych danych.

Rozwój Internet Rzeczy i systemów sterowania przemysłowego

Internet Rzeczy wskazywany jest jako jeden z kluczowych elementów cyfryzacji światowej gospodarki, jednak jego szybki rozwój skutkuje wzrostem liczby podatnych na ataki urządzeń, które mogą być wykorzystane do przeprowadzania cyberataków, tworzenia botnetów, kradzieży danych, naruszania prywatności użytkowników czy też zakłócania funkcjonowania infrastruktury krytycznej⁵³. Szacunki dotyczące liczby urządzeń IoT na

⁵³ F. Meneghello, C. Matteo Daniel. Zucchetto, M. Polese, A. Zanella, *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*, „IEEE Internet of Things Journal” 2019, vol. 6, issue 1.

świecie nie są precyzyjne i wahają się od kilkunastu do kilkudziesięciu miliardów takich urządzeń w 2025 roku⁵⁴ przy corocznym wzroście o 13–15%⁵⁵.

Ogromna liczba i różnorodność urządzeń IoT (od prostych czujników po nowoczesne samochody czy systemy inteligentnych miast) tworzy coraz bardziej skomplikowany i rozległy ekosystem⁵⁶ z rosnącą liczbą podatności i wektorów ataków. Urządzenia IoT kierowane na rynek konsumencki stają się łatwym celem dla atakujących ze względu na ich często słabe zabezpieczenia, ograniczone możliwości aktualizacji oprogramowania i niewielką świadomość użytkowników na temat potencjalnych zagrożeń. Wiele z urządzeń Internetu Rzeczy jest projektowanych z naciskiem na funkcjonalność i niski koszt oraz działa w publicznej sieci Internet, co czyni je bardziej podatnymi na ataki niż inne systemy informatyczne.

Znacznie poważniejsze zagrożenie stanowią ataki ukierunkowane na systemy sterowania przemysłowego (ICS), kluczowe dla funkcjonowania wielu branż i sektorów, w tym infrastruktury krytycznej. Tradycyjnie systemy te charakteryzowały się izolacją od innych systemów oraz sieci publicznych, jednak potrzeba zdalnego monitorowania, analizy danych i integracji z korporacyjnymi systemami informacyjnymi doprowadziła do stopniowego otwierania ich na zewnętrzne połączenia sieciowe. Otwieranie dostępu bardzo często nie jest powiązane z wdrażaniem zaawansowanych mechanizmów zabezpieczeń, co w połączeniu z niewystarczającą separacją poszczególnych systemów umożliwia cyberprzestępcom rozpowszechnianie szkodliwego oprogramowania (np. *ransomware*) i rozszerzanie obszarów objętych atakiem.

Konwergencja systemów IoT, ICS oraz innych systemów informatycznych wspierających funkcjonowanie organizacji powoduje, że udane ataki na konsumenckie i przemysłowe systemy mogą mieć bardzo szerokie konsekwencje, obejmujące nie tylko zakłócenia w działaniu systemów komputerowych, ale także fizyczne uszkodzenia sprzętu i infrastruktury oraz zagrożenia dla zdrowia i życia ludzi. W lutym 2025 roku polskie Ministerstwo Cyfryzacji opublikowało komunikat informujący o rosnącej liczbie ataków na przemysłowe systemy sterowania oraz wpływie na działanie fizycznych systemów i konsekwencjach dla użytkowników usług oferowanych przez takie systemy⁵⁷. Należy

⁵⁴ R. Rodseth, M. Mayer, J. Rothkugel, *IIoT at a Tipping Point*, 2024, <https://activantcapital.com/research/iiot-at-a-tipping-point> (12.04.2025).

⁵⁵ *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*, <https://iot-analytics.com/number-connected-iot-devices/> (12.04.2025).

⁵⁶ Zob. szerzej o przykładzie ekosystemu: A. Drab-Kurowska, A. Budziewicz-Guźlecka, *The Digital Post Ecosystem – Example of Poland in the Context of Research*, „Sustainability” 2021, no. 13(5), 2550.

⁵⁷ Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa ws. ataków na przemysłowe systemy sterowania, <https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-ws-a-takow-na-przemyslowe-systemy-sterowania3> (15.04.2025).

się spodziewać, że skala zagrożeń będzie nadal wzrastać wraz z postępującą cyfryzacją i automatyzacją procesów przemysłowych oraz rosnącą liczbą urządzeń IoT.

Technologie chmurowe

Technologia chmurowa (ang. *cloud computing*) stanowi obecnie jeden z najdynamiczniej rozwijających się obszarów sektora IT, znacząco zmieniając sposób przechowywania, przetwarzania oraz zarządzania danymi. Szereg korzyści, wśród których wymienić można elastyczny i skalowalny dostęp do zasobów (wirtualne serwery, moc obliczeniowa, przestrzeń dyskowa, systemy zarządzania bazami danych), zmniejszenie kosztów utrzymania sprzętu, możliwość szybkiego wdrażania nowych usług i aplikacji oraz wysoki poziom dostępności danych niezależnie od lokalizacji użytkownika, spowodowało, że rozwiązania oparte na chmurze obliczeniowej są coraz częściej wykorzystywane przez organizacje i przedsiębiorstwa z wielu sektorów, m.in. finansowego, edukacyjnego, medycznego oraz publicznego⁵⁸. Ocenia się, że w krajach Unii Europejskiej w 2023 roku średnio 42,5% przedsiębiorstw kupowało usługi *cloud computing*. W Polsce odsetek ten był nieco wyższy i wynosił ponad 55%. Najwyższy udział obserwuje się w krajach skandynawskich, gdzie osiąga on 70–80%⁵⁹. Zarówno globalny, jak i europejski rynek usług chmurowych rośnie dynamicznie w tempie około 20% rocznie⁶⁰, przy czym w Polsce w roku 2023 zarejestrowano wzrost o 34%⁶¹.

Pomimo licznych zalet rozwój i popularyzacja technologii chmurowych przyczynia się do pojawienia się nowych zagrożeń związanych z cyberbezpieczeństwem, takich jak nieautoryzowany dostęp do danych, problemy z prywatnością, brak lub ograniczenie kontroli nad przechowywanymi zasobami oraz zwiększona ekspozycja na ataki sieciowe.

Szybki rozwój technologii chmurowych, duża liczba dostawców oferujących często dziesiątki usług, złożoność stosowanych rozwiązań oraz mechanizmów bezpieczeństwa stanowią coraz większe wyzwanie związane z zapobieganiem incydentom cyberbezpieczeństwa i likwidacją ich skutków. Dodatkowym problemem jest związana ze środowiskiem chmurowym koncepcja współodpowiedzialności za bezpieczeństwo, która oznacza, że odpowiedzialność za bezpieczeństwo spoczywa zarówno na dostawcy infrastruktury

58 A. Mazhar, S.U. Khan, A.V. Vasilakos, *Security in cloud computing: Opportunities and challenges*, „Information Sciences” 2015, no. 305, s. 357–383.

59 Eurostat, *Cloud computing – statistics on the use by enterprises*, 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (4.04.2025).

60 Gartner Forecasts Worldwide Public Cloud End-User Spending to Total \$723 Billion in 2025, <https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025> (4.04.2025).

61 Value of the Polish cloud computing market increased by 1 billion PLN in 2023, <https://www.pmrmarkexperts.com/en/news/value-of-the-polish-cloud-computing-market-increased-by-1-billion-pln-in-2023/> (4.04.2025).

i usług chmurowych, jak i na jej użytkownikach oraz klientach. W praktyce oznacza to, że incydent bezpieczeństwa może zostać spowodowany np. błędną konfiguracją po stronie dostawcy lub błędem użytkownika (np. nieprawidłowo przyznane uprawnienia w zakresie dostępu do danych). W tym kontekście znaczącym problemem staje się brak strategii rozwoju i wiedzy niezbędnej do efektywnego i bezpiecznego wykorzystania potencjału *cloud computing*. W wielu organizacjach wdrażanie usług chmurowych odbywa się często bez należytego nadzoru ze strony specjalistów ds. bezpieczeństwa, a priorytetem staje się szybkie wykorzystanie funkcjonalności kosztem bezpieczeństwa⁶².

W efekcie odsetek organizacji, które doświadczyły incydentów bezpieczeństwa związanych z usługami chmurowymi, wzrósł w 2024 roku do 61% (24% w roku 2023)⁶³. Najczęściej wskazywane obszary zagrożeń dotyczyły nieautoryzowanego dostępu (59%) i naruszeń związanych z danymi (61%)⁶⁴. Aż 96% badanych organizacji wskazuje na brak zdolności do skutecznego zarządzania ryzykiem w obszarze usług chmurowych, a jako najważniejsze bariery utrudniające podejmowanie skutecznych działań mitygujących zagrożenia wymieniano: brak świadomości pracowników w zakresie zagrożeń (41%), szybkie zmiany technologiczne (38%) i brak personelu posiadającego odpowiednie kwalifikacje (37%).

Podkreślić należy, że zagrożenia związane z technologiami chmurowymi dotyczą nie tylko wykorzystania podatności rozwiązań chmurowych czy ataków na infrastrukturę, usługi oraz dane znajdujące się w środowisku chmurowym. Przestępcy coraz częściej wykorzystują usługi chmurowe w swojej działalności. Popularność usług chmurowych, takich jak Amazon Web Services, Microsoft Azure czy Google Cloud Platform, sprawia, że ich infrastruktura jest powszechnie uznawana za zaufaną, co cyberprzestępcy wykorzystują do ukrywania infrastruktury C2 (*Command and Control*)⁶⁵, przechowywania i dystrybucji złośliwego oprogramowania, a także do organizowania kampanii phishingowych oraz przeprowadzania ataków DDoS.

Technologia kwantowa

Technologia kwantowa opiera się na zasadach mechaniki kwantowej – nauki badającej bardzo małe cząstki, takie jak elektrony czy fotony. Przedstawiana jest ona jako jeden

⁶² P. Waszczuk, *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, <https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance/> (4.04.2025).

⁶³ Check Point, *Cloud Security Report 2024*, <https://engage.checkpoint.com/2024-cloud-security-report/> (6.04.2025).

⁶⁴ Trend Micro, *Cloud Security Report 2024*, <https://www.trendmicro.com/explore/cloud-security-eu> (6.04.2025).

⁶⁵ *Command and Control* to termin odnoszący się do infrastruktury lub mechanizmu umożliwiającego cyberprzestępcom zdalne zarządzanie zainfekowanymi systemami, urządzeniami lub sieciami.

z filarów głębokiej transformacji w dziedzinie informatyki i komunikacji, jaka nastąpi w najbliższych latach. Jednym z praktycznych efektów tej transformacji, która określana jest mianem rewolucji kwantowej, będzie opracowanie komputerów, które będą w stanie rozwiązywać skomplikowane problemy (np. z obszaru kryptografii, komunikacji, problemów optymalizacyjnych, modelowania skomplikowanych zjawisk czy uczenia maszynowego) szybciej niż najpotężniejsze superkomputery⁶⁶. Należy jednak podkreślić, że z uwagi na szczególne ograniczenia tej technologii komputery kwantowe nie zastąpią klasycznych komputerów, a staną się ich uzupełnieniem, umożliwiając rozwiązywanie najbardziej złożonych zadań i problemów.

Technologia, która otwiera nowe horyzonty w nauce i sferze biznesowej, stwarza jednak poważne wyzwania dla istniejącej infrastruktury cyberbezpieczeństwa. Związane są one przede wszystkim z zagrożeniem, jakie technologia kwantowa może stanowić dla mechanizmów kryptograficznych. Bezpieczeństwo obecnie stosowanych metod szyfrowania opiera się na trudności rozwiązania określonych problemów matematycznych przez komputery. Algorytmy kwantowe będą w stanie rozwiązać te problemy w czasie wielokrotnie krótszym, czyniąc obecne zabezpieczenia praktycznie bezużytecznymi⁶⁷. W praktyce może to oznaczać poważne problemy związane z bezpieczeństwem w takich obszarach, jak:

- a) komunikacja i przetwarzanie danych – poprzez złamanie dostępnych obecnie metod szyfrowania (możliwość odczytywania zaszyfrowanych danych);
- b) podpisy cyfrowe i certyfikaty – podważenie wiarygodności poprzez złamanie stosowanych w tym obszarze zabezpieczeń kryptografii asymetrycznej i możliwość podszywania się pod inne podmioty;
- c) technologia *blockchain* – poprzez złamanie mechanizmów wykorzystywanych do zabezpieczenia i podpisywania transakcji (możliwość fałszowania transakcji kryptowalutowych i podważenie zaufania do rozwiązań opartych na *blockchain*);
- d) konsumenckie i przemysłowe systemy sterowania – poprzez przełamanie zabezpieczeń chroniących komunikację i przesyłane polecenia (możliwość przejęcia kontroli nad urządzeniami IoT/ICS).

Chociaż obecnie ta technologia znajduje się na etapie badań, to eksperci ds. bezpieczeństwa (w tym amerykańska Narodowa Agencja Bezpieczeństwa) podkreślają, że zagrożenia mogą pojawiać się jeszcze przed osiągnięciem przez nią pełnej funkcjonalności⁶⁸.

⁶⁶ T. Kulas, *Komputery kwantowe zmieniają świat biznesu. Jak przygotować firmę?*, „MIT Sloan Management Review Polska”, 19 sierpnia 2019, <https://mitsmr.pl/b/komputery-quantowe-zmienia-swiat-biznesu-jak-przygotowac-firme/P1Im4TmHH> (7.04.2025).

⁶⁷ EITM, *The Rise of Quantum Computing: What It Means for Cybersecurity*, 2024, <https://www.eimt.edu.eu/the-rise-of-quantum-computing-what-it-means-for-cybersecurity> (7.04.2025).

⁶⁸ *Quantum of Lies*, <https://www.kaspersky.com/blog/quantum-cryptography-2024-hype/52884/> (7.04.2025).

Jednym ze scenariuszy jest wykorzystanie strategii „zbierz teraz, odszyfruj później” (ang. *harvest now, decrypt later*), w której przestępcy lub aktorzy finansowani przez rządy gromadzą już teraz zaszyfrowane treści, aby móc uzyskać do nich dostęp, gdy odpowiednia technologia stanie się dostępna.

Już obecnie największe firmy technologiczne, jak Amazon, IBM, Google i Microsoft, uruchomiły komercyjne usługi chmurowe wykorzystujące obliczenia kwantowe, a szacowany czas, w jakim stworzone zostaną w pełni funkcjonalne komputery kwantowe, to 5 do 10 lat⁶⁹.

Należy zauważyć, że wskazane czynniki technologiczne to bardzo ważne, ale nie jedyne elementy, które w najbliższym czasie będą oddziaływać na globalny poziom cyberbezpieczeństwa. Wpływ na kształtowanie i rozwój cyberzagrożeń będą miały również zjawiska i trendy o charakterze politycznym, społecznym i ekonomicznym (rynkowym). Wśród takich czynników należy wskazać przede wszystkim:

1. Wzrost napięć i konfliktów międzynarodowych oraz polaryzacji społecznej – konflikty i napięcia geopolityczne sprzyjają intensyfikacji aktywności państwowych i niepaństwowych grup cyberprzestępczych. Dotyczy to np. wzrostu liczby prowadzonych przez podmioty sponsorowane przez państwa ataków typu APT, których celem jest infrastruktura krytyczna, instytucje rządowe, sektor obronny i energetyczny czy systemy wyborcze. Z kolei postępująca polaryzacja społeczna przyczynia się do zwiększenia częstotliwości i skuteczności kampanii dezinformacyjnych oraz tzw. operacji wpływu. Podziały społeczne zwiększają podatność na fałszywe narracje, destabilizację polityczną i obniżanie zaufania do instytucji publicznych⁷⁰.
2. Ewolucja cyberprzestępczości – grupy cyberprzestępcze coraz częściej działają jak zorganizowane przedsiębiorstwa: korzystają z outsourcingu usług, prowadzą kampanie marketingowe i oferują wsparcie techniczne. Rośnie też popularności usług świadczonych przez wyspecjalizowane grupy przestępcze, polegających na realizacji na zlecenie ataków (np. typu *ransomware*, DDoS) czy łamaniu zabezpieczeń i haseł. Działania takie określane są terminem „cyberprzestępczość jako usługa” (ang. *Crime-as-a-Service* – CaaS) i są oferowane w modelu biznesowym zbliżonym do usług chmurowych, co ułatwia dostęp do cyberataków osobom bez specjalistycznych kompetencji technicznych⁷¹.

⁶⁹ KPMG, *Quantum is coming – and bringing new cybersecurity threats with it*, <https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html> (7.04.2025).

⁷⁰ C. Wardle, H. Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe 2017, <https://rm.coe.int/information-disorder-report-november-2017/1680764666> (10.04.2025).

⁷¹ Europol, *Internet Organised Crime Threat Assessment*, 2023, <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023> (10.04.2025).

3. Rozwój modeli pracy zdalnej i hybrydowej – wraz z rozwojem telepracy i elastycznych form zatrudnienia powiększeniu ulegają potencjalne powierzchnie ataku. Praca w środowisku domowym, wykorzystanie własnych komputerów i infrastruktury sieciowej (często pozbawionych wystarczających mechanizmów zabezpieczeń) oraz niska świadomość zagrożeń wśród pracowników wpływają na zwiększenie podatności organizacji na cyberzagrożenia⁷².
4. Zmiany społeczne i demograficzne – luka kompetencyjna w zakresie kompetencji cyfrowych oraz nierównomierny społecznie i geograficznie poziom tych kompetencji sprawiają, że osoby o niedostatecznych kompetencjach w zakresie nowych technologii i cyberhigieny są znacznie bardziej podatne na ataki phishingowe, oszustwa internetowych czy nieświadome rozpowszechnianie nieprawdziwych treści i złośliwego oprogramowania. Problemem jest też utrzymujące się zjawisko niedoboru specjalistów ds. cyberbezpieczeństwa, co utrudnia organizacjom skuteczne reagowanie na zagrożenia i skutkuje ograniczoną odpornością zarówno sektora prywatnego, jak i publicznego na coraz bardziej zaawansowane formy cyberprzestępczości⁷³.

3.3. Techniki i narzędzia ograniczania cyberzagrożeń

W systemach cyberbezpieczeństwa techniczne rozwiązania są jednym z filarów, na których opiera się kompleksowa ochrona danych i infrastruktury teleinformatycznej. Pozostałe filary stanowią aspekty organizacyjno-prawne oraz kompetencje i edukacja użytkowników.

O ile regulacje prawne, procedury zarządzania bezpieczeństwem czy działania podnoszące świadomość i kompetencje użytkowników są fundamentem trwałości systemu, to rozwiązania techniczne pełnią funkcję operacyjną – są odpowiedzialne za bezpośrednie przeciwdziałanie zagrożeniom, ich wykrywanie i neutralizację, a także przywracanie sprawności systemów w przypadku incydentu. Ich znaczenie i poziom zaawansowania wzrasta wraz z rozwojem skali i poziomu skomplikowania ataków.

Współczesne rozwiązania techniczne w zakresie cyfrowego bezpieczeństwa obejmują mechanizmy zabezpieczające na różnych poziomach skomplikowania, począwszy od relatywnie prostych rozwiązań, takich jak systemy antywirusowe czy zapory sieciowe (*firewall*), aż po zaawansowane platformy oparte na sztucznej inteligencji, analizie behawioralnej i technologiach uczenia maszynowego. Zróżnicowanie technik i narzędzi zabezpieczających jest związane z koniecznością ich dostosowania do ochrony

⁷² *The Impact of Remote Work on Security and Compliance*, <https://360advanced.com/the-impact-of-remote-work-on-security-and-compliance/> (10.04.2025).

⁷³ *Closing The Cybersecurity Skills Gap: Strategies for Employers and Aspiring Professionals*, <https://www.cybrary.it/blog/closing-cybersecurity-skills-gap> (10.04.2025).

realizowanej na różnych poziomach systemów informatycznych, poczynawszy od warstwy fizycznej obejmującej sprzęt (ang. *hardware*), poprzez warstwę sieciową, systemową, aplikacyjną, aż po ochronę danych i tożsamości użytkowników.

Należy zaznaczyć, że techniczne środki ochrony nie funkcjonują w próżni, a ich skuteczność zależy w dużej mierze od integracji z procedurami zarządzania ryzykiem, stałego monitorowania, testowania oraz aktualizacji systemu. Współczesne podejście do cyberbezpieczeństwa opiera się na koncepcji *defense-in-depth* (obrony warstwowej), która zakłada zastosowanie wielu nakładających się na siebie warstw zabezpieczeń w celu ochrony systemów informatycznych, danych i infrastruktury. Jej głównym celem jest zwiększenie odporności na ataki dzięki temu, że po przełamaniu jednej warstwy zabezpieczeń atakujący napotyka kolejne zabezpieczenia, które utrudniają i wydłużają czas niezbędny do uzyskania pełnego dostępu, zwiększając tym samym szanse na powstrzymanie ataku. Przykłady warstw stosowanych w systemach informatycznych to np. zabezpieczenia związane z fizycznym dostępem (np. dostęp do serwerowni), zabezpieczenia sieciowe (*firewall*, VPN), zabezpieczenia systemowe (aktualizacje, systemy antywirusowe) i zabezpieczenia aplikacji (kontrola dostępu, uwierzytelnianie). Główne założenia warstwowej obrony obejmują m.in.:

- a) redundancję zabezpieczeń – różne mechanizmy chronią te same zasoby;
- b) zróżnicowanie – zastosowanie różnych technologii i metod (np. zapory sieciowe, systemy wykrywania włamań, kontrola dostępu, szyfrowanie danych, monitoring systemu);
- c) segmentację – ograniczenie zasięgu potencjalnego naruszenia przez dzielenie systemu na oddzielne obszary (segmenty) o różnym poziomie ochrony;
- d) bezpieczeństwo użytkownika i urządzeń końcowych – zarządzanie uprawnieniami użytkowników, stosując zasadę najmniejszych niezbędnych uprawnień, oraz zarządzanie bezpieczeństwem urządzeń, z których korzystają użytkownicy (komputery, laptopy, smartfony itp.), w celu ochrony przed infekcją czy naruszeniem danych.

Wykorzystanie zróżnicowanych technik i metod w ramach obrony warstwowej pozwala na stworzenie spójnego, wzajemnie uzupełniającego się ekosystemu zabezpieczeń, który znacząco zwiększa odporność systemu na różnorodne zagrożenia. Poniżej scharakteryzowano najważniejsze techniki i narzędzia stosowane w ograniczaniu cyberzagrożeń.

Zarządzanie tożsamością i kontrola dostępu. Autoryzacja i uwierzytelnianie stanowią podstawowe mechanizmy kontroli dostępu w systemach informatycznych. Ich głównym celem jest zagwarantowanie, że dostęp do zasobów mają wyłącznie osoby uprawnione oraz że zakres ich uprawnień jest ściśle określony i kontrolowany. Techniki te mają kluczowe znaczenie w ograniczaniu ryzyka nieautoryzowanego dostępu do zasobów, przejęcia kont, kradzieży danych oraz eskalacji uprawnień, czyli działań będących elementem wielu wektorów ataku stosowanych przez cyberprzestępców. Mechanizm

uwierzytelniania (ang. *authentication*) polega na weryfikacji tożsamości użytkownika. Tradycyjnie odbywa się to poprzez podanie loginu i hasła, jednak ze względu na podatność takich metod na ataki (np. typu *phishing*, *brute-force*⁷⁴ czy *credential stuffing*⁷⁵) coraz częściej stosuje się silniejsze mechanizmy, w tym:

1. Uwierzytelnianie dwuskładnikowe (2FA) oraz wieloskładnikowe (MFA), które wymaga co najmniej dwóch niezależnych elementów uwierzytelniających, np. loginu i hasła (jeden element uwierzytelniający) oraz aplikacji lub klucza sprzętowego (drugi element uwierzytelniający)⁷⁶.
2. Uwierzytelnianie biometryczne – coraz powszechniej stosowane w urządzeniach mobilnych i systemach korporacyjnych, opiera się na weryfikacji unikalnych cech fizjologicznych użytkownika (odcisk palca, głos, skan twarzy lub siatkówki oka).
3. FIDO2/WebAuthn – nowoczesne standardy uwierzytelniania bezhasłowego opracowane przez FIDO Alliance i W3C, których celem jest wyeliminowanie potrzeby stosowania tradycyjnych haseł na rzecz bezpieczniejszych i bardziej odpornych na ataki kluczy kryptograficznych (prywatny klucz uwierzytelniający pozostaje na urządzeniu użytkownika i nigdy nie opuszcza jego pamięci, natomiast publiczny klucz jest przechowywany po stronie serwera). Proces logowania opiera się na mechanizmie podpisu cyfrowego, który potwierdza autentyczność użytkownika bez ujawniania jakichkolwiek danych uwierzytelniających⁷⁷.

Autoryzacja (ang. *authorization*) następuje po uwierzytelnieniu i polega na przyznaniu użytkownikowi określonych uprawnień dostępu do zasobów systemu zgodnie z zasadą najmniejszych uprawnień (ang. *least privilege*). Mechanizmy autoryzacji są zwykle realizowane przez systemy kontroli dostępu, które definiują, do jakich danych lub funkcji użytkownik może uzyskać dostęp w zależności od jego roli, kontekstu działania czy przydzielonych zadań.

Wdrażanie skutecznych systemów uwierzytelniania i autoryzacji wynika nie tylko z zaleceń i dobrych praktyk, ale jest także wymogiem wielu norm i regulacji prawnych, w tym RODO, normy ISO/IEC 27001 oraz dyrektywy NIS2.

Wykrywanie i zapobieganie włamaniom. Systemy wykrywania i zapobiegania włamaniom (ang. *Intrusion Detection Systems/Intrusion Prevention Systems* – IDS/IPS) są stosowane w celu zwiększenia poziomu bezpieczeństwa sieci poprzez monitorowanie

⁷⁴ *Brute force* (czyli atak siłowy) to metoda łamania haseł lub kluczy szyfrujących poprzez testowanie wszystkich ich możliwych kombinacji. Odmianą metodą jest atak słownikowy, w którym wykorzystuje się tzw. słowniki, czyli listy najpopularniejszych haseł.

⁷⁵ *Credential stuffing* to technika ataku, w której cyberprzestępcy wykorzystują wcześniej wykradzione (np. z innego serwisu) loginy i hasła w nadziei, że ofiary używają tych samych danych logowania na różnych stronach i serwisach internetowych.

⁷⁶ NIST, SP 800-63 *Digital Identity Guidelines*, 2017, <https://doi.org/10.6028/NIST.SP.800-63-3> (12.04.2025).

⁷⁷ FIDO Authentication, *A passwordless vision*, <https://fidoalliance.org/fido2/> (12.04.2025).

ruchu sieciowego i aktywności systemów w celu identyfikacji oraz przeciwdziałania złośliwej aktywności i naruszeniom zasad bezpieczeństwa.

Zadaniem IDS jest monitorowanie ruchu sieciowego i aktywności w chronionym systemie oraz wykrywanie anomalii lub wzorców charakterystycznych dla znanych zagrożeń. IDS jest systemem pasywnym, czyli nie podejmuje działań bezpośrednio ingerujących w ruch lub system, a jedynie generuje ostrzeżenia, które mogą być analizowane przez osoby lub działy odpowiedzialne za bezpieczeństwo cyfrowe organizacji⁷⁸.

Wyróżnia się dwa podstawowe rodzaje IDS:

- a) NIDS (*Network-based IDS*) – analizują w czasie rzeczywistym ruch w całej sieci;
- b) HIDS (*Host-based IDS*) – monitorują konkretne systemy lub urządzenia końcowe (hosty), analizując np. zmiany konfiguracji, dostęp do plików systemowych itp.

IPS, w przeciwieństwie do IDS, jest systemem aktywnym, który nie tylko wykrywa, ale również automatycznie blokuje wykryte zagrożenia, zapobiegając lub minimalizując ich skutki. Działania IPS mogą obejmować np. blokowanie ruchu sieciowego czy odcinanie dostępu do zasobów lub usług. Zarówno IDS, jak i IPS wykorzystują różnorodne techniki identyfikacji zagrożeń⁷⁹:

- a) detekcję sygnaturową – polega na porównywaniu aktywności lub ruchu sieciowego z bazą znanych wzorców zagrożeń (tzw. sygnatur); jest nieskuteczna w przypadku nowych lub nietypowych zagrożeń o nieznanym wzorcu (np. ataki z wykorzystaniem podatności *zero-day*);
- b) detekcję anomalii – opiera się na analizie odchyśleń od typowych zachowań; pozwala wykrywać nowe, nieznanne wcześniej zagrożenia, jednak może generować więcej fałszywych alarmów;
- c) detekcję behawioralną – identyfikuje zagrożenia poprzez obserwację i uczenie się zachowań użytkowników oraz systemów (coraz częściej wykorzystuje algorytmy sztucznej inteligencji i uczenia maszynowego).

Wdrożenie systemu IDS/IPS pozwala nie tylko na wczesne wykrycie prób naruszenia bezpieczeństwa, ale również na skrócenie czasu potrzebnego na reakcję, a tym samym na minimalizację potencjalnych szkód. Systemy te są często zintegrowane z rozwiązaniami typu SIEM oraz SOAR, co umożliwia kompleksowe zarządzanie i automatyzację procesów reagowania na incydenty.

Zarządzanie bezpieczeństwem informacji z wykorzystaniem systemów SIEM (ang. *Security Information and Event Management*) i SOAR (ang. *Orchestration, Automation and Response*). To zaawansowane systemy umożliwiające centralne monitorowanie zdarzeń, kompleksową analizę danych oraz automatyzację procesów reagowania na

⁷⁸ M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary. Automatyka. Robotyka” 2013, R. 17, nr 2, s. 166–170.

⁷⁹ *Kompendium wiedzy – IDS i IPS*, <https://whitehats.pwr.edu.pl/research/kompendium-ids-ips/> (13.04.2025).

incydenty bezpieczeństwa w całej infrastrukturze IT organizacji. Ich głównym celem jest zapewnienie kompleksowej oceny stanu bezpieczeństwa, umożliwienie szybkiego wykrywania i reagowania na incydenty bezpieczeństwa oraz zapewnienie zgodności z przepisami i wymogami w zakresie cyberbezpieczeństwa.

SIEM pełni funkcję centralnej bazy danych gromadzącej informacje o zdarzeniach pochodzących z różnych komponentów infrastruktury IT, takich jak zapory sieciowe, IDS/IPS, serwery, systemy operacyjne, aplikacje, bazy danych, urządzenia końcowe i systemy zarządzania tożsamością⁸⁰. Podstawowe funkcje SIEM to:

- a) agregacja danych – system gromadzi dane z wielu źródeł i przekształca je do wspólnego formatu;
- b) korelacja zdarzeń – pozornie przypadkowe zdarzenia są łączone i analizowane w celu identyfikacji ukrytych powiązań i wzorców wskazujących na potencjalne zagrożenia (np. próby skanowania sieci, wielokrotnego logowania i eskalacji uprawnień);
- c) generowanie alertów i raportowanie – po wykryciu anomalii lub incydentów system umożliwia ich klasyfikację, analizę oraz raportowanie zgodnie z wymaganiami norm i regulacji (np. ISO 27001, RODO, NIS2);
- d) analiza trendów cyberbezpieczeństwa – zebrane dane pozwalają na śledzenia aktualnych trendów i zagrożeń w cyberprzestrzeni, umożliwiając organizacjom dostosowanie strategii bezpieczeństwa do nowych cyberzagrożeń.

SOAR został zaprojektowany w celu zwiększenia skuteczności i szybkości reakcji na incydenty przy jednoczesnym odciążeniu zespołów analityków bezpieczeństwa. W przeciwieństwie do SIEM, który koncentruje się na analizie danych i wykrywaniu anomalii, SOAR skupia się na reakcji operacyjnej, tj. automatyzacji reakcji na incydenty i usprawnianiu procesów bezpieczeństwa, oraz działaniach naprawczych⁸¹. Łączy różne narzędzia bezpieczeństwa, elementy systemu i dane, automatyzując działania związane z mitygacją zagrożeń. Dzięki temu znacząco upraszcza pracę zespołów bezpieczeństwa i przyspiesza reakcję na wykryte zagrożenia⁸².

Wybór pomiędzy rozwiązaniami SIEM i SOAR zależy od specyficznych potrzeb organizacji, przy czym coraz częściej są one wdrażane łącznie, jako uzupełniające się elementy systemów cyberbezpieczeństwa.

⁸⁰ *Co to jest SIEM – Security Information and Event Management? Definicja, komponenty, korzyści i wyzwania*, <https://nflo.pl/baza-wiedzy/co-to-jest-siem-security-information-and-event-management-definicja-komponenty-korzysci-i-wyzwania/> (13.04.2025).

⁸¹ *Co wybrać: SOAR czy SIEM? Różnice i czynniki ważne podczas wyboru*, <https://nflo.pl/baza-wiedzy/co-wybrac-soar-czy-siem-roznice-i-czynniki-wazne-podczas-wyboru/> (13.04.2025).

⁸² *Security Orchestration, Automation and Response (SOAR)*, <https://www.oneidentity.com/learn/what-is-soar.aspx> (13.04.2025).

Zarządzanie podatnościami i aktualizacjami. Zarządzanie podatnościami to proces identyfikacji, klasyfikacji, oceny oraz usuwania luk bezpieczeństwa w systemach komputerowych, aplikacjach i infrastrukturze sieciowej⁸³. Nowoczesne podejście do zarządzania podatnościami coraz częściej zakłada integrację z systemami klasy SIEM, SOAR oraz systemami zarządzania konfiguracją i inwentaryzacją zasobów (ang. *Configuration Management Database* – CMDB). Dzięki temu możliwa jest automatyczna reakcja na zidentyfikowane podatności (np. uruchomienie automatycznego procesu instalacji poprawki lub zablokowanie ruchu sieciowego do podatnego zasobu). Na proces zarządzania podatnościami składa się z kilka kluczowych etapów⁸⁴:

- a) wykrywanie – szczegółowa inwentaryzacja zasobów IT, skanowanie systemów, aplikacji i infrastruktury, testy penetracyjne w poszukiwaniu luk z wykorzystaniem dostępnych baz podatności, np. CVE;
- b) ocena – analiza zidentyfikowanych podatności pod kątem ryzyka, z wykorzystaniem systemów oceny, np. CVSS;
- c) priorytetyzacja – klasyfikacja podatności według poziomu zagrożenia, ze szczególnym uwzględnieniem luk o charakterze krytycznym;
- d) usuwanie podatności – implementacja poprawek, rekonfiguracja systemów lub wdrożenie innych środków zaradczych;
- e) walidacja i audyt – ponowne skanowanie w celu potwierdzenia usunięcia podatności oraz dokumentowanie działań w celu zapewnienia zgodności z procedurami i wymogami regulacyjnymi.

Wdrożenie w organizacji skutecznego procesu zarządzania lukami stanowi jeden z kluczowych elementów ochrony przed zagrożeniami typu *ransomware*, eskalacja uprawnień, zdalne wykonanie kodu czy kradzież danych.

Segmentacja sieci to praktyka dzielenia sieci komputerowej na mniejsze izolowane segmenty (podsieci)⁸⁵. Jej celem jest ograniczenie rozprzestrzeniania się zagrożeń w przypadku naruszenia bezpieczeństwa, poprawa wydajności sieci, ułatwienie zarządzania i monitorowania ruchu oraz zwiększenie ogólnego poziomu bezpieczeństwa. Może być realizowana logicznie poprzez stworzenie wirtualnych sieci lokalnych (VLAN) lub poprzez fizyczne oddzielenie elementów infrastruktury sieciowej⁸⁶.

⁸³ Zarządzanie podatnościami, <https://csirt-mon.wp.mil.pl/aktualnosci/zarządzanie-podatnosciami/> (13.04.2025).

⁸⁴ Czym jest zarządzanie podatnościami IT (Vulnerability Management) i dlaczego jest kluczowe dla cyberbezpieczeństwa?, <https://nflo.pl/baza-wiedzy/czym-jest-zarządzanie-podatnosciami-it-vulnerability-management-i-dlaczego-jest-kluczowe-dla-cyberbezpieczeństwa/> (13.04.2025).

⁸⁵ Segmentacja sieci – podstawy podstaw, <https://www.grupae.pl/segmentacja-sieci-podstawy-podstaw/> (13.04.2025).

⁸⁶ Bezpieczeństwo w sieci – Co to jest, główne zagrożenia, szyfrowanie, segmentacja sieci i polityka bezpieczeństwa, <https://nflo.pl/baza-wiedzy/bezpieczenstwo-w-sieci/#dlaczego-segmentacja-sieci-jest-wazna-dla-bezpieczenstwa> (13.04.2025).

Korzyści ze stosowania segmentacji w infrastrukturze sieciowej obejmują:

- a) ograniczenie dostępności pomiędzy różnymi grupami urządzeń (np. oddzielenie sieci biurowej od sieci urządzeń obsługujących procesy produkcyjne);
- b) zmniejszenie powierzchni ataku (np. uniemożliwienie złośliwemu oprogramowaniu swobodnego przemieszczania się w sieci);
- c) umożliwienie stosowania odmiennych polityk bezpieczeństwa dla różnych obszarów infrastruktury.

Rozwinięciem segmentacji sieci jest koncepcja mikroseparacji, dzięki której możliwa jest kontrola komunikacji nie tylko pomiędzy segmentami sieci, ale także między poszczególnymi elementami wewnątrz tych segmentów, np. pomiędzy aplikacjami, serwerami lub usługami.

Kopie zapasowe i odzyskiwanie danych. Efektywne zabezpieczanie danych organizacji obejmuje zarówno rozwiązania zapewniające możliwość odtworzenia informacji po incydentach związanych z naruszeniem danych, jak i zapobiegające ich nieautoryzowanemu wyprowadzeniu (wyciekowi). Podstawę zabezpieczenia danych stanowią kopie zapasowe (ang. *backup*), czyli duplikaty danych przechowywane w bezpiecznym miejscu, aby umożliwić ich odzyskanie w przypadku utraty, uszkodzenia lub zniszczenia. Regularne tworzenie kopii zapasowych jest kluczowym elementem umożliwiającym ochronę danych i ich szybkie przywrócenie w przypadku awarii, błędów ludzkich, ataków *ransomware* czy katastrof naturalnych⁸⁷.

Należy podkreślić, że w odniesieniu do niektórych podmiotów, szczególnie przetwarzania danych osobowych oraz ochrony systemów informatycznych w instytucjach publicznych i firmach (np. w sektorach finansowym, medycznym, telekomunikacyjnym), obowiązek wykonywania kopii bezpieczeństwa może wynikać z przepisów prawa (np. RODO, NIS2)⁸⁸. Proces tworzenia kopii zapasowych powinien obejmować takie elementy, jak:

- a) inwentaryzacja danych i zasobów podlegających backupowi – identyfikacja zasobów wymagających ochrony;
- b) ustalenie parametrów kopii zapasowych, np. maksymalny dopuszczalny czas niedostępności systemu po awarii czy maksymalna akceptowalna utrata danych mierzona w czasie, które pozwolą ustalić częstotliwość backupu i sposób jego realizacji;
- c) wybór strategii – obejmuje wybór rodzaju (np. pełny, różnicowy lub przyrostowy), formatu i harmonogramu tworzenia kopii bezpieczeństwa;

⁸⁷ Co to jest tworzenie kopii zapasowych?, <https://nflo.pl/slownik/tworzenie-kopii-zapasowych/> (13.04.2025).

⁸⁸ Co NIS2 mówi o tworzeniu kopii zapasowych?, <https://arkanet.pl/baza-wiedzy/co-nis2-mowi-o-tworzeniu-kopii-zapasowych/> (15.04.2025).

- d) określenie metody przechowywania i liczby kopii – kopie mogą być przechowywane lokalnie (w siedzibie organizacji), zdalnie (w chmurze) lub hybrydowo; dominującym modelem dotyczącym tworzenia i przechowywania kopii zapasowych jest zasada 3-2-1 oznaczająca, że organizacja powinna posiadać co najmniej trzy kopie danych, na dwóch różnych nośnikach, z jedną kopią przechowywaną poza siedzibą organizacji;
- e) zapewnienie poufności kopii zapasowej – szyfrowane backupu, aby chronić dane przed niepożądanym dostępem;
- f) testowanie procedur odzyskiwania danych – regularne testy odtwarzania kopii oraz weryfikacja, czy odzyskane dane są kompletne, poprawne i użyteczne.

Tworzenie kopii bezpieczeństwa jest integralnym elementem szerszego systemu przywracania działalności po awarii (ang. *disaster recovery* – DR), obejmującego zestaw procedur, narzędzi i zasobów technicznych, które umożliwiają odtworzenie działania systemów informatycznych po poważnej awarii lub incydencie. W odróżnieniu od systemu kopii zapasowych, DR obejmuje szerszy zakres, w tym przywracanie działania systemów operacyjnych, aplikacji, sieci oraz infrastruktury IT⁸⁹.

W kontekście rozwiązań z zakresu ochrony danych i informacji istotną rolę pełnią także systemy zapobiegania utracie danych (ang. *Data Loss Prevention* – DLP). To rozwiązania mające na celu monitorowanie, wykrywanie i blokowanie nieautoryzowanego przepływu poufnych danych poza organizację. Stanowią one skuteczne narzędzie zapobiegające kradzieżom lub wyciekom informacji w organizacjach przetwarzających dane wrażliwe, osobowe, finansowe czy informacje stanowiące tajemnicę przedsiębiorstwa⁹⁰.

Zabezpieczenia punktów końcowych (EPP/EDR) obejmują rozwiązania mające na celu ochronę urządzeń końcowych, takich jak komputery stacjonarne, laptopy, smartfony, serwery i urządzenia IoT przed różnorodnymi zagrożeniami⁹¹. Urządzenia te są często wykorzystywane jako wektory ataku w kampaniach phishingowych, atakach *ransomware*, atakach wykorzystujących złośliwe oprogramowanie, a także w atakach APT.

Wśród narzędzi służących do ochrony punktów końcowych można wyróżnić dwa podstawowe systemy:

1. Platformy ochrony punktów końcowych (ang. *Endpoint Protection Platform* – EPP) to rozwiązania, których celem jest zapobieganie infekcjom oraz eliminowanie znanych zagrożeń przed ich wykonaniem na urządzeniu końcowym. Podstawowe funkcje EPP obejmują identyfikację i ochronę przed złośliwym oprogramowaniem, ochronę

⁸⁹ What is a Disaster Recovery Plan?, <https://cloud.google.com/learn/what-is-disaster-recovery> (15.04.2025).

⁹⁰ Czym jest ochrona przed utratą danych (DLP)?, <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-data-loss-prevention-dlp> (15.04.2025).

⁹¹ M. Ofir Geveye, *Protecting Endpoints in an Evolving Threat Landscape*, 2024, <https://www.centraleyes.com/protecting-endpoints-in-an-evolving-threat-landscape/> (15.04.2025).

przed phishingiem i złośliwymi stronami internetowymi, integrację z systemami szyfrowania danych. System EPP działa w sposób prewencyjny, a jego celem jest wykrycie i zablokowanie znanych zagrożeń.

2. System wykrywania i reagowania na punktach końcowych (ang. *Endpoint Detection and Response* – EDR) to bardziej zaawansowane rozwiązania, które zapewniają ciągłe monitorowanie i analizę aktywności w punktach końcowych w celu wykrywania takich zagrożeń, jak ataki, *exploity*, *zero-day* czy APT. W odróżnieniu od systemów EPP, które koncentrują się na blokowaniu znanych zagrożeń, EDR posiada zdolność wykrywania nieznanych wcześniej zagrożeń oraz umożliwia szczegółowe badanie incydentów. Wśród możliwości systemów EDR wymienić można: stałe monitorowanie i rejestrowanie aktywności w punktach końcowych, analizę danych w celu wykrycia podejrzanej aktywności, automatyczne działania powstrzymujące zagrożenia, wysyłanie ostrzeżeń do administratorów systemu oraz możliwość szczegółowej analizy incydentu i określenia jego zakresu (*post factum*). Systemy EDR są często integrowane z SIEM i SOAR, co umożliwia kompleksową identyfikację zagrożeń i szybsze reagowanie na incydenty.

Ponieważ techniczna sfera cyberbezpieczeństwa rozwija się bardzo dynamicznie i obejmuje szerokie spektrum technologii i narzędzi, które wspierają ochronę systemów informatycznych na różnych poziomach, przedstawione rozwiązania obejmują jedynie najważniejsze i najczęściej stosowane techniczne środki ochrony w zakresie cyberbezpieczeństwa.

Kompetencje i edukacja cyfrowa jako kluczowe elementy systemu cyberbezpieczeństwa w Polsce

Cyberbezpieczeństwo i cyberodporność we współczesnym świecie opierają się na szeregu wzajemnie powiązanych elementów, wśród których ogromne znaczenie przypisuje się kompetencjom oraz świadomości zagrożeń w obszarze cyfrowym. Szybko postępująca cyfryzacja oraz coraz bardziej złożony krajobraz zagrożeń cyfrowych wymagają nie tylko stworzenia ram prawnych i organizacyjnych, wykorzystania zaawansowanych rozwiązań technicznych i procedur, ale także powszechnego zrozumienia i stosowania zasad związanych z cyberbezpieczeństwem przez wszystkich obywateli.

Już w 1975 roku w przełomowej publikacji poświęconej ochronie informacji w systemach komputerowych¹ wskazano dziesięć podstawowych zasad bezpieczeństwa. Wśród nich znalazły się trzy, które – obok aspektów technicznych – uwzględniały również czynniki psychologiczne i ekonomiczne. Zasady te podkreślały, że mechanizmy bezpieczeństwa powinny być psychologicznie akceptowalne dla użytkowników, którzy mają z nich korzystać. Użytkownicy indywidualni i organizacje jako całość powinni mieć do czynienia z możliwie jak najmniejszą liczbą różnych mechanizmów zabezpieczających, a koszty przełamania zabezpieczeń muszą przewyższać potencjalne korzyści dla atakującego.

Pomimo tych wczesnych i trafnych obserwacji przez kolejne dekady rozwój bezpieczeństwa komputerowego koncentrował się niemal wyłącznie na aspektach technicznych. Główny nacisk kładziono na ochronę systemów informatycznych oraz infrastruktury komunikacyjnej odpowiedzialnych za przechowywanie i przesyłanie danych. Ludzie byli traktowani jako elementy systemu, których zachowanie można określić za pomocą ustalonych zasad i kontrolować za pomocą mechanizmów bezpieczeństwa i ewentualnych sankcji².

¹ J.H. Saltier, M.D. Schroeder, *Protection of information in computer systems*, „IEEE” 1975, no. 3(12).

² ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2019, <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity> (15.04.2025).

Wraz z upływem czasu podejście takie okazało się nieskuteczne, a wyniki badań wykazały, że bezpieczeństwo całego systemu zależy od najsłabszego ogniwa, którym bardzo często jest człowiek i podejmowane przez niego działania lub też brak działań (zaniechania)³. Użytkownicy systemów i usług komputerowych z uwagi na braki wiedzy i motywacji często ignorują ostrzeżenia⁴, a także omijają zasady i mechanizmy ustalone w celu podniesienia poziomu cyberbezpieczeństwa (np. w zakresie tworzenia bezpiecznych haseł czy szyfrowania wrażliwych danych)⁵. Dodatkowo niezajomość zagrożeń i konsekwencji u użytkowników, ale też twórców systemów informatycznych czy aplikacji, prowadzi do błędnego przekonania o nadmiernie wysokich kosztach zabezpieczeń, a co za tym idzie – obniżania poziomu lub rezygnacji z zabezpieczeń np. na korzyść ergonomii czy funkcjonalności.

Dostrzeżenie takich zjawisk przyczyniło się do zwiększenia świadomości tego, że techniczne środki cyberbezpieczeństwa nie istnieją w próżni i muszą opierać się na ludziach i działać z nimi w harmonii. Wiedza i umiejętności społeczeństwa oraz odpowiednia do zapotrzebowania rynkowego liczba wykwalifikowanych specjalistów IT zajmujących się cyberbezpieczeństwem stają się obecnie podstawą budowania systemowej odporności, wpływając bezpośrednio na możliwość minimalizacji skutków incydentów i ataków o charakterze cyfrowym.

Badania prowadzone na poziomie europejskim oraz poszczególnych krajów członkowskich⁶ wskazują, że pomimo wzrastającej świadomości zagrożeń cyfrowych wśród mieszkańców Unii Europejskiej poziom kompetencji w tym zakresie pozostaje zróznicowany i niewystarczający, zwłaszcza wśród takich grup demograficznych, jak osoby starsze, mieszkańcy obszarów wiejskich oraz kobiety. Te grupy szczególnie często narażone są na negatywne konsekwencje luk kompetencyjnych, które ograniczają ich pełne uczestnictwo w społeczeństwie cyfrowym. Jednocześnie zauważalny jest spadek zaufania Europejczyków do własnych zdolności ochrony przed cyberzagroženiami, co może świadczyć o rosnącej świadomości zagrożeń oraz potrzebie intensyfikacji działań edukacyjnych.

Opracowanie skutecznych rozwiązań systemowych powinno obejmować zarówno analizę aktualnego stanu kompetencji obywateli, jak i tworzenie programów edukacyjnych dostosowanych do specyfiki i potrzeb różnych grup społecznych. Odpowiedzią na

³ A. Whitten, D. Tygar, *Why Johnny can't encrypt: A usability evaluation of pgp 5.0* [w:] *Proceedings of the 8th conference on USENIX Security Symposium*, vol. 8 (SSYM'99), USENIX Association, USA 1999.

⁴ C. Herley, *So long, and no thanks for the externalities: the rational rejection of security advice by users*. *Proceedings of the New Security Paradigms Workshop (NSPW)*, ACM 2009.

⁵ A. Adams, M.A. Sasse, *Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures*, „Communications of the ACM” 1999, no. 42(12), s. 40–46.

⁶ ENISA, *2024 Report on the State of the Cybersecurity in the Union*, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (18.04.2025).

wskazane wyzwania powinno być też wypracowanie nowoczesnych modeli zarządzania cyberbezpieczeństwem, opartych na współdziałaniu instytucji państwowych, sektora prywatnego oraz obywateli, co zapewni spójność i kompleksowość podejmowanych działań.

4.1. Świadomość i kompetencje Polaków w zakresie cyberbezpieczeństwa – wyniki badań empirycznych

Metodyka badania

Badanie zrealizowano w okresie lipiec–sierpień 2024 roku na ogólnopolskiej próbie internautów. Jego celem było zebranie opinii respondentów na temat świadomości, wiedzy i umiejętności w zakresie cyberbezpieczeństwa.

W celu pozyskania danych empirycznych dotyczących poziomu wiedzy, postaw oraz praktyk związanych z cyberbezpieczeństwem przeprowadzono badanie z wykorzystaniem metody CAWI (ang. *Computer-Assisted Web Interview*). Jest to metoda gromadzenia danych, w której respondenci samodzielnie wypełniają kwestionariusz ankiety za pośrednictwem Internetu. Jako jedna z odmian badań ilościowych umożliwia dotarcie do szerokiego grona uczestników w relatywnie krótkim czasie oraz sprzyja standaryzacji procesu pomiaru⁷.

Jako narzędzie badawcze wykorzystano formularz ankietowy obejmujący dziewięć pytań, w tym cztery pytania jednokrotnego wyboru, jedno pytanie wielokrotnego wyboru oraz cztery pytania wielopunktowe (wieloitemowe). Formularz ankiety został przedstawiony w załączniku 1.

Próba badawcza

Próba badawcza została dobrana z użyciem losowania warstwowego dwustopniowego. Przed losowaniem badani byli warstwowani według województw, a następnie w ramach województw według klasy miejscowości zamieszkania z wyróżnieniem dużych miast (powyżej 100 tys. mieszkańców), średnich miast (20–100 tys. mieszkańców), małych miast (poniżej 20 tys. mieszkańców) oraz wsi. W losowaniu warstwowym zastosowano alokację proporcjonalną na poziomie województw stosownie do liczby mieszkańców powyżej 18. roku życia oraz na poziomie klasy miejscowości zamieszkania proporcjonalnie do liczby gmin odpowiednich wielkości.

⁷ R.D. Fricker, M. Schonlau, *Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature*, „Field Methods” 2002, no. 14(4), s. 347–367.

Populację badania stanowiły osoby w wieku 18–65 lat mieszkające w Polsce. Zrealizowano łącznie 1108 wywiadów. Struktura próby jest zgodna ze strukturą populacji generalnej, z której pochodzi.

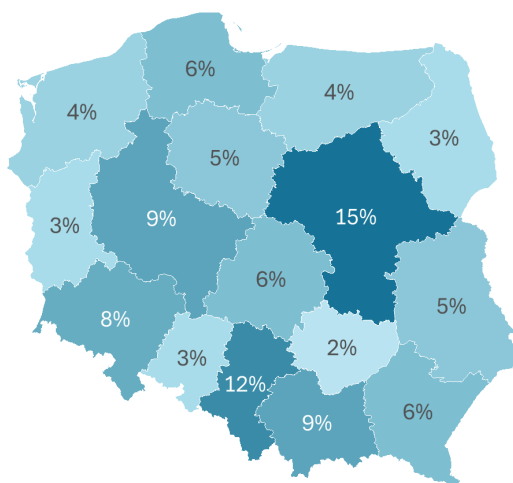
Metoda ilościowa oraz dobór próby zastosowany w badaniu umożliwiają uogólnienie wyników na całą populację dorosłych z błędem szacunku na poziomie $\pm 3\%$ (poziom ufności 95%).

Odsetek wywiadów przeprowadzonych w poszczególnych grupach demograficznych przedstawiono na rysunkach 4–8.



Rysunek 4. Struktura respondentów ze względu na płeć

Źródło: opracowanie własne.



Rysunek 5. Struktura respondentów pod względem województwa

Źródło: opracowanie własne.



Rysunek 6. Struktura respondentów pod względem wykształcenia

Źródło: opracowanie własne.



Rysunek 7. Struktura respondentów pod względem wieku

Źródło: opracowanie własne.



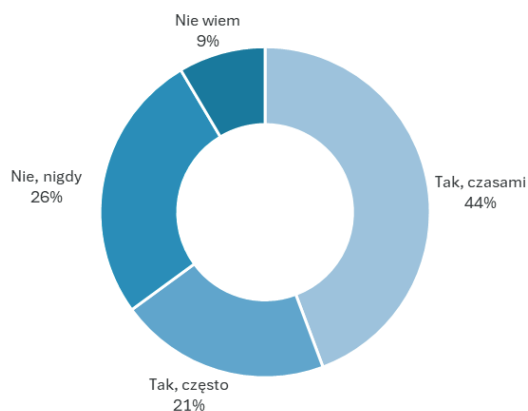
Rysunek 8. Struktura respondentów pod względem wielkości miejsca zamieszkania (liczba mieszkańców)

Źródło: opracowanie własne.

Wyniki badania

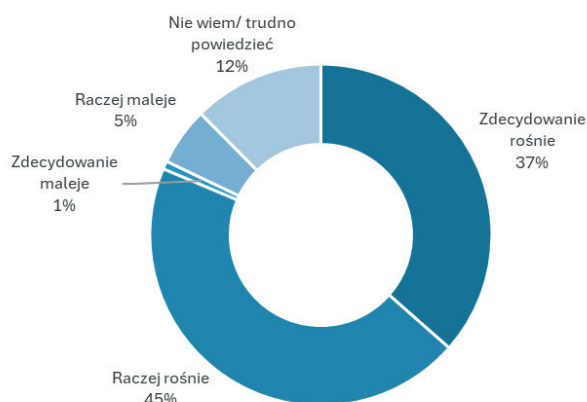
Pierwszą część badania ankietowego dotyczyła świadomości cyberzagrożeń oraz doświadczeń (osobistych i dotyczących bliskich/znajomych) związanych z cyberatakami. W tej części respondenci udzielili odpowiedzi na trzy pytania.

Pytanie 1 – Czy podczas korzystania z Internetu odczuwasz obawy dotyczące swojego bezpieczeństwa?



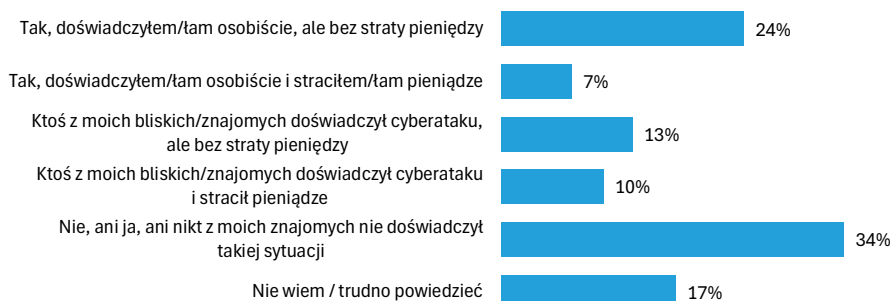
Zdecydowana większość respondentów (65%) na tak postawione pytanie udzieliła odpowiedzi twierdzącej, przy czym 44% osób wskazywało, że takie obawy towarzyszą im czasami, a 21% – że często. Wśród ankietowanych osób 26% odpowiedziało, że nie ma obaw dotyczących swojego bezpieczeństwa w sieci, a 9% wybrało odpowiedź „nie wiem”. Mężczyźni istotnie częściej (32% vs. 23% kobiet) odpowiadali, że nie mają obaw dotyczących swego bezpieczeństwa w sieci.

Pytanie 2 – Czy uważasz, że liczba zagrożeń cyfrowych obecnie rośnie?



W odpowiedzi na pytanie 2 zdecydowana większość respondentów (82%) wskazywała na odczuwalny w ich przekonaniu trend wzrostowy – 37% odpowiedzi „zdecydowanie rośnie” i 45% odpowiedzi „raczej rośnie”. Jedynie 6% wskazało na zmniejszający się poziom cyberzagrożeń, a 12% ankietowanych nie potrafiło dokonać oceny – odpowiedzi „nie wiem/trudno powiedzieć”. Brak oceny był istotnie częściej (17%) wybierany w porównaniu z całą populacją przez mieszkańców wsi.

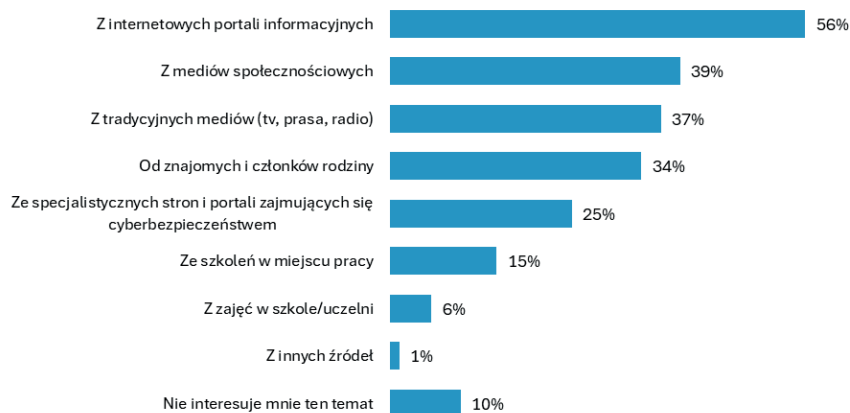
Pytanie 3 – Czy doświadczyłeś/doświadczyłaś jakiejś formy cyberataku?



Odpowiedzi na pytanie 3 pokazują, że ponad połowa ankietowanych (54%) lub ich bliscy czy znajomi doświadczyli jakiejś formy cyberataku. W tej grupie najwięcej osób (24%) wskazywało, że doświadczyło osobiście cyberataku, ale bez konsekwencji finansowych, oraz że takie doświadczenia mieli ich bliscy/znajomi (13%). Respondenci, którzy osobiście doświadczyli utraty pieniędzy w wyniku cyberataku lub wskazali, że takie zdarzenia dotknęły ich bliskich lub znajomych, stanowili odpowiednio 7% i 10%. Wśród ankietowanych 34% nie doświadczyło takiej sytuacji, a 17% odpowiedziało „nie wiem/trudno ocenić”. Osoby starsze, w wieku 56–65 lat, istotnie częściej w porównaniu z resztą badanych odpowiadały (48% odpowiedzi), że ani osobiście, ani nikt z ich znajomych nie doświadczył cyberataku.

Druga część badania obejmowała pytania mające na celu zidentyfikowanie najważniejszych źródeł, z których Polacy pozyskują wiedzę w zakresie cyberbezpieczeństwa, ocenę działań edukacyjnych, jakie prowadzone są przez różne podmioty i kanały komunikacji, chęci poszerzenia swojej wiedzy w tym zakresie oraz zbadanie deklarowanego poziomu wiedzy dotyczącej najczęściej spotykanych zagrożeń. W tej części respondenci odpowiedzieli na cztery pytania.

Pytanie 4 – Skąd czerpiesz wiedzę na temat cyberbezpieczeństwa?

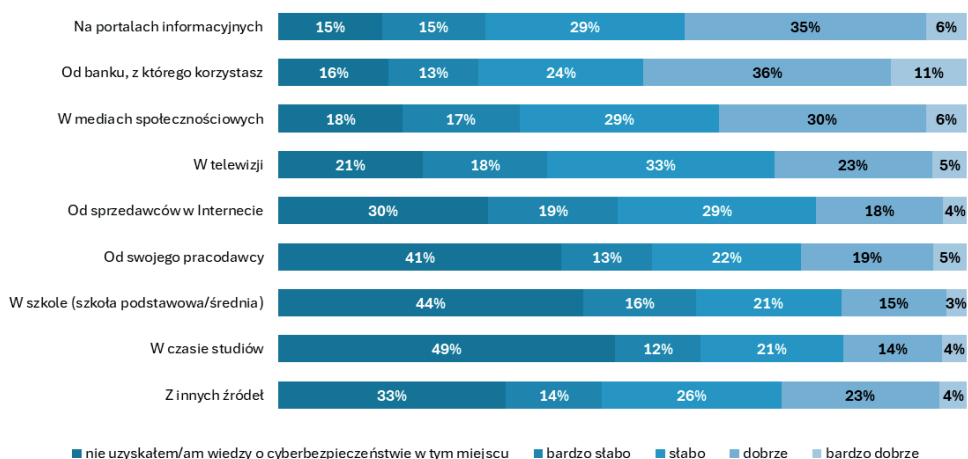


Jako źródła informacji na temat cyberbezpieczeństwa najczęściej wymieniane były portale informacyjne (56%), media społecznościowe (39%) oraz tradycyjne media (37%). Wśród ankietowanych osób 34% wskazywało, że źródłem informacji są znajomi oraz członkowie rodzin. Znacznie rzadziej wybierane były specjalistyczne portale zajmujące się cyfrowym bezpieczeństwem (25%) oraz szkolenia organizowane przez pracodawców (15%). Jedynie 6% ankietowanych wskazało na zajęcia w szkołach oraz w czasie studiów. Znacząca grupa respondentów (10%) odpowiedziała, że taka wiedza nie jest im potrzebna.

Zauważalne są różnice demograficzne w pozyskiwaniu informacji o cyberbezpieczeństwie z różnych źródeł: mężczyźni częściej niż kobiety wymieniają portale informacyjne (64% mężczyzn vs. 49% kobiet), specjalistyczne strony i portale (34% vs. 16%). Kobiety częściej wymieniają takie źródła, jak znajomi i członkowie rodziny (38% kobiet vs. 30% mężczyzn) oraz zajęcia w szkole/uczelnii (8% vs. 4%).

Osoby w wieku 18–25 lat najczęściej czerpią wiedzę z zakresu cyberbezpieczeństwa z mediów społecznościowych (52%), częściej niż pozostali też ze szkoły/uczelnii (28%), rzadziej niż reszta z tradycyjnych mediów (27%).

Pytanie 5 – Jak oceniasz informacje/wiedzę na temat cyberbezpieczeństwa, które uzyskałeś?



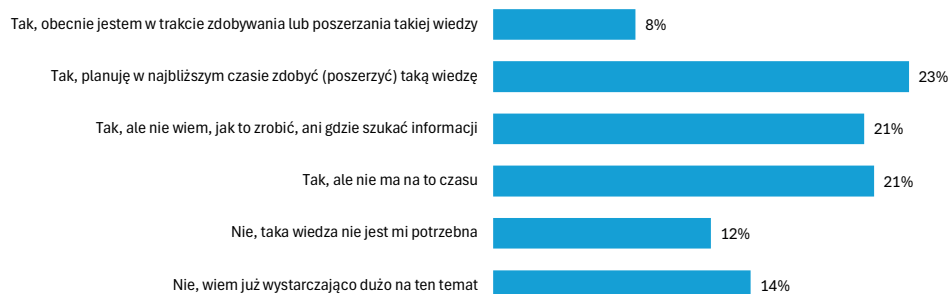
Wśród najlepiej ocenianych źródeł informacji na temat cyberbezpieczeństwa znalazły się banki, z których korzystają respondenci (47% ocen „dobrze” i „bardzo dobrze”), portale informacyjne (41% ocen pozytywnych) i media społecznościowe (36% ocen pozytywnych). Gorzej oceniane były informacje publikowane za pośrednictwem telewizji i innych (niewskazanych z nazwy) źródeł, którym oceny pozytywne przyznało odpowiednio 28% i 27% respondentów. Pracodawcy i sklepy internetowe uzyskały odpowiednio 24% i 22% pozytywnych odpowiedzi. Najniżej osoby ankietowane oceniły informacje na temat cyberbezpieczeństwa, jakie uzyskały na etapie edukacji w szkołach oraz w czasie studiów. Jedynie 18% respondentów przyznało oceny pozytywne, a aż w 44% (szkoły podstawowe i średnie) i 49% (studia) przypadków ankietowani wskazali, że w trakcie edukacji nie uzyskali żadnej wiedzy w zakresie cyberbezpieczeństwa.

Na uzyskane w tym zakresie wyniki niewątpliwie wpływa fakt, że wśród respondentów były osoby w różnym wieku, w tym także starsze, których formalna edukacja nie

obejmowała nie tylko zagadnień dotyczących cyberbezpieczeństwa, ale też technologii komputerowych. Biorąc pod uwagę wyniki uzyskane wyłącznie w grupie wiekowej 18–25 lat, czyli wśród osób, których programy edukacyjne obejmowały już zagadnienia związane z nowymi technologiami i bezpieczeństwem cyfrowym, odsetek odpowiedzi „dobrze” i „bardzo dobrze” pozostaje nadal na bardzo niskim poziomie i wynosi jedynie 35% (szkoła) i 32% (studia). Niemal 20% respondentów w tej grupie wskazało, że nie zdobyło żadnej wiedzy na temat cyberbezpieczeństwa w szkole, a aż 38% ankietowanych (osoby z wykształceniem wyższym i studiujące) odpowiedziało, że takiej wiedzy nie zdobyło w czasie studiów.

Wiedzę przekazywaną przez pracodawców istotnie lepiej oceniają mężczyźni (27% odpowiedzi „dobrze” i „bardzo dobrze”) niż kobiety (22%) oraz osoby w wieku 26–40 lat (29% ocen dobrych i bardzo dobrych wobec 24% w całej populacji).

Pytanie 6 – Czy chciałbyś zdobyć (poszerzyć) wiedzę na temat cyberbezpieczeństwa?

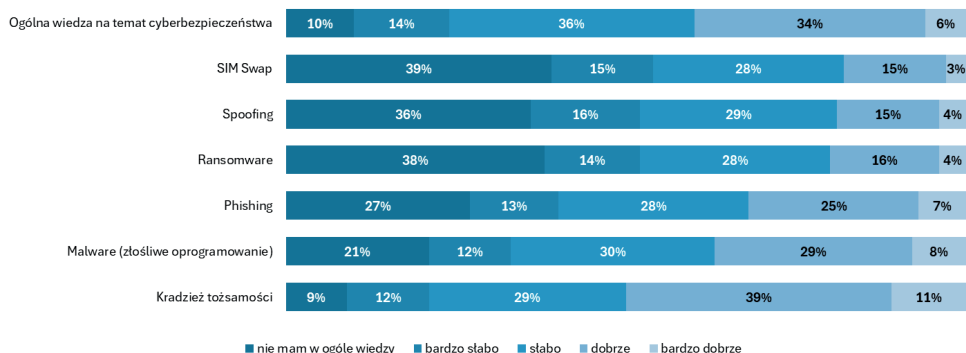


Wśród wszystkich ankietowanych osoby, które są w trakcie zdobywania/poszerzania wiedzy w zakresie cyberbezpieczeństwa lub planują działania edukacyjne w najbliższym czasie, stanowiły 31%. Respondenci, którzy wyrażali chęć zdobycia lub rozszerzenia wiedzy, ale nie wiedzą, jak to zrobić i gdzie szukać informacji, lub identyfikują problem związany z brakiem czasu, stanowili łącznie 42%. Brak potrzeby wskazało 26% ankietowanych, z czego 14% zadeklarowało, że dysponują wiedzą, która jest wystarczająca, a 12% uważa, że wiedza dotycząca cyberbezpieczeństwa nie jest im potrzebna (wynik ten jest zbliżony do odsetka odpowiedzi „nie interesuje mnie ten temat” w pytaniu 4).

Osoby z najstarszej badanej grupy wiekowej (56–65 lat) istotnie częściej niż pozostali respondenci wskazywały odpowiedź „tak, ale nie wiem, jak to zrobić ani gdzie szukać informacji” (26%).

Emeryci i renciści częściej niż pozostałe osoby wskazywali, że nie chcą poszerzać wiedzy o cyberbezpieczeństwie, ponieważ uważają, że wiedzą już wystarczająco na ten temat (22% emerytów aktywnych zawodowo i 28% emerytów nieaktywnych zawodowo).

Pytanie 7 – Jak oceniasz swoją wiedzę na temat poniższych zagrożeń?

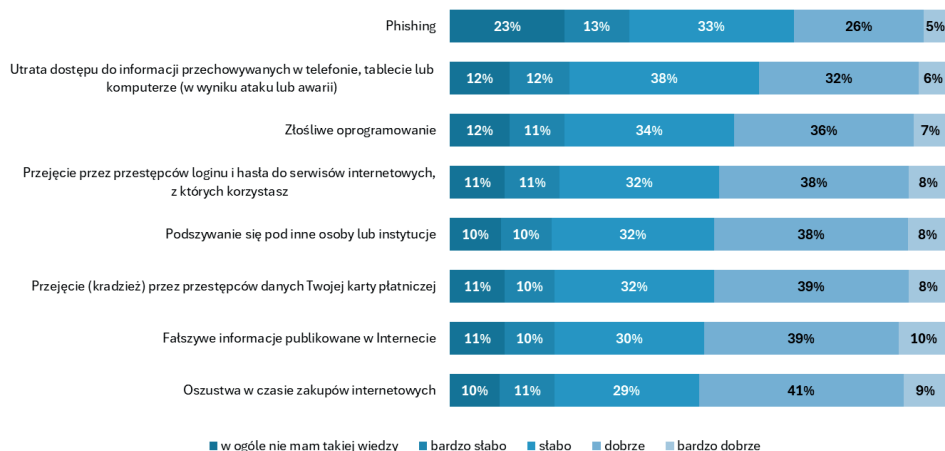


Udzielone odpowiedzi wskazują, że 60% respondentów ocenia swoją ogólną wiedzę w sposób niewystarczający (odpowiedzi: „nie mam w ogóle wiedzy”, „bardzo słabo” i „słabo”), a 10% wskazuje na całkowity brak wiedzy. W odniesieniu do poszczególnych zagrożeń ankietowani zadeklarowali, że najlepiej orientują się w zagadnieniach dotyczących kradzieży tożsamości – odsetek osób oceniających swoją wiedzę na poziomie dobrym i bardzo dobrym to 50%. Odsetek osób deklarujących posiadanie wiedzy na temat *malware* i *phishingu* wyniósł odpowiednio 37% i 32%. Najniższy deklarowany poziom wiedzy wskazano dla zagrożeń obejmujących *ransomware*, *spoofing* i *SIM swap* (oszustwa związane z nielegalnym klonowaniem kart SIM) – odsetek osób deklarujących posiadanie wystarczającej wiedzy wyniósł odpowiednio 20%, 19% i 18%.

Deklaratywna ocena własnej wiedzy w każdej ze wskazanych kategorii była istotnie wyższa w przypadku mężczyzn niż kobiet. W odniesieniu do ogólnej wiedzy mężczyźni wybierali odpowiedzi „dobrze” i „bardzo dobrze” w 46% przypadków, natomiast kobiety – w 33%.

W trzeciej części badania respondenci odpowiadali na dwa pytania, których celem było zbadanie umiejętności obrony przed zagrożeniami, a także praktycznego wykorzystania technicznych rozwiązań zmniejszających ryzyko wystąpienia incydentów cyfrowych.

Pytanie 8 – Jak oceniasz swoją wiedzę i umiejętności obrony przed poniższymi zagrożeniami (czy wiesz, jak się przed nimi bronić?)



Odsetek respondentów, którzy ocenili, że wiedzą, jak bronić się przed najpopularniejszymi zagrożeniami, wahał się w przedziale od 31% do 50%. Najwyższy odsetek odpowiedzi wskazujących na posiadanie wystarczających kompetencji (odpowiedzi „dobrze” i „bardzo dobrze”) w tym zakresie dotyczył obrony przed oszustwami w czasie zakupów internetowych oraz fałszywymi informacjami publikowanymi w Internecie (49% odpowiedzi), a najniższy – obrony przed phishingiem (31%) i ryzykiem utraty danych w wyniku awarii lub ataku (38%).

Różnice demograficzne w udzielanych odpowiedziach dotyczyły płci i wieku respondentów. Istotnie częściej swoją wiedzę i umiejętności obrony przed zagrożeniami na poziomie „dobrym” i „bardzo dobrym” oceniali mężczyźni i osoby w wieku 18–25 lat.

Pytanie 9 – Czy stosujesz poniższe rozwiązania?



Odpowiedzi na pytanie dotyczące praktycznego stosowania technicznych rozwiązań w zakresie cyberbezpieczeństwa wskazują, że zdecydowana większość ankietowanych zabezpiecza komputery za pomocą oprogramowania antywirusowego (84% odpowiedzi „tak” i „częściowo”) oraz stosuje uwierzytelnienie dwuskładnikowe (80% odpowiedzi). Stosowanie odpowiednio długich i unikalnych haseł zadeklarowało odpowiednio 78% i 76%. Ponad połowa respondentów wskazała, że wykonuje kopie bezpieczeństwa swoich danych (66%), sprawdza, czy nie doszło do wycieku haseł (59%), i zapisuje swoje hasła w przeglądarce internetowej (58%). Najmniej ankietowanych (49%) zadeklarowało, że korzysta z menedżera haseł zainstalowanego na swoim telefonie.

Z wyników badania wynika, że różnice w zakresie stosowanych rozwiązań pojawiają się głównie w zależności od płci respondentów. Mężczyźni częściej niż kobiety deklarują, że zainstalowali na komputerze program antywirusowy (74% odpowiedzi „tak” vs. 67% wśród kobiet). Również istotnie częściej stosują uwierzytelnianie dwuskładnikowe (58% vs. 50% kobiet), tworzą inne hasła do każdego serwisu, z którego korzystają (47% vs. 40% kobiet), i robią kopie zapasowe swoich danych (48% vs. 37% kobiet). Mężczyźni (40%) oraz mieszkańcy wsi (40%) częściej niż pozostali sprawdzają okresowo, czy nie wyciekły ich hasła dostępu.

Mężczyźni także częściej niż kobiety zapisują hasła w przeglądarce internetowej (35% vs. 28% kobiet).

Wnioski z badania

Wnioski z przeprowadzonego badania sformułowano w odniesieniu do trzech kluczowych obszarów cyberbezpieczeństwa, tj. poziomu świadomości, poziomu i źródeł wiedzy oraz umiejętności praktycznych w zakresie, który był przedmiotem badania ankietowego.

1. Świadomość zagrożeń w cyberprzestrzeni

Wyniki badania potwierdzają, że znaczna część społeczeństwa ma świadomość zagrożeń płynących z korzystania z zasobów cyfrowych. Aż 64% respondentów zadeklarowało, że odczuwa obawy związane z bezpieczeństwem w Internecie – co czwarta osoba wskazała, że zdarza się to często, a prawie połowa – że czasami. Wynik ten jest szczególnie istotny w kontekście rosnącej liczby cyberataków oraz informacji o incydentach z udziałem obywateli, instytucji publicznych i firm. Obawy użytkowników mogą świadczyć nie tylko o wzroście świadomości ryzyka, ale również o poczuciu braku kontroli nad zagrożeniami cyfrowymi.

Istotną różnicą demograficzną jest fakt, że mężczyźni częściej niż kobiety deklarowali brak obaw (32% mężczyzn vs. 23% kobiet).

Równocześnie 82% badanych jest przekonanych, że liczba zagrożeń cyfrowych rośnie. Taki poziom percepcji świadczy o tym, że Polacy dostrzegają dynamiczny rozwój technik

ataków oraz ich coraz większą skalę i złożoność. Tylko niewielki odsetek respondentów (6%) uważa, że poziom zagrożeń spada. Może to wynikać zarówno z indywidualnych doświadczeń, jak i niskiej wiedzy na temat aktualnych zagrożeń.

Przekonanie o wzroście liczby zagrożeń dominuje w niemal wszystkich grupach społecznych, choć osoby mieszkające na wsi częściej (17%) niż reszta populacji deklarują brak zdania w tej kwestii.

Należy też odnotować, że ponad połowa badanych (54%) wskazuje, iż oni sami lub osoby z ich najbliższego otoczenia padły ofiarą jakiegoś rodzaju cyberataku. W szczególności zwraca uwagę fakt, że 17% respondentów (7% osobiście, w 10% ich bliscy) doświadczyło realnych strat finansowych w wyniku takich incydentów. Dane te dowodzą, że cyberzagrożenia nie są już tylko abstrakcyjnym problemem, ale mają coraz częściej wymiar praktyczny i bezpośrednio wpływają na życie obywateli.

W grupie wiekowej 56–65 lat niemal połowa (48%) zadeklarowała brak jakiegokolwiek doświadczenia z cyberatakami, co może wskazywać na mniejszą aktywność cyfrową lub ograniczoną percepcję zagrożeń.

2. Wiedza i źródła informacji na temat zagrożeń

Analiza odpowiedzi udzielonych przez respondentów wskazuje, że wiedza na temat zagrożeń cyfrowych w polskim społeczeństwie jest często powierzchowna i niesystematyczna. Ponad 60% osób ocenia swoją wiedzę jako niewystarczającą, z czego aż 10% przyznaje, że nie posiada żadnej wiedzy w tym zakresie. Istnieje wyraźna zależność pomiędzy typem zagrożenia a poziomem wiedzy – najlepiej rozpoznawanym zjawiskiem jest kradzież tożsamości (50% deklaracji wiedzy na poziomie dobrym i bardzo dobrym), natomiast znacznie słabiej znane są takie zagrożenia, jak *ransomware* (20%), *spoofing* (19%) czy *SIM swap* (18%).

Mężczyźni wykazują wyraźnie wyższy poziom samooceny w tym zakresie – 46% z nich ocenia swoją ogólną wiedzę jako dobrą lub bardzo dobrą wobec 33% takich ocen wśród kobiet.

Znaczącą część społeczeństwa czerpie wiedzę o cyberbezpieczeństwie z niespecjalistycznych źródeł, takich jak portale informacyjne (56%) i media społecznościowe (39%). Istotną rolę odgrywają też tradycyjne media (37%) oraz informacje przekazywane przez znajomych i rodzinę (34%). Znacznie rzadziej wykorzystywane są źródła specjalistyczne, takie jak portale tematyczne (25%) czy szkolenia organizowane przez pracodawców (15%). Zdecydowanie najmniej osób wskazuje na formalne źródła edukacyjne, takie jak szkoły i uczelnie wyższe – zaledwie 6% respondentów uznało je za źródło swojej wiedzy w tym obszarze.

Analiza uzyskanych wyników wskazuje na znaczące różnice demograficzne: mężczyźni częściej niż kobiety korzystają z portali specjalistycznych (34% vs. 16%), natomiast kobiety częściej sięgają po informacje od znajomych i rodziny (38% vs. 30%). Młodzież

(18–25 lat) częściej niż inne grupy wiekowe wskazuje na media społecznościowe (52%) oraz szkoły i uczelnie (28%) jako źródło wiedzy.

Niezwykle istotna jest także niska ocena jakości wiedzy uzyskanej w procesie kształcenia – niemal połowa badanych przyznaje, że nie zdobyła żadnej wiedzy na temat cyberbezpieczeństwa ani w szkole (44%), ani na studiach (49%). Wyjątkiem są osoby w wieku 18–25 lat, które częściej pozytywnie oceniają szkolną edukację (35% w przypadku szkoły i 32% w przypadku studiów). Odpowiedzi respondentów świadczą o istnieniu systemowej luki w programach nauczania i wskazują na konieczność szerszego uwzględniania zagadnień związanych z cyberbezpieczeństwem w działaniach edukacyjnych.

Warto odnotować, że mimo ograniczonego poziomu wiedzy aż 73% respondentów deklaruje chęć jej poszerzenia. Co istotne, 42% z nich napotyka bariery w dostępie do informacji – nie wiedzą, gdzie szukać wiedzy, lub nie mają na to czasu. Jest to zatem grupa potencjalnych beneficjentów działań edukacyjnych i informacyjnych, które mogłyby znacząco poprawić ogólny poziom kompetencji społecznych w zakresie bezpieczeństwa cyfrowego. Przekonanie, że dodatkowa wiedza nie jest już potrzebna, występuje częściej wśród emerytów i rencistów niż w innych grupach.

3. Umiejętności praktyczne i stosowanie narzędzi zabezpieczających

Deklaracje respondentów wskazują, że mimo niedostatecznej wiedzy teoretycznej wiele osób stosuje w praktyce podstawowe środki ochrony. Zdecydowana większość ankietowanych zadeklarowała, że korzysta z programów antywirusowych (84%) oraz uwierzytelnienia dwuskładnikowego (80%), co może świadczyć o skuteczności działań informacyjnych prowadzonych przez banki, platformy zakupowe i media. Wysoki odsetek osób stosujących unikalne i długie hasła (odpowiednio 78% i 76%) również można uznać za pozytywny wskaźnik świadomości higieny cyfrowej. Mężczyźni częściej niż kobiety deklarują stosowanie niemal wszystkich zabezpieczeń.

Jednak nie wszystkie praktyki zabezpieczające są równie powszechne. Tylko 49% badanych korzysta z menedżerów haseł zainstalowanych na urządzeniach mobilnych. Może to wynikać z braku zaufania do takich narzędzi, braku wiedzy o ich istnieniu lub trudności w ich obsłudze.

Poziom deklarowanych umiejętności obronnych przed konkretnymi zagrożeniami także jest zróżnicowany. Największe przekonanie o własnych kompetencjach występuje w odniesieniu do oszustw związanych z zakupami internetowymi (50%) i dezinformacją (50%). Znacznie niższe kompetencje respondenci przypisują sobie w zakresie ochrony przed phishingiem (31%) oraz zabezpieczenia danych przed utratą wskutek awarii lub ataku (38%). Na deklarowany poziom kompetencji istotnie wpływają płeć i wiek respondentów. Najwyższy poziom kompetencji w tym zakresie deklarują mężczyźni oraz osoby w wieku 18–25 lat.

Wyniki badania pozwalają sformułować kilka kluczowych wniosków:

1. Wysoka świadomość zagrożeń – Polacy dostrzegają wzrost ryzyka i mają osobiste doświadczenia z cyberatakami, co świadczy o rosnącej roli bezpieczeństwa cyfrowego w życiu codziennym. Zauważalne są różnice demograficzne – młodsze osoby i mężczyźni częściej wykazują obawy i doświadczenia związane z cyberatakami, podczas gdy osoby starsze i mieszkańcy wsi rzadziej identyfikują się z tymi zagadnieniami.
2. Niski poziom wiedzy formalnej – system edukacji nie dostarcza wystarczającej wiedzy w zakresie cyberbezpieczeństwa, a dominujące źródła informacji to media masowe i społecznościowe.
3. Gotowość do nauki – duża część respondentów deklaruje chęć poszerzania wiedzy, co stwarza szansę na skuteczne wdrożenie kampanii edukacyjnych i szkoleń.
4. Częściowa implementacja dobrych praktyk – wiele osób stosuje podstawowe środki zabezpieczające, choć wiedza na temat bardziej zaawansowanych narzędzi i zagrożeń pozostaje niska.
5. Różnice płci i wieku są istotne dla projektowania polityk edukacyjnych – konieczne jest dostosowanie treści i kanałów edukacyjnych do konkretnych grup społecznych, uwzględniając ich styl życia i preferencje informacyjne.

4.2. Znaczenie świadomości i edukacji dla budowy systemu cyberbezpieczeństwa w Polsce

W obliczu dynamicznie rozwijającego się środowiska cyfrowego kompetencje cyfrowe stają się kluczowym elementem zapewniającym skuteczną ochronę przed zagrożeniami w cyberprzestrzeni. Badania i dokumenty strategiczne jednoznacznie wskazują, że świadomość, wiedza i umiejętności w zakresie technologii cyfrowych stanowią niezbędny fundament dla budowania skutecznego systemu cyberbezpieczeństwa⁸. Zarówno na poziomie indywidualnym, organizacyjnym, jak i państwowym deficyty w obszarze kompetencji cyfrowych zwiększają podatność na cyberzagrożenia, podczas gdy ich systematyczny rozwój wzmacnia zdolność do identyfikacji zagrożeń, reagowania na nie oraz odbudowy po incydentach. Analiza współczesnych strategii i programów rozwoju kompetencji cyfrowych wskazuje na rosnące znaczenie czynnika ludzkiego w kontekście krajowych systemów cyberbezpieczeństwa oraz jego fundamentalną rolę w budowaniu cyberodporności społeczeństwa.

W kontekście cyberbezpieczeństwa należy zauważyć, że czynnik ludzki odnosi się nie tylko do zwykłych użytkowników systemów i usług informatycznych, ale także do

⁸ A. Budziewicz-Guźlecka, *Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych*, Szczecin 2019, s. 247.

specjalistów, techników, administratorów, menedżerów odpowiedzialnych za projektowanie, wdrażanie oraz nadzór nad infrastrukturą bezpieczeństwa oraz decydentów. Kluczowym zagadnieniem staje się w tym ujęciu poziom świadomości, wiedzy i kompetencji w zakresie identyfikowania, unikania oraz reagowania na zagrożenia cyfrowe. W kontekście cyberbezpieczeństwa pojęcia „świadomość”, „wiedza” oraz „kompetencje” odnoszą się do różnych, choć wzajemnie powiązanych aspektów przygotowania jednostek i organizacji do rozpoznawania, reagowania i zapobiegania zagrożeniom cyfrowym.

Świadomość cyberbezpieczeństwa jest podstawowym i często pierwszym etapem budowania odporności na zagrożenia cyfrowe. To poziom uważności i gotowości użytkownika na zagrożenia oraz zrozumienie, że jego działania w przestrzeni cyfrowej mogą mieć konsekwencje dla bezpieczeństwa informacji. Obejmuje zarówno znajomość podstawowych zagrożeń, jak i zrozumienie własnej roli w systemie bezpieczeństwa. Nie wymaga posiadania specjalistycznej wiedzy technicznej – jej celem jest wykształcenie ostrożności i odpowiedzialności w korzystaniu z nowych technologii.

Według ENISA świadomość cyberbezpieczeństwa to „zdolność użytkowników do rozpoznawania zagrożeń oraz stosowania się do zasad i praktyk zwiększających bezpieczeństwo w środowisku cyfrowym”⁹. Podkreślenie roli świadomości znaleźć można w wielu dokumentach o charakterze strategicznym oraz w rekomendacjach i wytycznych, w których wskazuje się, że to obywatele i ich zrozumienie współczesnych zagrożeń powinny stanowić pierwszą linię obrony w cyberprzestrzeni. Podejście takie znaleźć można m.in. w strategii cyberbezpieczeństwa Wielkiej Brytanii, w polskich Krajowych Ramach Polityki Cyberbezpieczeństwa oraz w rekomendacjach ENISA.

Największe wyzwania związane z budowaniem świadomości w zakresie cyberbezpieczeństwa obejmują konieczność nadążania za szybko pojawiającymi się nowymi zagrożeniami, zmniejszanie wpływu i skutków ludzkich błędów, motywowanie i zwiększanie zaangażowania ludzi w działania związane z dbaniem o cyberhigienę oraz przestrzeganiem zasad. Świadomość traktowana jest jako element kultury bezpieczeństwa organizacyjnego oraz fundament działań edukacyjnych.

Wiedza w zakresie cyberbezpieczeństwa oznacza zrozumienie pojęć, technologii i procesów związanych z ochroną informacji, systemów oraz sieci przed nieautoryzowanym dostępem, atakami lub innymi formami naruszenia integralności i poufności danych. W tym kontekście wiedza może mieć charakter zarówno ogólny (np. elementarna wiedza na temat tworzenia bezpiecznych haseł, znajomość typów zagrożeń, takich jak *phishing*, *malware*), jak i specjalistyczny (np. znajomość kryptografii, testów penetracyjnych, standardów i regulacji prawnych czy też procedur zarządzania incydentami). Umożliwia zrozumienie, dlaczego dane zachowanie jest bezpieczne bądź niebezpieczne

⁹ ENISA, *Cybersecurity Culture Guidelines...*

oraz jak działają narzędzia i metody ochrony danych, dzięki czemu stanowi podstawę dla budowania i rozwijania kompetencji.

Kompetencje są definiowane jako połączenie wiedzy, umiejętności i postaw, które umożliwia jednostce skuteczne działanie w określonej sytuacji¹⁰. W ujęciu systemowym kompetencje można rozumieć jako zdolność do wykorzystania zasobów wewnętrznych (wiedzy, umiejętności, postaw) oraz zewnętrznych (narzędzi, procedur) w celu rozwiązywania problemów i podejmowania decyzji w konkretnych warunkach. Odnosząc pojęcie „kompetencje” do obszaru cyberbezpieczeństwa, należy zauważyć, że w zakresie cyberbezpieczeństwa są one ściśle powiązane z kompetencjami cyfrowymi.

Kompetencje cyfrowe (ang. *digital competences*) rozumiane są jako ogólny zbiór umiejętności, wiedzy i postaw umożliwiających skuteczne i bezpieczne korzystanie z technologii cyfrowych w życiu prywatnym, zawodowym i społecznym. Uznaje się, że udział w życiu społecznym i gospodarczym w dzisiejszych czasach wymaga zestawu kompetencji związanych z technologiami, które w ciągu ostatniej dekady zaczęły być rozumiane jako „umiejętności życiowe”, porównywalne do pisania i liczenia¹¹. Ich znaczenie zostało podkreślone w zaleceniu Rady Europejskiej z 22 maja 2018 roku, które ustanawia kompetencje cyfrowe jako jedną z ośmiu kluczowych kompetencji w procesie uczenia się przez całe życie. Zgodnie z definicją zawartą w tym dokumencie „kompetencje cyfrowe obejmują pewne, krytyczne i odpowiedzialne korzystanie z technologii cyfrowych oraz stosowanie ich w nauce, pracy i uczestnictwie w życiu społecznym. Obejmują one umiejętność korzystania z informacji i danych, komunikowanie się i współpracę, umiejętność korzystania z mediów, tworzenie treści cyfrowych (w tym programowanie), bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem), kwestie dotyczące własności intelektualnej, rozwiązywanie problemów i krytyczne myślenie”¹². Zgodnie z definicją Ministerstwa Cyfryzacji „kompetencje cyfrowe to harmonijna kompozycja wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym, tj. społeczeństwie wykorzystującym w życiu codziennym i pracy technologie cyfrowe”¹³.

W ujęciu strukturalnym kompetencje cyfrowe obejmują trzy zasadnicze kategorie:

- a) kompetencje informatyczne – posługiwanie się komputerem i innymi urządzeniami elektronicznymi, bezpieczne korzystanie z Internetu, aplikacji i oprogramowania, wykorzystanie nowych inteligentnych technologii cyfrowych oraz

¹⁰ M. Mulder, *Conceptions of Professional Competence* [w:] *International Handbook of Research in Professional and Practice Based Learning*, red. S. Billett, C. Harteis, H. Gruber, Springer 2014, s. 107–137.

¹¹ OECD, *Learning to Change: ICT in Schools*, 2001, https://www.oecd.org/en/publications/learning-to-change-ict-in-schools_9789264195714-en.html (18.04.2025).

¹² Zalecenie Rady w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, 22 maja 2018 r., ST 9009 2018 INIT, [https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)).

¹³ *Kompetencje cyfrowe*, 2020, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe> (18.04.2025).

umiejętność rozwiązywania problemów w oparciu o metody wywodzące się z informatyki (myślenie komputacyjne);

- b) kompetencje informacyjno-komunikacyjne – umiejętność wyszukiwania informacji, rozumienia jej, selekcji i oceny krytycznej, jak również komunikowania się na odległość za pomocą technologii cyfrowych;
- c) kompetencje funkcjonalne – dotyczące realnego wykorzystania powyższych kompetencji w różnych sferach codziennego życia (np. finanse, praca i rozwój zawodowy, utrzymywanie relacji, zdrowie, hobby, zaangażowanie obywatelskie) zgodnie z zasadami bezpiecznego korzystania z technologii cyfrowych.

Kompetencje w zakresie cyberbezpieczeństwa (ang. *cybersecurity competences*) stanowią jeden z elementów kompetencji cyfrowych i odnoszą się bezpośrednio do wiedzy, umiejętności i postaw umożliwiających rozpoznawanie zagrożeń, ochronę zasobów cyfrowych, bezpieczne korzystanie z systemów i urządzeń oraz reagowanie na incydenty bezpieczeństwa. Ich zakres obejmuje m.in. znajomość zagrożeń, zasad bezpiecznego zarządzania hasłami, stosowania uwierzytelniania wieloskładnikowego, szyfrowania danych, a także stosowania w praktyce metod i narzędzi zabezpieczających oraz zasad odpowiedzialnego zachowania w środowisku cyfrowym.

Charakteryzując relacje pomiędzy oboma rodzajami kompetencji, trzeba wskazać na ich komplementarny charakter, przy czym kompetencje w zakresie cyberbezpieczeństwa są integralnym komponentem kompetencji cyfrowych i jednocześnie są budowane i rozwijane w oparciu o ogólne umiejętności korzystania z nowych technologii.

W praktyce brak kompetencji jednostki w zakresie cyberbezpieczeństwa może prowadzić do narażenia siebie lub organizacji na poważne zagrożenia mimo posiadania ogólnych kompetencji cyfrowych. Przykładowo użytkownik potrafiący sprawnie korzystać z takich narzędzi komunikacji, jak poczta elektroniczna czy komunikatory internetowe (kompetencja cyfrowa), może stać się ofiarą phishingu, jeśli nie dysponuje wiedzą i umiejętnościami z zakresu ochrony przed tego typu zagrożeniem (kompetencja z zakresu cyberbezpieczeństwa).

Dostrzegając coraz większe znaczenie kompetencji cyfrowych, większość krajów podejmuje liczne inicjatywy mające na celu podnoszenie poziomu umiejętności cyfrowych obywateli, wspieranie edukacji w zakresie nowych technologii oraz rozwój zdolności niezbędnych do bezpiecznego i świadomego funkcjonowania w społeczeństwie informacyjnym. W ramach tych działań duży nacisk kładziony jest na systematyczną ocenę i monitorowanie poziomu kompetencji cyfrowych.

Przykładem działań zmierzających do identyfikacji, rozwoju i oceny kluczowych kompetencji cyfrowych na poziomie Unii Europejskiej jest projekt DigComp (ang. *Digital Competence Framework for Citizens*). To ramowy model kompetencji cyfrowych opracowany przez Wspólne Centrum Badawcze Komisji Europejskiej (Joint Research Centre – JRC), który ma na celu wspieranie obywateli Unii Europejskiej w nabywaniu, rozwijaniu i ocenie umiejętności niezbędnych do aktywnego, świadomego

i bezpiecznego uczestnictwa w życiu społecznym, zawodowym i obywatelskim w erze cyfrowej. Ramy te zostały zaprezentowane po raz pierwszy w 2013 roku, następnie zaktualizowane jako DigComp 2.0 (2016) i DigComp 2.1 (2017), a ostatnia wersja – DigComp 2.2 – została opublikowana w 2022 roku¹⁴.

Najnowsza wersja ram DigComp zawiera odniesienia do nowych obszarów związanych z rozwojem technologicznym, w tym m.in. Internet Rzeczy, sztucznej inteligencji, rozszerzonej i wirtualnej rzeczywistości, a także dezinformacji, cyberbezpieczeństwa oraz ekologicznych aspektów wykorzystania technologii informatycznych. Kolejna aktualizacja ram zapowiadana jest pod koniec 2025 roku¹⁵.

DigComp definiuje pięć głównych obszarów kompetencji cyfrowych, które odpowiadają kluczowym aspektom aktywności człowieka w środowisku cyfrowym:

- a) informacja i dane – umiejętność wyszukiwania, oceny, zarządzania i wykorzystywania informacji cyfrowych w sposób krytyczny i odpowiedzialny;
- b) komunikacja i współpraca – zdolność do interakcji, dzielenia się zasobami oraz współpracy za pomocą technologii cyfrowych z zachowaniem netykiety i świadomości międzykulturowej;
- c) tworzenie treści cyfrowych – tworzenie i edytowanie treści cyfrowych, rozumienie praw autorskich, programowanie i inne aspekty produkcji cyfrowej;
- d) bezpieczeństwo – ochrona urządzeń, danych osobowych, prywatności oraz zdrowia i środowiska w kontekście korzystania z technologii cyfrowych;
- e) rozwiązywanie problemów – identyfikowanie potrzeb i problemów technicznych, dobieranie narzędzi cyfrowych, uczenie się z pomocą technologii oraz innowacyjne wykorzystywanie technologii.

Każdy z tych obszarów zawiera kompetencje szczegółowe (łącznie 21), dla których określono osiem poziomów zaawansowania (od podstawowego – A1 do wysoce specjalistycznego – D8), co pozwala na elastyczne wykorzystanie DigComp w różnych obszarach edukacyjnych, szkoleniowych i zawodowych¹⁶.

Obszar związany z bezpieczeństwem cyfrowym (obszar 4) w ramie DigComp obejmuje cztery szczegółowe kompetencje:

¹⁴ *Digital Competence Framework for Citizens (DigComp)*, https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en (19.04.2025).

¹⁵ *Current developments on DigComp (2024–2025)*, https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/current-developments-digcomp-2024-2025_en (19.04.2025).

¹⁶ R. Vuorikari, S. Klutzer, Y. Punie, *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg 2022.

- a) ochronę urządzeń – umiejętność stosowania środków bezpieczeństwa chroniących sprzęt i dane przed zagrożeniami cyfrowymi;
- b) ochronę danych osobowych i prywatności – zrozumienie, jak dane są przetwarzane oraz jakie są prawa i obowiązki związane z ich ochroną;
- c) bezpieczne zachowania w sieci – świadomość zagrożeń psychologicznych i społecznych w środowisku cyfrowym, takich jak cyberprzemoc, nadużycia, dezinformacja;
- d) zdrowie i środowisko cyfrowe – umiejętność bezpiecznego i zrównoważonego korzystania z technologii z uwzględnieniem zdrowia psychicznego, fizycznego i ochrony środowiska.

Ten komponent stanowi integralny element europejskich programów kształcenia obywatelskiego i zawodowego w zakresie cyberbezpieczeństwa i cyberhigieny.

Ramy DigComp znajdują szerokie zastosowanie w podejmowanych na poziomie krajów członkowskich działaniach związanych z:

- a) tworzeniem programów edukacyjnych – jako podstawa programów kształcenia formalnego i nieformalnego na poziomie krajowym i lokalnym;
- b) projektowaniem polityk publicznych – m.in. w strategiach cyfryzacji, programach włączenia społecznego czy aktywizacji zawodowej;
- c) tworzeniem narzędzi diagnostycznych i ewaluacyjnych – takich jak testy kompetencji cyfrowych, systemy samooceny i certyfikacji;
- d) planowaniem kariery i szkolenia pracowników – jako narzędzie do analizy luk kompetencyjnych i planowania rozwoju zawodowego.

W kontekście monitorowania i oceny kompetencji cyfrowych DigComp tworzy fundament dla rozwoju dodatkowych narzędzi diagnostycznych, takich jak DigCompEdu (dla nauczycieli i edukatorów), DigCompConsumers (dla konsumentów) czy DigCompOrg (dla instytucji edukacyjnych) oraz DigCompSAT i Europass Digital Skills (narzędzia diagnostyczne do samooceny kompetencji cyfrowych),

Dodatkowo ramy DigComp stanowią teoretyczną i metodologiczną podstawę dla tworzenia innych systemów służących diagnostyce i certyfikacji w zakresie kompetencji cyfrowych. Jednym z przykładów jest Indeks Gospodarki Cyfrowej i Społeczeństwa Cyfrowego (ang. *Digital Economy and Society Index* – DESI) – narzędzie opracowane przez Komisję Europejską w celu monitorowania i porównywania postępów krajów Unii Europejskiej w zakresie cyfryzacji. Jest on publikowany corocznie i stanowi jedno z kluczowych źródeł danych dotyczących poziomu transformacji cyfrowej państw członkowskich. Umożliwia ocenę poziomu cyfryzacji w oparciu o zestaw 35 wskaźników dojrzałości cyfrowej, które są grupowane w cztery główne obszary:

- a) kompetencje cyfrowe – ocena umiejętności obywateli w zakresie korzystania z technologii cyfrowych, takich jak obsługa komputera czy internetowe narzędzia pracy;

- b) infrastruktura cyfrowa – analiza dostępności szybkiego Internetu, w tym rozwoju sieci 5G oraz szerokopasmowego Internetu;
- c) transformacja cyfrowa przedsiębiorstw – badanie stopnia integracji technologii cyfrowych w działalności firm, w tym wykorzystania *e-commerce* czy technologii chmurowych;
- d) cyfryzacja usług publicznych – ocena dostępności i jakości usług administracyjnych online, takich jak np. publiczne e-usługi czy *e-government*.

DESI umożliwia identyfikację obszarów wymagających interwencji, takich jak brak podstawowych umiejętności cyfrowych (w tym obejmujących cyberbezpieczeństwo) wśród określonych grup wiekowych lub zawodowych, oraz dostosowanie polityk publicznych do zdiagnozowanych potrzeb w zakresie edukacji cyfrowej. Odgrywa też istotną rolę w analizie postępów w realizacji celów polityk cyfrowych Unii Europejskiej, takich jak np. Kompas Cyfrowy 2030 (ang. *Digital Compass 2030*) oraz „Droga ku cyfrowej dekadzie” (ang. *Digital decade*), w których wyznaczono cele dotyczące rozwoju kompetencji cyfrowych zakładające m.in., że do 2030 roku co najmniej 80% dorosłych obywateli Unii Europejskiej będzie posiadać przynajmniej podstawowe umiejętności cyfrowe¹⁷. Indeks ten jest również wykorzystywany jako narzędzie do oceny skuteczności inwestycji w technologie cyfrowe oraz reform wspieranych przez fundusze unijne, takie jak Instrument na rzecz Odbudowy i Zwiększania Odporności (ang. *Recovery and Resilience Facility* – RRF).

Uzupełnieniem rozwiązań umożliwiających diagnozę i monitoring kompetencji cyfrowych są systemy certyfikacji, które pozwalają na walidację i standaryzację umiejętności cyfrowych obywateli, pracowników oraz specjalistów zatrudnionych w obszarze IT. Ich celem jest nie tylko formalne potwierdzenie posiadanego poziomu wiedzy i umiejętności, ale także wspieranie rozwoju zawodowego, zwiększanie mobilności na rynku pracy, a w szerszym kontekście – wzmacnianie odporności cyfrowej społeczeństwa.

Na świecie funkcjonuje wiele systemów certyfikacji, w tym zarówno zgodnych z międzynarodowymi standardami (np. DigComp czy CompTIA), jak i systemów branżowych (np. w obszarze finansowym, opieki zdrowotnej, administracji czy sektorze obronnym) czy systemów stworzonych przez konkretne firmy (np. CISCO, Microsoft czy Google). W zależności od systemu certyfikacja może obejmować różne obszary (od podstawowych kompetencji ICT, poprzez obszary związane z cyberbezpieczeństwem, projektowanie i zarządzanie systemami sieciowymi, aż po zarządzanie projektami z obszaru IT) i różne poziomy zaawansowania.

¹⁷ *Cyfrowa dekada Europy: cele cyfrowe na 2030 r.*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl (19.04.2025).

Jednym z najstarszych i najbardziej rozpoznawalnych certyfikatów opartych na ramach kwalifikacji DigComp jest międzynarodowy certyfikat ECDL/ICDL (ang. *European/International Computer Driving Licence*). Potwierdza on kompetencje z różnych obszarów (np. obsługa komputera, oprogramowanie biurowe czy bezpieczeństwo cyfrowe), jest wydawany w 150 krajach i w 41 językach, w tym w Polsce¹⁸. Na ramach DigComp opierają się również certyfikaty ECCC (Europejski Certyfikat Kompetencji Cyfrowych) czy ITPass, a w Polsce certyfikat TDCE (ang. *The Digital Competence Exam*) funkcjonujący w ramach Zintegrowanego Systemu Kwalifikacji (ZSK). Kolejnym przykładem jest certyfikat wydawany przez Stowarzyszenie Technologii Informatycznych (ang. *The Computing Technology Industry Association – CompTIA*) – amerykańską niezależną organizację non-profit, która od lat 80. XX wieku zajmuje się m.in. promowaniem standardów w branży informatycznej, formułowaniem zaleceń dla sektora edukacyjnego oraz rządowego, a także wydawaniem certyfikatów zawodowych dla branży technologii informatycznych. Z uwagi na współpracę oraz uznanie ze strony firm branży ICT, instytucji edukacyjnych oraz rządowych stowarzyszenie jest ważnym podmiotem w światowym systemie rozwoju kompetencji cyfrowych. Certyfikaty CompTIA potwierdzają m.in. praktyczne umiejętności dotyczące podstaw technologii informatycznych, obsługi sprzętu komputerowego i systemów operacyjnych, projektowania, konfigurowania i rozwiązywania problemów w sieciach komputerowych, zagadnień związanych z cyberbezpieczeństwem, analiz bezpieczeństwa aplikacji i usług, testów penetracyjnych, analizy danych czy technologii chmurowych¹⁹.

Certyfikaty CompTIA są bardzo cenione w Stanach Zjednoczonych oraz wielu krajach europejskich i często wymagane lub uznawane przez pracodawców w procesach rekrutacyjnych i awansach zawodowych. Wykorzystywane są również jako element kwalifikacji w przetargach publicznych i procedurach potwierdzania zgodności z normami.

Systemy certyfikacji pełnią ważną rolę w procesach rozwoju i obiektywnej oceny kompetencji cyfrowych. Wśród licznych korzyści wskazać można np.:

- a) standaryzację i możliwość porównywania kompetencji cyfrowych;
- b) pozytywny wpływ na jakość edukacji poprzez wymuszenie zgodności programów nauczania z umiejętnościami oczekiwanymi przez firmy i organizacje;
- c) motywację obywateli do rozwoju kompetencji – zewnętrzną gratyfikację oraz potwierdzenie zdobytej wiedzy;
- d) wsparcie mobilności i rozwoju zawodowego dzięki szerokiemu uznawaniu certyfikatów;
- e) lepsze dopasowanie kompetencji do potrzeb – określenie i dostosowanie posiadanych umiejętności do zapotrzebowania zgłaszanego przez pracodawców.

¹⁸ O certyfikacji ECDL/ICDL, <https://pti.org.pl/polskie-biuro-ecdl/> (19.04.2025).

¹⁹ CompTIA Certifications, <https://www.comptia.org/certifications> (19.04.2025).

Chociaż certyfikacja kompetencji cyfrowych przynosi liczne korzyści, to zauważyć należy także problemy i wyzwania, jakie wiążą się z obecnie wykorzystywanymi w tym zakresie systemami:

- a) brak jednolitego standardu globalnego – funkcjonuje wiele równoległych systemów certyfikacji, co może prowadzić do nieporozumień i trudności w uznawalności certyfikatów między krajami i sektorami;
- b) koszty certyfikacji – uzyskanie certyfikatu często wiąże się z kosztami zarówno po stronie uczestników (opłaty egzaminacyjne), jak i instytucji oferujących szkolenia, co może ograniczać dostępność certyfikacji dla osób z niższym statusem społeczno-ekonomicznym;
- c) ryzyko formalizacji i pomijania kompetencji nieformalnych – systemy certyfikacji koncentrują się często na mierzalnych umiejętnościach, pomijając kompetencje miękkie lub umiejętności zdobyte w sposób nieformalny, co może prowadzić do zawężenia rozumienia kompetencji cyfrowych;
- d) dezaktualizacja treści objętych certyfikacją – w dynamicznie zmieniającym się środowisku technologicznym istnieje ryzyko, że treści i wymagania podlegające certyfikacji nie będą nadążać za aktualnymi trendami;
- e) nadmierne skupienie się na aspekcie formalnym – posiadanie certyfikatu może stać się celem samym w sobie, pomijając faktyczny rozwój umiejętności cyfrowych, co wpłynie na obniżenie jego znaczenia na rynku pracy.

Systemy certyfikacji kompetencji cyfrowych pełnią ważną rolę w tworzeniu i rozwoju kompetencji cyfrowych, jednak ich skuteczność zależy od aktualności i standaryzacji treści, szerokiej akceptacji oraz sposobu wdrożenia i wykorzystania tych systemów w praktyce na poziomie międzynarodowym i krajowym. Charakterystyka kompetencji niezbędnych do efektywnego i bezpiecznego wykorzystania cyfrowych technologii oraz narzędzia do oceny, monitoringu i certyfikacji tych kompetencji są częścią szerszych działań, które mają na celu integrację umiejętności, wiedzy i postaw w systemie cyberbezpieczeństwa państw, instytucji, podmiotów gospodarczych i obywateli.

W tym zakresie zarówno Unia Europejska, jak i kraje członkowskie, w tym również Polska, podejmują liczne działania strategiczne i systemowe mające na celu wzrost poziomu cyfrowego bezpieczeństwa i związanych z nim kompetencji, a także zwiększenie liczby wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa.

Rozwój kompetencji w dziedzinie cyberbezpieczeństwa został uznany za jeden z filarów, na których opiera się podejście Unii Europejskiej do wyzwań związanych z bezpieczeństwem cyfrowym. Strategia Unii w zakresie cyberbezpieczeństwa uznaje umiejętności i wiedzę za niezbędne elementy budowania odporności cyfrowej Europy w obliczu rosnących zagrożeń i zakłada stworzenie wspólnego europejskiego systemu cyberbezpieczeństwa oraz znaczące inwestycje w rozwój kompetencji cyfrowych obywateli

i ekspertów z dziedziny bezpieczeństwa²⁰. Znaczenie rozwoju kompetencji w obszarze cyberbezpieczeństwa znalazło odzwierciedlenie w unijnym programie Cyfrowa Europa (ang. Digital Europe Programme), który ma za zadanie wspierać proces cyfrowej transformacji europejskiej gospodarki, przemysłu i społeczeństwa. Program dysponuje budżetem 8,2 mld euro na lata 2021–2027, z czego na cyberbezpieczeństwo i zaawansowane umiejętności cyfrowe przeznaczono blisko 30% środków. Warte podkreślenia jest, że Cyfrowa Europa nie jest jedynym narzędziem finansowania działań w obszarze cyfrowej edukacji. Wsparcie finansowe dla rozwoju kompetencji cyfrowych w latach 2021–2027 zaplanowano też w ramach takich programów, jak Europejski Fundusz Społeczny Plus (ponad 2 mld euro), Instrument na rzecz Odbudowy i Zwiększania Odporności (24 mld euro), Erasmus+, Horyzont Europa czy Europejski Fundusz Dostosowania do Globalizacji dla Zwalnianych Pracowników²¹.

Istotnym elementem unijnej strategii było utworzenie w 2021 roku Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC)²² w celu zwiększenia bezpieczeństwa środowiska online oraz sieci i systemów informacyjnych o krytycznym znaczeniu. Misja ECCC obejmuje kilka kluczowych obszarów związanych z rozwojem kompetencji, w tym:

- a) wzmocnienie pozycji i autonomii strategicznej Unii Europejskiej w dziedzinie cyberbezpieczeństwa poprzez rozwój zdolności badawczych, naukowych, społecznych, technologicznych i przemysłowych;
- b) zwiększenie świadomości i umiejętności w zakresie bezpieczeństwa cyfrowego;
- c) ograniczanie niedoborów wykwalifikowanych pracowników i specjalistów w zakresie cyberbezpieczeństwa w Unii.

ECCC we współpracy z krajowymi centrami kompetencji tworzonymi w państwach członkowskich ma wzmacniać rozwój kompetencji oraz koordynować finansowanie badań i innowacji w zakresie cyberbezpieczeństwa.

W ramach realizacji strategicznych celów Unia Europejska realizuje szereg praktycznych inicjatyw, które mają na celu ograniczenie luki kompetencyjnej w zakresie cyberbezpieczeństwa. Jednym z przykładów takich inicjatyw jest Akademia Umiejętności w Dziedzinie Cyberbezpieczeństwa (ang. The Cybersecurity Skills Academy – CSA), której celem jest umożliwienie wszystkim zainteresowanym osobom dostępu do szkoleń, certyfikacji oraz programów edukacyjnych z zakresu cyberbezpieczeństwa, a także

²⁰ *The EU's Cybersecurity Strategy for the Digital Decade*, <https://ec.europa.eu/newsroom/dae/redirection/document/72164> (19.04.2025).

²¹ European Commission, *Digital skills initiatives*, <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives> (22.04.2025).

²² Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC), <https://www.gov.pl/web/cyber-nccpl/eccc> (22.04.2025).

koordynacja działań edukacyjnych i szkoleniowych na poziomie europejskim. W skład Akademii wchodzi platforma internetowa Digital Skills and Jobs, na której udostępniane są oferty dotyczące możliwości zmiany lub podnoszenia kwalifikacji w obszarze cyberbezpieczeństwa, a także granty dla instytucji edukacyjnych chcących prowadzić szkolenia z zakresu cyberbezpieczeństwa.

Poza rozwojem wiedzy i działalnością szkoleniową inicjatywy CSA obejmują także:

- a) finansowanie projektów – wsparcie projektów związanych z rozwijaniem umiejętności w dziedzinie cyberbezpieczeństwa oraz koordynację działań związanych z pozyskiwaniem źródeł finansowania;
- b) budowanie sieci współpracy – tworzenie partnerstw biznesowo-akademickich oraz współpracę z sektorem prywatnym mającą na celu podniesienie jakości oferowanych szkoleń;
- c) monitorowanie zmian w kompetencjach dotyczących cyberbezpieczeństwa – analizę potrzeb rynku pracy, śledzenie zmian oraz trendów w zakresie kompetencji z obszaru cyberbezpieczeństwa, co pozwala na skuteczne dostosowanie programów edukacyjnych do wymagań rynkowych.

Istotne znaczenie dla rozwoju umiejętności dotyczących cyberbezpieczeństwa na poziomie Unii Europejskiej mają też działania podejmowane przez ENISA, która wspiera wymianę dobrych praktyk, opracowuje raporty i ekspertyzy, a także promuje działania międzynarodowe, których celem jest zwiększenie świadomości i edukacja z obszaru cyberbezpieczeństwa. Najważniejsze działania agencji w tych obszarach to:

1. Tworzenie ram i wytycznych – opracowanie dokumentu pod nazwą *Europejskie Ramy Kompetencji w Zakresie Cyberbezpieczeństwa* (ang. *European Cybersecurity Skills Framework – ECSF*), który zawiera zestawienie kompetencji, umiejętności oraz wiedzy wymaganej od specjalistów ds. cyberbezpieczeństwa w Unii Europejskiej. Powstały one, aby ustandaryzować wymagania zawodowe, wspierać rozwój kompetencji oraz promować jednolite podejście do edukacji i szkolenia specjalistów cyberbezpieczeństwa w całej Europie. Są powszechnie wykorzystywane w europejskich programach szkoleniowych, w tym przez Akademię Umiejętności w Dziedzinie Cyberbezpieczeństwa²³.
2. Koordynacja i wsparcie inicjatyw krajowych – wsparcie krajowych organów w opracowywaniu i wdrażaniu takich mechanizmów, jak krajowe ramy kompetencji w zakresie cyberbezpieczeństwa. Agencja prowadzi też analizy działań, które są podejmowane przez poszczególne państwa członkowskie w celu ograniczenia niedoboru kompetencji w zakresie cyberbezpieczeństwa.

²³ *European Cybersecurity Skills Framework (ECSF)*, <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsfc> (22.04.2025).

3. Organizacja ćwiczeń i programów szkoleniowych – opracowywanie scenariuszy materiałów szkoleniowych i cyklicznych ćwiczeń z zakresu cyberbezpieczeństwa (np. Cyber Europe czy International Cybersecurity Challenge) na poziomie lokalnym, międzynarodowym oraz ogólnounijnym.
4. Rozwój i wsparcie platform i zasobów edukacyjnych – prowadzenie internetowych platform szkoleniowych oraz repozytoriów programów szkoleniowych. Przykładem są platformy: CyberEducation, która udostępnia różnorodne zasobów edukacyjnych z zakresu cyberbezpieczeństwa, dostosowane do potrzeb szkół podstawowych i średnich, oraz CyberHEAD, która zawiera weryfikowane informacje na temat programów edukacyjnych w zakresie bezpieczeństwa cyfrowego, realizowanych przez wyższe uczelnie w krajach Unii Europejskiej i EFTA.
5. Współpraca i tworzenie partnerstw – nawiązywanie współpracy z różnymi podmiotami (w tym z sektora publicznego i prywatnego) w celu promowania dobrych praktyk w zakresie cyberbezpieczeństwa oraz podnoszenia ogólnej świadomości na temat zagrożeń cyfrowych. ENISA angażuje się także w liczne działania, które mają na celu rozwijanie wiedzy i kompetencji w zakresie cyberbezpieczeństwa we wszystkich sektorach gospodarki.

Analizy działań w zakresie rozwoju umiejętności w obszarze bezpieczeństwa cyfrowego podejmowanych na poziomie poszczególnych krajów europejskich wskazują na zróżnicowany ich poziom i zakres. W przeprowadzonej przez ENISA ewaluacji²⁴ średni poziom dojrzałości krajowych systemów edukacyjnych w obszarze cyberbezpieczeństwa został oceniony na 66%, co odpowiada czterem z pięciu poziomów dojrzałości (nieistniejący, wstępny/doraźny, zdefiniowany, ugruntowany, optymalny). Uzyskany wynik oznacza, że państwa członkowskie podjęły już szereg inicjatyw na rzecz edukacji w zakresie cyberbezpieczeństwa, jednak w opracowaniu podkreślono, że podejście do edukacji i podejmowane działania w poszczególnych krajach są bardzo zróżnicowane i w większości opierają się na zdecentralizowanych inicjatywach lub znajdują się na początkowym etapie wdrażania. Jako najważniejsze wyzwania wskazano ograniczone zasoby, w tym niewystarczającą liczbę przeszkolonych nauczycieli i trenerów, trudności we współpracy z wieloma zaangażowanymi podmiotami oraz powolną integrację edukacji obejmującej cyberbezpieczeństwo z krajowymi programami nauczania.

W ostatnich latach również w Polsce podejmowane są systemowe i wielopoziomowe działania na rzecz edukacji w zakresie cyberbezpieczeństwa, które stanowią odpowiedź na rosnące wyzwania związane z cyfryzacją społeczeństwa, gospodarki i administracji publicznej. Realizowane w tym obszarze inicjatywy obejmują zarówno tworzenie i wdrażanie strategii w zakresie cyberbezpieczeństwa, zmiany legislacyjne, jak i praktyczne

²⁴ ENISA, *Cybersecurity Education Maturity Assessment*, 2024, <https://www.enisa.europa.eu/publications/cybersecurity-education-maturity-assessment> (22.04.2025).

programy edukacyjne skierowane do różnych grup społecznych – od dzieci i młodzieży, przez nauczycieli, studentów, pracowników administracji publicznej i sektora prywatnego, aż po seniorów oraz osoby zagrożone wykluczeniem cyfrowym. W podejmowane działania zaangażowane są m.in.: Ministerstwo Cyfryzacji, Ministerstwo Edukacji Narodowej, Ministerstwo Nauki i Szkolnictwa Wyższego, Ministerstwo Rozwoju i Technologii, Ministerstwo Obrony Narodowej, Centrum Projektów Polska Cyfrowa, Polska Agencja Rozwoju Przedsiębiorczości, NASK, jednostki samorządu terytorialnego, organizacje pozarządowe oraz partnerstwa publiczno-prywatne.

Znaczenie zagadnień związanych z edukacją dla cyberbezpieczeństwa znajduje odzwierciedlenie w strategicznych dokumentach i działaniach podejmowanych na szczeblu rządowym. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 wyraźnie podkreślała rolę edukacji i podnoszenia świadomości jako kluczowego elementu budowania odporności na cyberzagrożenia, konieczność wdrażania edukacji dla cyberbezpieczeństwa na wszystkich poziomach systemu oświaty oraz w ramach kształcenia ustawicznego, a także wspierania inicjatyw społecznych i współpracy z sektorem prywatnym. Czwarty cel szczegółowy tej strategii obejmował „budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa”. Z informacji dotyczących planowanego zakresu kolejnej Strategii cyberbezpieczeństwa Polski na lata 2025–2029²⁵ wynika, że działania mające na celu podniesienie świadomości i kompetencji w zakresie cyberbezpieczeństwa na różnych poziomach będą jednym z głównych obszarów rozwijanym w najbliższym czasie. Założenia strategiczne znalazły odzwierciedlenie w przyjętym przez Radę Ministrów w 2023 roku Programie Rozwoju Kompetencji Cyfrowych, którego celem jest wzrost poziomu kompetencji cyfrowych (w tym dotyczących cyberbezpieczeństwa) zarówno wśród zwykłych użytkowników technologii cyfrowych, jak i specjalistów ICT.

Podejmowane działania wskazują na spójność polityki państwa w zakresie rozwoju świadomości i wiedzy oraz potwierdzają priorytetowe traktowanie rozwoju umiejętności związanych z cyberbezpieczeństwem na poziomie krajowym.

Praktycznym efektem realizowanych działań edukacyjnych stało się wprowadzenie zagadnień dotyczących rozpoznawania i ochrony przed cyberzagrożeniami do programów nauczania na poziomie szkół podstawowych i średnich, gdzie wybrane zagadnienia dotyczące m.in. cyberprzemocy, cyberhigieny, ochrony prywatności, wiarygodności informacji czy cyberbezpieczeństwa militarnego w systemie bezpieczeństwa państwa znalazły się w podstawie programowej takich przedmiotów, jak informatyka i edukacja dla bezpieczeństwa. Dodatkowo prowadzone są obecnie prace zmierzające do rozszerzania tego obszaru poprzez wprowadzenie do szkół przedmiotu dotyczącego szeroko

²⁵ Co z podatkiem cyfrowym i Strategią cyberbezpieczeństwa?, <https://cyberdefence24.pl/cyberbezpieczenstwo/co-z-podatkiem-cyfrowym-i-strategia-cyberbezpieczenstwa> (23.04.2025).

rozumianych kompetencji cyfrowych i edukacji medialnej²⁶. Równolegle do edukacji dzieci i młodzieży realizowane są projekty zmierzające do podniesienia kwalifikacji nauczycieli, które obejmują tworzenie przewodników i scenariuszy do zajęć, warsztaty i kursy (zarówno w formie stacjonarnej, jak i szkoleń online) umożliwiające zdobycie aktualnej wiedzy i praktycznych umiejętności w zakresie cyberbezpieczeństwa.

Ministerstwo Edukacji Narodowej w programie polityki oświatowej na lata 2024–2025 podkreśliło, że jednym z kluczowych elementów edukacji ma być rozwój umiejętności cyfrowych nauczycieli, ze szczególnym uwzględnieniem bezpiecznego poruszania się w sieci oraz krytycznej analizy informacji dostępnych w Internecie²⁷.

Cyberbezpieczeństwo jest przedmiotem kształcenia również na poziomie studiów wyższych i edukacji zawodowej. Polskie uczelnie wyższe oraz instytucje edukacyjne oferują szeroką gamę programów studiów i kursów związanych z cyberbezpieczeństwem. Tematyka dotycząca bezpieczeństwa cyfrowego i jego różnych wymiarów jest omawiana w ramach dedykowanych kierunków studiów lub specjalizacji. Uczelnie oferują też studia podyplomowe i kursy z zakresu cyberbezpieczeństwa skierowane do profesjonalistów pragnących podnieść swoje kwalifikacje lub osób chcących zdobyć nowe umiejętności²⁸.

W rozwój kompetencji cyfrowych oraz kompetencji związanych z cyberbezpieczeństwem zaangażowane są także organy administracji centralnej. Znaczącą rolę w tym zakresie odgrywają np. Ministerstwo Cyfryzacji i Ministerstwo Obrony Narodowej, które były organizatorami szeregu programów i inicjatyw edukacyjnych (np. projekty Cyberlekcje 3.0, Bezpieczna Szkoła w Cyberprzestrzeni, Cyber.mil z klasą). W 2024 roku Ministerstwo Cyfryzacji i Centrum Projektów Polska Cyfrowa ogłosiły pięć projektów, których celem jest dofinansowanie szkoleń ukierunkowanych na rozwój umiejętności cyfrowych Polaków. Ich beneficjentami mają być nauczycieli przedszkolni, nauczyciele szkolni, obywatele, urzędnicy i osoby wykluczone cyfrowo²⁹.

Uzupełnieniem formalnych programów edukacyjnych są liczne inicjatywy mające na celu podniesienie świadomości społeczeństwa na temat cyberbezpieczeństwa. Agencje rządowe, takie jak NASK, prowadzą kampanie edukacyjne adresowane do różnych grup demograficznych i obejmujące m.in. takie zagadnienia, jak przeciwdziałanie dezinformacji, ochrona wizerunku w sieci, bezpieczne korzystanie z Internetu, bankowości elektronicznej, technologii cyfrowych i narzędzi e-administracji. NASK jest też koordynatorem corocznego wydarzenia organizowanego przez ENISA z inicjatywy Komisji

²⁶ *Edukacja cyfrowa dzieci. Co planuje rząd?*, <https://cyberdefence24.pl/cyberbezpieczenstwo/edukacja-cyfrowa-dzieci-co-planuje-rzad> (23.04.2025).

²⁷ *Cyberbezpieczeństwo w szkole*, <https://www.rodosfera.pl/post/cyberbezpieczenstwo-w-szkole> (23.04.2025).

²⁸ *#CyberMagazyn: Gdzie można studiować cyberbezpieczeństwo?*, <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-gdzie-mozna-studiowac-cyberbezpieczenstwo> (25.04.2025).

²⁹ *Prawie 400 mln zł na rozwój umiejętności cyfrowych Polaków*, <https://www.gov.pl/web/cyfryzacja/prawie-400-mln-zl-na-rozwoj-umiejtnosci-cyfrowych-polakow> (25.04.2025).

Europejskiej pod nazwą Europejski Miesiąc Cyberbezpieczeństwa, którego celem jest podnoszenie świadomości na temat cyberbezpieczeństwa i nowoczesnych technologii.

Oprócz działań podejmowanych przez instytucje państwowe istotną rolę w edukacji dla cyberbezpieczeństwa odgrywają organizacje pozarządowe, które realizują liczne projekty edukacyjne skierowane do różnych grup społecznych. Przykładem są np. działania edukacyjne prowadzone przez Fundację Dajemy Dzieciom Siłę (projekt Saferinternet realizowany we współpracy z NASK), Fundację Bezpieczna Cyberprzestrzeń (projekty Cyberbastion i CYBER-EXE Polska) czy Fundację Instytut Cyberbezpieczeństwa (tworzenie materiałów edukacyjnych i prowadzenie szkoleń).

Rosnąca liczba incydentów cyberbezpieczeństwa oraz wzrost poczucia zagrożenia wśród użytkowników technologii cyfrowych, mogące prowadzić do obniżenia popytu na innowacyjne produkty i usługi, skłania także podmioty prywatne do intensyfikacji działań w obszarze rozwoju kompetencji dotyczących bezpieczeństwa cyfrowego. W odpowiedzi na wyzwania w zakresie cyberbezpieczeństwa podmioty sektora prywatnego coraz częściej angażują się samodzielnie lub we współpracy w ramach partnerstw publiczno-prywatnych w projekty mające na celu podnoszenie poziomu wiedzy i kompetencji wśród obecnych i potencjalnych klientów.

Przykładami takich działań są: Program Współpracy w Cyberbezpieczeństwie (PWCyber)³⁰ prowadzony przez Ministerstwo Cyfryzacji z udziałem firm technologicznych i organizacji społecznych, którego cele obejmują promowanie innowacyjnych rozwiązań technologicznych oraz prowadzenie kampanii edukacyjno-informacyjnych, a także zainaugurowany w 2017 roku projekt „Bezpieczeństwo w Cyberprzestrzeni”, w którym uczestniczą banki, fundacje, firmy IT oraz wydawcy kart płatniczych. Celem tego projektu jest edukowanie Polaków w zakresie bezpiecznego korzystania z nowoczesnych narzędzi cyfrowych, w tym bankowości elektronicznej, oraz popularyzacja gospodarki elektronicznej poprzez wykłady prowadzone stacjonarnie i online, webinary, szkolenia oraz kursy e-learningowe dostępne bezpłatnie dla wszystkich zainteresowanych. Obok podmiotów działających w sferze finansowej duże zaangażowanie w realizację kampanii edukacyjnych wykazują podmioty z branży *e-commerce* i handlu detalicznego, operatorzy telekomunikacyjni oraz podmioty działające w branży technologicznej (np. Google i Microsoft).

Równolegle, z uwagi na deficyt wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa oraz pracowników posiadających kompetencje umożliwiające bezpieczne korzystanie z technologii cyfrowych w ramach obowiązków zawodowych, podmioty prywatne coraz częściej rozwijają własne systemy kształcenia w obszarze

³⁰ Program Współpracy w Cyberbezpieczeństwie (PWCyber), <https://www.gov.pl/web/baza-wiedzy/o-programie> (25.04.2025).

cyberbezpieczeństwa kierowane do obecnych i przyszłych pracowników, czego przykładem są działania prowadzone np. przez firmy Microsoft, Google, Orange i Cisco³¹.

Wzrost liczby inicjatyw i działań edukacyjnych jest bez wątpienia konsekwencją coraz większych środków finansowych, jakie ze źródeł publicznych i prywatnych przeznaczane są na rozwój kompetencji cyfrowych i kompetencji związanych z cyberbezpieczeństwem. W ostatnich latach dostrzegany jest wyraźny wzrost wydatków budżetowych na różne inicjatywy i programy dotyczące podnoszenia poziomu bezpieczeństwa cyfrowego. Jednym z przykładów są wydatki realizowane poprzez Fundusz Cyberbezpieczeństwa, którego głównym celem jest wspieranie działań mających zapewnić bezpieczeństwo systemów teleinformatycznych, w tym wsparcie finansowe dla specjalistów zatrudnianych w tym obszarze. Począwszy od 2024 roku zgodnie z zapowiedziami ministra cyfryzacji z budżetu państwa ma być przekazywane na ten cel 250 mln złotych rocznie. Tylko w roku 2025 zaplanowano przeznaczenie na cyberbezpieczeństwo rekordowej kwoty 4 mld złotych (obejmuje ona zarówno wydatki cywilne, jak i wojskowe), co stanowi największą dotychczasową inwestycję Polski w tej dziedzinie³². Łączna kwota wydatków budżetowych na cyberbezpieczeństwo w latach 2025–2026 ma wynieść około 10 mld złotych³³, z czego część będzie przeznaczona na podniesienie kompetencji cyfrowych różnych grup społecznych – od dzieci i młodzieży, przez osoby zagrożone wykluczeniem cyfrowym, po specjalistów i urzędników administracji publicznej i samorządowej.

Istotnym źródłem finansowania działań związanych z cyberbezpieczeństwem są też fundusze unijne. W ramach programu Fundusze Europejskie na Rozwój Cyfrowy na lata 2021–2027 (FERC) Polska otrzymała blisko 2 mld euro na wsparcie transformacji cyfrowej, w tym na wzmocnienie cyberbezpieczeństwa. Dodatkowo na rozwój infrastruktury cyfrowej oraz kompetencji obywateli w ramach szerszych inwestycji przewidziano 11,4 mld euro³⁴.

Znaczące środki na cyberbezpieczeństwo i rozwój e-kompetencji zastały zaplanowane również w ramach Krajowego Planu Odbudowy. Na realizację tych działań w latach 2021–2027 ma być przeznaczane co najmniej 184 mln euro (około 800 mln złotych)

31 *Niemal ćwierć miliona Europejczyków przeszkolonych przez Cisco w dziedzinie cyberbezpieczeństwa w ciągu ostatniego roku*, <https://brief.pl/niemal-cwierc-miliona-europejczykow-przeszkolonych-przez-cisco-w-dziedzinie-cyberbezpieczenstwa-w-ciagu-ostatniego-roku/> (26.04.2025).

32 *Cyberbezpieczeństwo w 2025 roku: kluczowe wsparcie dla samorządów*, <https://samorząd.pap.pl/kategoria/e-urząd/cyberbezpieczenstwo-w-2025-roku-kluczowe-wsparcie-dla-samorzadow> (26.04.2025).

33 *Ministerstwo Cyfryzacji zamierza wydać 10 mld zł na cyberbezpieczeństwo*, https://www.pap.pl/aktualnosci/ministerstwo-cyfryzacji-zamierza-wydac-10-mld-zl-na-cyberbezpieczenstwo?utm_source=chatgpt.com (26.04.2025).

34 *Fundusze Europejskie na Rozwój Cyfrowy 2021–2027*, <https://www.polskacyfrowa.gov.pl/strony/o-programie/fundusze-europejskie-na-rozwoj-cyfrowy-2021-2027-2028/> (26.04.2025).

z możliwością rozszerzenia finansowania o środki z innych programów unijnych i krajowych. Obejmuje to zarówno inwestycje w kompetencje cyfrowe, jak i wsparcie infrastrukturalne dla bezpieczeństwa cyfrowego administracji i obywateli³⁵.

Widoczny staje się też wzrost wydatków związanych z cyberbezpieczeństwem w sektorze prywatnym. Firmy coraz częściej dostrzegają konieczność nie tylko inwestowania w technologie zabezpieczające, ale także w rozwój kompetencji pracowników, aby skutecznie przeciwdziałać zagrożeniom cyfrowym. Według raportu KPMG w 2023 roku znacząco wzrosły budżety przeznaczane na ten cel. Największy przyrost (12 p.p. w porównaniu z poprzednim rokiem) miał miejsce w obszarach zarządzania tożsamością i dostępem oraz bezpieczeństwa w procesach wytwarzania oprogramowania³⁶. Należy przypuszczać, że konieczność dostosowania się polskich organizacji do obowiązków związanych z wejściem w życie nowych regulacji dotyczących cyberbezpieczeństwa (DORA, NIS2) przyczyni się do dalszego zwiększania wydatków w obszarze bezpieczeństwa cyfrowego.

Rezultatem podejmowanych wysiłków w zakresie podnoszenia poziomu szeroko rozumianego bezpieczeństwa cyfrowego jest widoczny wzrost liczby inicjatyw i przeszkolonych osób, który przekłada się na coraz wyższy poziom świadomości i kompetencji, systematyczny rozwój infrastruktury edukacyjnej oraz postępującą integrację polityki edukacyjnej z krajową strategią cyberbezpieczeństwa.

4.3. Rekomendacje na rzecz rozwoju kompetencji cyberbezpieczeństwa w Polsce

W ostatnich latach Polska, podobnie jak większość krajów europejskich, znacząco zwiększyła wysiłki i nakłady mające na celu podniesienie poziomu cyberbezpieczeństwa obywateli oraz instytucji. Pomimo intensywnych działań podejmowanych przez instytucje publiczne oraz znaczących nakładów finansowych przeznaczanych na rozwój ogólnych kompetencji cyfrowych i kompetencji w zakresie cyberbezpieczeństwa poziom tych kompetencji w Polsce nadal pozostaje niezadowolający.

Badania pokazują, że świadomość społeczna dotycząca cyberzagrożeń jest wciąż niska, a odsetek osób posiadających zaawansowaną wiedzę i umiejętności pozwalające na skuteczne przeciwdziałanie zagrożeniom w cyberprzestrzeni pozostaje niższy niż w większości krajów Unii Europejskiej.

³⁵ NIK, *Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa*, 2022, <https://www.nik.gov.pl/kontrola/P/21/003/KAP/> (27.04.2025).

³⁶ KPMG, *Barometr cyberbezpieczeństwa*, 2024, <https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf> (27.04.2025).

Biorąc pod uwagę kompetencje cyfrowe zarówno na poziomie podstawowym, jak i ponadpodstawowym, czyli dwa z kilku elementów, na podstawie których tworzony jest DESI, Polska w 2024 roku znalazła się wśród siedmiu najgorszych krajów. Jedynie 44,3% Polaków posiada kompetencje cyfrowe na poziomie podstawowym, a zaledwie 20% na poziomie ponadpodstawowym, podczas gdy średnia w krajach Unii Europejskiej to odpowiednio 56% i 27%. Niezadowolający jest nie tylko osiągnięty poziom, ale także tempo jego wzrostu. Aby osiągnąć zaplanowany do 2030 roku odsetek 80% obywateli posiadających co najmniej podstawowe kompetencje cyfrowe, tempo wzrostu musiałoby być pięciokrotnie wyższe, niż miało to miejsce w ostatnich latach. Deficyt ogólnych kompetencji cyfrowych powoduje, że Polacy nie dysponują wystarczającą wiedzą i umiejętnościami w zakresie cyberbezpieczeństwa. Pomimo coraz większej liczby kampanii informacyjnych i działań edukacyjnych znacząca część społeczeństwa nadal nie zna lub nie stosuje zasad cyberhigieny oraz nie potrafi w sposób bezpieczny korzystać z Internetu i nowoczesnych usług. Przedstawione w punkcie 4.1 wyniki badań wskazują, że pomimo wysokiego poziomu świadomości zagrożeń i obaw związanych z wykorzystaniem technologii cyfrowych wiedza i poziom umiejętności, które pozwalają je niwelować, są w przypadku około 60% społeczeństwa niewystarczające. Uzyskane przez autora wyniki nie odbiegają znacząco od innych badań w tym zakresie. Przykładowo badanie przeprowadzone przez CBM Indicator na zlecenie Google wskazało, że większość Polaków można zaliczyć do grupy określanej jako cyfrowi nowicjusze (*Newbies*). Jest to grupa osób, które mają niewystarczające kompetencje, aby bezpiecznie poruszać się w Internecie, nie mają świadomości zagrożeń czyhających na nich w cyberprzestrzeni, nie wiedzą, jak się przed nimi bronić oraz jak na nie reagować. Do grupy tej zaliczono aż 56,9% polskich internautów³⁷.

Brak wystarczających kompetencji dotyczy jednak nie tylko obywateli i bezpieczeństwa osobistego. Rosnącym problemem jest także niedobór wykwalifikowanych pracowników i specjalistów w dziedzinie cyberbezpieczeństwa. Jak wynika z raportu PIIT, w Polsce już w 2023 roku niedobór wszystkich ekspertów IT sięgał 50 tys., z czego około 10 tys. stanowiły osoby zajmujące się cyberbezpieczeństwem³⁸. Według danych Eurostatu odsetek specjalistów w dziedzinie IT w stosunku do wszystkich zatrudnionych w Polsce wynosi 4,5% i jest niższy nie tylko od najlepszych krajów w rankingu (Luksemburg, Finlandia i Estonia), w których odsetek ten przekracza 7%, ale również od średniej unijnej

³⁷ *Jesteśmy coraz bardziej świadomi zagrożeń w sieci*, 2022, <https://polska.googleblog.com/2022/11/jestesmy-coraz-bardziej-swiadomi.html/> (28.04.2025).

³⁸ *Polska cierpi na brak specjalistów od cyberbezpieczeństwa. Luka kompetencyjna jest spora*, <https://www.bankier.pl/wiadomosc/Polska-cierpi-na-brak-specjalistow-od-cyberbezpieczenstwa-Luka-kompetencyjna-jest-spora-8641461.html> (28.04.2025).

wynoszącej 5%³⁹. Osiągnięcie zaplanowanego w dokumentach strategicznych poziomu 6% specjalistów oznacza konieczność zwiększania liczby specjalistów IT w Polsce o 30% do roku 2030, a podkreślić należy, że określony w Polsce poziom docelowy jest znacznie niższy niż zakładany w europejskim programie „Droga ku cyfrowej dekadzie”.

Efektom są narastające problemy z rekrutacją pracowników w obszarze cyberbezpieczeństwa, których według badania Cyberskills z 2024 roku doświadcza blisko 50% firm⁴⁰. Uzyskane wyniki wskazują, że aż 39% polskich przedsiębiorstw nie zatrudnia ani jednego pracownika odpowiedzialnego za cyberbezpieczeństwo⁴¹. Prognozy wskazują, że implementacja do polskiego porządku prawnego takich regulacji, jak NIS2 czy DORA, przyczyni się do dalszego wzrostu zapotrzebowania na wykwalifikowanych pracowników sektora cyberbezpieczeństwa.

Niewystarczający poziom kompetencji cyfrowych oraz niedobory specjalistów ds. cyberbezpieczeństwa mają swoje źródła zarówno w czynnikach systemowych, jak i społecznych.

Rozwijany w Polsce system cyberbezpieczeństwa skupiał się dotychczas na prawnych i technicznych zagadnieniach związanych z wybranymi obszarami, takimi jak ochrona infrastruktury krytycznej, jednostek administracji publicznej i samorządu terytorialnego, walka z terroryzmem, zwalczanie przestępczości gospodarczej itp. Regulacje prawne w zakresie cyberbezpieczeństwa dotyczyły głównie dużych podmiotów działających na rynku oraz instytucji publicznych. Znacznie mniejszy nacisk kładziono na bezpieczeństwo mniejszych podmiotów gospodarczych i obywateli oraz ich ochronę przed cyberzagrożeniami, a podejmowane w tym zakresie działania realizowane były często ze znacznym opóźnieniem. Istotnym problemem jest też niedostateczne dopasowanie systemu edukacji formalnej i szkoleń zawodowych do dynamicznie zmieniającego się krajobrazu cyberzagrożeń i związanych z tym potrzeb rynku cyfrowego. Braki wynikające z niewystarczającego poziomu edukacji oraz niewystarczająca świadomość dotycząca znaczenia kompetencji cyfrowych i umiejętności w zakresie cyberbezpieczeństwa we współczesnym świecie powodują, że pomimo znaczących nakładów na kampanie informacyjne i społeczne dotyczące rozpoznawania i ochrony przed cyberzagrożeniami charakteryzują się one ograniczoną efektywnością.

Krytyczną ocenę działań organów administracji publicznej w Polsce na rzecz podnoszenia kompetencji cyfrowych społeczeństwa w latach 2018–2021 przedstawiono

³⁹ Eurostat, 2024, https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/bar?lang=en (28.04.2025).

⁴⁰ Eurobarometr, *Cyberskills*, 2024, https://data.europa.eu/data/datasets/s3176_fl547_eng?locale=en (28.04.2025).

⁴¹ ENISA, 2024 *Report on the State of Cybersecurity in the Union*. European Union Agency for Cybersecurity, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (28.04.2025).

w raporcie Najwyższej Izby Kontroli⁴², w którym wskazano szereg zastrzeżeń dotyczących m.in.:

- a) braku spójnej koordynacji działań – nie wyznaczono jednego podmiotu odpowiedzialnego za koordynację, monitorowanie i wspieranie działań podejmowanych w celu podnoszenia kompetencji cyfrowych społeczeństwa pomimo zaangażowania w te działania wielu instytucji (m.in. KPRM, Ministerstwo Edukacji i Nauki, CPPC, Ministerstwo Rozwoju, Pracy i Technologii oraz gminy);
- b) opóźnień w przygotowaniu i wdrożeniu Programu Rozwoju Kompetencji Cyfrowych (PRKC);
- c) braku kompleksowej koncepcji dla szkolnictwa wyższego – nie opracowano koncepcji dotyczącej przygotowania i wykorzystania cyfrowych materiałów edukacyjnych na uczelniach ani podnoszenia kompetencji cyfrowych kadry akademickiej;
- d) problemów z wykorzystaniem materiałów cyfrowych przez nauczycieli, w tym braku chęci i potrzeby poświęcenia czasu na wyszukiwanie dodatkowych materiałów wykraczających poza komercyjne podręczniki, a także braku umiejętności tworzenia własnych materiałów;
- e) braku przygotowania przez Ministerstwo Edukacji i Nauki odrębnego programu promocji doskonalenia kompetencji cyfrowych nauczycieli;
- f) problemów i nieprawidłowości w realizacji projektów na poziomie gmin – w tym np. braku właściwej weryfikacji uczestników grantu, braku rzetelnego nadzoru gminy nad realizacją grantu, niewłaściwego rozliczenia wydatków, nierzetelnego sporządzenia sprawozdań z realizacji grantów oraz nieosiągnięcia zaplanowanych wskaźników;
- g) braku badań dotyczących potrzeb przedsiębiorców – nie przeprowadzono własnych badań pozwalających określić poziom kompetencji cyfrowych przedsiębiorców i potrzeb gospodarki, opierając się głównie na danych z GUS, Eurostatu i DESI;
- h) opóźnienia w przeglądzie kwalifikacji w Zintegrowanym Systemie Kwalifikacji (ZSK) w dziale informatyzacja;
- i) braku określenia potrzeb pracodawców w zakresie przyznawania certyfikatów w ramach kompetencji cyfrowych.

W świetle przedstawionych danych wydaje się oczywiste, że dotychczasowe podejście do rozwoju kompetencji cyfrowych i cyberbezpieczeństwa w Polsce wymaga istotnych korekt na poziomie strategicznym i operacyjnym. Konieczne jest podjęcie szerszych i zintensyfikowanych działań, które będą efektywnie łączyć edukację formalną,

⁴² NIK, *Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa*, 2022, <https://www.nik.gov.pl/kontrole/P/21/003/KAP/> (28.04.2025).

szkolenia specjalistyczne oraz szeroko zakrojone kampanie społeczne ukierunkowane na podnoszenie świadomości zagrożeń w cyberprzestrzeni. Ponadto w celu sprostania rosnącemu zapotrzebowaniu na specjalistów IT i ekspertów ds. cyberbezpieczeństwa niezbędne staje się wypracowanie systemowych rozwiązań wspierających kształcenie zawodowe oraz współpracę między instytucjami edukacyjnymi, sektorem publicznym oraz przedsiębiorstwami. Proponowane w tym zakresie działania powinny obejmować przede wszystkim:

1. Przyspieszenie działań związanych z wdrożeniem i aktualizacją strategicznych programów dotyczących cyberbezpieczeństwa i kompetencji cyfrowych

Przyspieszenie działań związanych z wdrażaniem oraz regularną aktualizacją programów strategicznych stanowi warunek skutecznego kształtowania polityki cyberbezpieczeństwa państwa. W tym kontekście szczególnie istotne jest opracowanie i wdrożenie Strategii cyberbezpieczeństwa Polski na lata 2025–2029 oraz jej wyraźne powiązanie z założeniami Programu Rozwoju Kompetencji Cyfrowych, które powinno się odbywać na poziomie zarówno celów ogólnych, jak i szczegółowych, a także obejmować wspólne mechanizmy realizacji. Dzięki temu możliwe będzie skuteczne zwiększenie poziomu świadomości zagrożeń cyfrowych oraz systematyczny wzrost kompetencji cyfrowych społeczeństwa, co stanowi fundament odporności kraju na zagrożenia w cyberprzestrzeni. Dla osiągnięcia tego celu kluczowe jest wyznaczenie precyzyjnego harmonogramu wdrażania poszczególnych działań oraz jasne określenie ram odpowiedzialności dla poszczególnych instytucji i podmiotów administracji publicznej.

Ze względu na szybkie tempo zmian technologicznych i dynamicznie zmieniające się formy zagrożeń cyfrowych konieczne jest ustanowienie regularnych cykli aktualizacji dokumentów strategicznych. Strategia cyberbezpieczeństwa powinna być poddawana regularnym przeglądom oraz odpowiednio modyfikowana w reakcji na pojawiające się nowe rodzaje zagrożeń oraz zmiany w technologiach czy praktykach cyberprzestępczych. Wskazane jest też włączenie w ten proces ekspertów reprezentujących różne środowiska – od administracji publicznej, przez sektor prywatny, aż po środowiska akademickie oraz organizacje pozarządowe. Pozwoli to na uwzględnienie różnych perspektyw, co zwiększy skuteczność podejmowanych działań.

Integralnym elementem wdrażania i aktualizacji programów strategicznych powinien być także mechanizm monitorowania postępów w realizacji założeń strategicznych. Proces ten obejmować powinien zarówno ocenę stopnia realizacji działań przewidzianych w strategii, jak i jakościową ocenę ich efektywności, opartą na mierzalnych wskaźnikach, takich jak wzrost poziomu kompetencji cyfrowych społeczeństwa, liczba przeszkolonych specjalistów czy spadek liczby skutecznych ataków cyfrowych. Regularne raportowanie postępów oraz transparentność tego procesu będą miały istotne znaczenie

nie tylko dla odpowiedzialnych instytucji, ale również dla społeczeństwa, które powinno mieć dostęp do informacji o skuteczności podejmowanych działań.

Dodatkowym aspektem, który warto uwzględnić, jest specyfika regionalna w kontekście cyfryzacji oraz kompetencji cyfrowych. Polska, będąc krajem zróżnicowanym regionalnie, wymaga dostosowania działań strategicznych do lokalnych potrzeb i możliwości. Uwzględnienie specyfiki regionalnej pozwoli skuteczniej dystrybuować zasoby oraz bardziej trafnie odpowiadać na specyficzne potrzeby poszczególnych społeczności, co w konsekwencji powinno prowadzić do równomiernego wzrostu kompetencji cyfrowych i podnoszenia poziomu cyberbezpieczeństwa na terenie całego kraju.

2. Wzmocnienie zarządzania i lepsza koordynacja działań w zakresie podnoszenia kompetencji cyfrowych i kompetencji w zakresie cyberbezpieczeństwa

Podniesienie efektywności działań związanych z rozwojem kompetencji cyfrowych i cyberbezpieczeństwem wymaga usprawnienia mechanizmów zarządzania oraz lepszej koordynacji działań podejmowanych w tym obszarze na poziomie krajowym i międzynarodowym. Skutecznym rozwiązaniem może być ustanowienie lub wzmocnienie istniejącej instytucji, takiej jak Centrum Rozwoju Kompetencji Cyfrowych (CRKC) lub CERT Polska, przyznając jej rolę centralnego koordynatora inicjatyw dotyczących rozwoju kompetencji cyfrowych w Polsce. Wyraźne określenie kompetencji tego podmiotu umożliwi efektywne monitorowanie realizacji działań oraz zapewni spójność strategii realizowanej przez różne instytucje i podmioty. Instytucja pełniąca rolę koordynatora powinna mieć jasno sprecyzowane uprawnienia i obowiązki w zakresie inicjowania projektów krajowych oraz regionalnych, które są zgodne z celami strategicznymi kraju w dziedzinie cyberbezpieczeństwa i kompetencji cyfrowych. Podejmowane działania powinny się opierać na systemie stałej wymiany informacji pomiędzy poszczególnymi jednostkami edukacyjnymi i administracyjnymi. Zapewni to spójność realizowanych programów szkoleniowych, umożliwi dzielenie się najlepszymi praktykami oraz efektywniejsze zarządzanie zasobami. Dodatkowo konieczne są regularne oceny prowadzonych działań edukacyjnych, co pozwoli na bieżąco dostosowywać treści i formy działań edukacyjnych do zmieniających się potrzeb technologicznych, społecznych i gospodarczych.

Praktycznym przykładem działań koordynacyjnych mogłoby być utworzenie platformy wymiany dobrych praktyk i narzędzi dla wszystkich interesariuszy (samorządy, szkoły, uczelnie, pracodawcy, NGO), która stanowiłaby punkt dostępu do wiedzy, narzędzi, scenariuszy edukacyjnych, forum wymiany doświadczeń oraz aktualnych informacji o zagrożeniach i rekomendacjach w zakresie cyberbezpieczeństwa. Takie rozwiązanie umożliwi skuteczną i szybką dystrybucję informacji oraz wsparcie dla podmiotów o różnym poziomie dojrzałości cyfrowej, a także zminimalizuje ryzyko błędów i zwiększy efektywność działań.

3. Rozwój programów edukacyjnych i dostosowanie ich treści do szybko zmieniającego się krajobrazu cyberbezpieczeństwa na wszystkich poziomach kształcenia

Jednym z podstawowych wyzwań związanych z podnoszeniem kompetencji w zakresie cyberbezpieczeństwa jest dynamiczny charakter zmian technologicznych oraz pojawiających się zagrożeń. W związku z tym niezbędne jest regularne aktualizowanie i dostosowywanie treści programów edukacyjnych na wszystkich poziomach kształcenia do aktualnego stanu wiedzy i najlepszych praktyk w obszarze cyberbezpieczeństwa. Istotne jest uwzględnienie w tym kontekście nie tylko podstaw teoretycznych, ale także aspektów praktycznych, które przygotowują uczniów, studentów oraz osoby dorosłe do rozpoznawania zagrożeń i reagowania na nie w realistycznych warunkach. Jednym z rekomendowanych rozwiązań jest stworzenie ogólnokrajowej infrastruktury edukacyjnej obejmującej sieć specjalistycznych laboratoriów cyberbezpieczeństwa. Placówki te powinny być wyposażone w sprzęt oraz narzędzia symulacyjne pozwalające na praktyczne szkolenie użytkowników w zakresie identyfikacji, analizy oraz reagowania na zagrożenia. Sieć laboratoriów powinna funkcjonować jako centra kompetencji cyfrowych wspierające szkoły, uczelnie oraz ośrodki szkoleniowe.

Zapewnienie wysokiego poziomu kształcenia wymaga, aby system edukacji został zaprojektowany w sposób elastyczny, umożliwiający szybkie wprowadzanie zmian programowych w odpowiedzi na nowe wyzwania pojawiające się w cyberprzestrzeni. Obejmuje to nie tylko aktualizację treści merytorycznych, ale również metod dydaktycznych. Należy rozwijać scenariusze dydaktyczne oparte na dostosowanych do poziomu uczestników praktycznych ćwiczeniach, wirtualnych symulacjach, analizach przypadków oraz zadaniach problemowych, które sprzyjają rozwijaniu umiejętności analitycznych i decyzyjnych. Tego rodzaju podejście zwiększa zaangażowanie uczestników edukacji i umożliwia skuteczniejsze nabywanie kompetencji praktycznych.

Ważnym elementem tego procesu jest też zapewnienie odpowiedniego poziomu przygotowania kadry dydaktycznej. Nauczyciele, wykładowcy i trenerzy powinni mieć dostęp do specjalistycznych szkoleń podnoszących ich wiedzę z zakresu cyberbezpieczeństwa oraz nowoczesnych form kształcenia. W tym celu należy opracować programy doskonalenia zawodowego dedykowane różnym poziomom edukacji – od szkoły podstawowej po szkolnictwo wyższe – oraz zapewnić ich regularne prowadzenie przy wsparciu instytucji naukowych i sektora prywatnego. Konieczne jest także rozwijanie narzędzi edukacyjnych i materiałów dydaktycznych wspierających nauczycieli w realizacji treści programowych w sposób angażujący i dostosowany do poziomu uczniów.

Dobrym przykładem tworzenia kompleksowych ram dla procesu kształcenia w zakresie cyberbezpieczeństwa może być europejski program Cyfrowa Europa (DIGITAL), działania podejmowane przez ENISA oraz realizowany w Finlandii od września 2022 roku pod patronatem Ministerstwa Transportu i Komunikacji oraz Uniwersytetu

Aalto 3-letni projekt, którego celem jest opracowanie pakietu edukacyjnego wspierającego kształcenie w zakresie cyberbezpieczeństwa w państwach członkowskich Unii Europejskiej.

4. Intensyfikacja działań związanych z edukacją nieformalną oraz samokształceniem

Edukacja nieformalna oraz samokształcenie odgrywają coraz większą rolę w rozwijaniu kompetencji cyfrowych, zwłaszcza w kontekście szybko zmieniających się wymagań rynku pracy oraz ograniczeń instytucjonalnych w dostosowywaniu treści programowych do aktualnych wyzwań. W warunkach postępującej cyfryzacji tradycyjne formy kształcenia formalnego okazują się często niewystarczające, co powoduje konieczność stworzenia skutecznych mechanizmów wspierających uczenie się przez całe życie, ze szczególnym uwzględnieniem obszaru cyberbezpieczeństwa.

Istotnym krokiem w tym kierunku jest rozwój powszechnie dostępnych cyfrowych zasobów edukacyjnych w otwartych formatach. Platformy e-learningowe, portale wiedzy, kursy typu MOOC (ang. *Massive Open Online Courses*) czy mikrokursy tematyczne powinny być stale rozbudowywane i wspierane przez instytucje publiczne we współpracy z uczelniami oraz partnerami z sektora prywatnego. Kluczowe znaczenie ma przy tym zapewnienie wysokiego poziomu merytorycznego oferowanych treści oraz ich aktualności wobec najnowszych trendów i rodzajów zagrożeń w cyberprzestrzeni. Niezwykle ważne staje się również promowanie i rozwój umiejętności krytycznej analizy źródeł oraz samodzielnego poszukiwania wiarygodnych informacji, co ma szczególne znaczenie w kontekście przeciwdziałania cyfrowej dezinformacji i manipulacji z wykorzystaniem mediów społecznościowych i generatywnej sztucznej inteligencji.

Niezbędna staje się także budowa świadomości społecznej na temat wartości edukacji nieformalnej jako równoważnego źródła kompetencji, a nie jedynie uzupełnienia kształcenia formalnego. Oznacza to konieczność prowadzenia kampanii informacyjnych, które promują kulturę samokształcenia i pokazują jego znaczenie dla bezpieczeństwa osobistego, zawodowego oraz państwowego. Celowe wydają się też wsparcie inicjatyw oddolnych, takich jak warsztaty, prelekcje i konkursy tematyczne (hackatony) organizowane przez pasjonatów i ekspertów, które integrują osoby o różnych poziomach wiedzy i doświadczenia.

Wzrost znaczenia edukacji nieformalnej i samokształcenia w polityce rozwoju kompetencji cyfrowych może znacząco zwiększyć elastyczność systemu edukacyjnego i umożliwić szybsze reagowanie na pojawiające się luki kompetencyjne. Pozwoli to również na dotarcie do grup, które z różnych względów nie uczestniczą w edukacji formalnej, a jednocześnie mogą stanowić cenne źródło przyszłych specjalistów ds. cyberbezpieczeństwa.

5. Działania związane z dalszym rozwojem i utrzymanie talentów w różnych obszarach dotyczących bezpieczeństwa cyfrowego

Zdolność do identyfikowania i rozwijania talentów w obszarze cyberbezpieczeństwa stanowi jeden z czynników warunkujących budowę silnego i odpornego na zagrożenia państwa. W obecnych warunkach nie wystarcza jedynie zwiększanie liczby osób z podstawową wiedzą technologiczną – konieczne jest podejmowanie działań umożliwiających wczesne rozpoznawanie potencjału osób wykazujących ponadprzeciętne zdolności techniczne, analityczne, logiczne oraz zainteresowanie tematyką bezpieczeństwa cyfrowego.

Jednym z priorytetów powinno być identyfikowanie i wsparcie rozwoju uzdolnionych osób już na poziomie edukacji podstawowej i średniej. Takie programy, jak olimpiady tematyczne, konkursy z zakresu programowania i cyberbezpieczeństwa, a także specjalistyczne ścieżki kształcenia w szkołach ponadpodstawowych i na studiach wyższych, powinny być intensywnie wspierane i rozwijane. Równocześnie należy tworzyć systemy stypendialne oraz programy mentoringowe skierowane do uczniów i studentów, którzy przejawiają szczególne zainteresowanie tematyką bezpieczeństwa cyfrowego, umożliwiając im rozwój pod opieką doświadczonych specjalistów.

W kontekście dużej konkurencji na krajowym i międzynarodowym rynku pracy oraz wyraźnych dysproporcji w poziomie wynagrodzeń oferowanych specjalistom ds. cyberbezpieczeństwa w sektorze prywatnym i publicznym konieczne jest wdrożenie rozwiązań systemowych mających na celu zwiększenie atrakcyjności zatrudnienia w Polsce oraz w instytucjach publicznych. Różnice płacowe, sięgające niekiedy kilkuset procent, stanowią istotną barierę dla pozyskiwania i utrzymywania wykwalifikowanej kadry w administracji państwowej oraz sektorze bezpieczeństwa narodowego. Rozwiązaniem może być wspieranie rozwoju zawodowego poprzez tworzenie jasnych ścieżek awansu, systemów nagradzania osiągnięć oraz zapewnianie dostępu do zaawansowanych szkoleń specjalistycznych. Szczególne znaczenie ma także umożliwienie specjalistom udziału w międzynarodowych inicjatywach badawczych i projektowych, co nie tylko przyczynia się do wzrostu kompetencji, ale również ułatwia tworzenie sieci wymiany wiedzy.

6. Wprowadzenie powszechnie akceptowalnego systemu certyfikacji kompetencji dotyczących cyberbezpieczeństwa na różnych poziomach

Skuteczna identyfikacja oraz weryfikacja kompetencji w zakresie cyberbezpieczeństwa wymaga wprowadzenia powszechnie uznawanego, transparentnego systemu certyfikacji. Taki system powinien stanowić narzędzie umożliwiające zarówno standaryzację wiedzy i umiejętności, ułatwienie dla podmiotów prowadzących proces rekrutacji, jak i wsparcie w planowaniu ścieżek kariery zawodowej. Certyfikacja powinna obejmować różne poziomy zaawansowania – od podstawowych kompetencji użytkowników cyfrowych, przez umiejętności techniczne specjalistów średniego szczebla, aż po kwalifikacje eksperckie i zarządcze w zakresie strategicznego bezpieczeństwa informacji.

W procesie projektowania systemu certyfikacji istotne powinno być uwzględnienie już istniejących międzynarodowych standardów i dobrych praktyk, takich jak np. ramy kompetencji European e-Competence Framework (e-CF) czy zalecenia takich organizacji, jak ENISA, międzynarodowe konsorcjum certyfikacji bezpieczeństwa systemów informatycznych (ang. International Information System Security Certification Consortium – ISC2), międzynarodowe stowarzyszenie zajmujące się zagadnieniami dotyczącymi audytu, kontroli i bezpieczeństwa systemów informatycznych (ang. Information Systems Audit and Control Association – ISACA) czy EC-Council (ang. International Council of E-Commerce Consultants) – organizacja zajmująca się techniczną certyfikacją cyberbezpieczeństwa. Integracja krajowego systemu z uznanymi normami europejskimi i globalnymi pozwoli na zwiększenie jego wiarygodności oraz mobilności specjalistów na rynku pracy. Jednocześnie konieczne jest zapewnienie mechanizmu weryfikacji jakości szkoleń przygotowujących do uzyskania certyfikatów oraz instytucji nadających uprawnienia w celu zapewnienia wydawanym certyfikatом rzeczywistej wartości merytorycznej i rynkowej.

Certyfikaty powinny pełnić funkcję nie tylko dokumentu potwierdzającego kompetencje, ale również elementu motywacyjnego w procesie rozwoju zawodowego. System ten może być dodatkowo powiązany z programami stypendialnymi, ścieżkami awansu w sektorze publicznym, a także obowiązkami wynikającymi z określonych ról zawodowych w instytucjach odpowiedzialnych za bezpieczeństwo cyfrowe. Powszechne wykorzystanie certyfikatów może znacząco ułatwić monitorowanie poziomu przygotowania kadr w skali kraju oraz identyfikowanie luk kompetencyjnych.

W dłuższej perspektywie system certyfikacji może się przyczynić do rozwoju kadr w obszarze cyberbezpieczeństwa. Jego wdrożenie sprzyjać będzie zwiększeniu liczby i kwalifikacji specjalistów, poprawie jakości usług świadczonych w tym sektorze oraz lepszemu dopasowaniu kompetencji do wymagań organizacyjnych i strategicznych administracji publicznej, sektora prywatnego oraz instytucji międzynarodowych.

7. Rozwój działań informacyjnych i kampanii społecznych dotyczących szeroko rozumianego cyberbezpieczeństwa

System cyberbezpieczeństwa wymaga nie tylko technologicznych i organizacyjnych środków ochrony, lecz również odpowiednio ukształtowanej świadomości użytkowników systemów informacyjnych. W tym kontekście niezbędne jest podjęcie wielowymiarowych działań informacyjnych oraz kampanii społecznych, które w sposób przystępny i zrozumiały będą promować dobre praktyki w zakresie bezpiecznego korzystania z technologii cyfrowych.

Szczególnej uwagi wymagają grupy społeczne charakteryzujące się podwyższoną podatnością na zagrożenia w cyberprzestrzeni, takie jak dzieci i młodzież, osoby starsze oraz pracownicy małych i średnich przedsiębiorstw. W przypadku dzieci i młodzieży

działania powinny się koncentrować na promowaniu postaw odpowiedzialnego i bezpiecznego korzystania z Internetu, rozpoznawaniu dezinformacji, ochronie prywatności oraz przeciwdziałaniu przemocy realizowanej za pomocą elektronicznych środków komunikacji. W przypadku seniorów działania te powinny się skupiać na wzmacnianiu podstawowych kompetencji cyfrowych, rozpoznawaniu oszustw internetowych oraz umiejętności krytycznego odbioru treści w mediach cyfrowych. Natomiast sektor MŚP wymaga wsparcia informacyjnego w zakresie ochrony danych firmowych, wykrywania ataków phishingowych, stosowania mechanizmów uwierzytelniania oraz bezpiecznego zarządzania zasobami cyfrowymi.

Działania informacyjne powinny być prowadzone w sposób ciągły i zróżnicowany pod względem kanałów komunikacji. Wskazane jest łączenie kampanii medialnych z działaniami lokalnymi – warsztatami, prelekcjami, dystrybucją materiałów edukacyjnych czy organizacją dni bezpieczeństwa cyfrowego w szkołach, bibliotekach i urzędach. Wykorzystanie narzędzi, platform cyfrowych i języka dostosowanego do konkretnej grupy odbiorców, a także zaangażowanie liderów opinii i instytucji zaufania publicznego może istotnie zwiększyć skuteczność przekazu.

Dobrze zaprojektowane kampanie społeczne mają potencjał nie tylko edukacyjny, ale również profilaktyczny, pozwalają bowiem ograniczać skalę incydentów wynikających z błędów ludzkich, wzmacniają poczucie odpowiedzialności za bezpieczeństwo cyfrowe oraz kształtować kulturę cyberhigieny. Ich konsekwentna realizacja powinna stanowić integralny element krajowej strategii budowania kompetencji w zakresie cyberbezpieczeństwa.

8. Stworzenie systemu monitorowania i oceny poziomu kompetencji

W celu skutecznego zarządzania rozwojem kompetencji w zakresie cyberbezpieczeństwa niezbędne jest opracowanie zintegrowanego systemu monitorowania i oceny ich poziomu w skali krajowej. Brak spójnych i aktualnych danych dotyczących stanu kompetencji cyfrowych oraz specjalistycznych umiejętności w obszarze cyberbezpieczeństwa utrudnia zarówno planowanie polityki państwa w tym zakresie, jak i podejmowanie decyzji przez instytucje edukacyjne, pracodawców oraz decydentów odpowiedzialnych za bezpieczeństwo narodowe. Taki system powinien obejmować użytkowników końcowych (obywateli) i instytucje publiczne, sektor prywatny oraz środowiska akademickie.

Jednym z potencjalnych rozwiązań jest powiązanie systemu monitorowania z istniejącym indeksem DESI, który stanowi podstawowy instrument Komisji Europejskiej służący do oceny postępów państw członkowskich w zakresie rozwoju cyfrowego. Wykorzystanie go wymagałoby jego rozszerzenia lub uzupełnienia o szczegółowy komponent dotyczący kompetencji w zakresie cyberbezpieczeństwa, obejmujący zarówno umiejętności użytkowników, jak i specjalistyczne kwalifikacje zawodowe. Taki komponent mógłby zawierać m.in. wskaźniki dotyczące znajomości zasad bezpiecznego korzystania

z Internetu, udziału w szkoleniach i programach certyfikacyjnych, stosowania praktyk ochrony danych oraz zatrudnienia specjalistów ds. cyberbezpieczeństwa w instytucjach.

System powinien się opierać na badaniach ilościowych i jakościowych prowadzonych w sposób umożliwiający identyfikację luk kompetencyjnych w różnych grupach społecznych i zawodowych oraz określenie różnic na poziomie sektorowym, regionalnym i międzynarodowym. Szczególnie istotne jest uwzględnienie dynamiki zmian – badania powinny być prowadzone cyklicznie i umożliwiać śledzenie postępów w czasie, co pozwoli na ocenę skuteczności wdrażanych strategii i programów edukacyjnych, a także tworzenie prognoz dotyczących zapotrzebowania na określone kompetencje w przyszłości.

Pozyskane w ten sposób dane mogą służyć jako narzędzie wspierające planowanie edukacji, projektowanie kampanii informacyjnych oraz ocenę skuteczności programów finansowanych ze środków publicznych.

Wdrażając system monitorowania i oceny, należy też zapewnić jego interoperacyjność z innymi zbiorami danych wykorzystywanymi w politykach krajowych i unijnych.

System monitorowania powinien być zarządzany przez instytucję o odpowiednich kompetencjach analitycznych i merytorycznych, działającą w ścisłej współpracy z ministerstwami, uczelniami, organizacjami branżowymi i pracodawcami.

9. Współpraca międzysektorowa w zakresie identyfikacji potrzeb i rozwoju kompetencji

Budowa i rozwój kompetencji w zakresie cyberbezpieczeństwa wymagają ścisłej współpracy międzysektorowej, obejmującej sektor publiczny, prywatny i edukacyjny. Jedynie skoordynowane działania tych podmiotów pozwolą na zidentyfikowanie realnych potrzeb kompetencyjnych, odpowiednie zaprojektowanie treści edukacyjnych oraz wdrażanie rozwiązań dostosowanych do dynamicznie zmieniającego się środowiska cyfrowego. Współpraca ta powinna mieć charakter trwały, strukturalny i opierać się na jasno określonych mechanizmach koordynacji oraz wymiany informacji.

Szczególne znaczenie ma w tym kontekście wzmocnienie zaangażowania sektora prywatnego, który dysponuje najnowszą wiedzą technologiczną, praktycznym doświadczeniem w zarządzaniu incydentami bezpieczeństwa oraz znacznymi zasobami szkoleniowymi. Podmioty prywatne, szczególnie z branży informatycznej, finansowej i telekomunikacyjnej, mogą pełnić rolę partnerów w tworzeniu nowoczesnych programów edukacyjnych, dostarczaniu materiałów dydaktycznych, prowadzeniu szkoleń i warsztatów, a także oferowaniu staży oraz mentoringu dla uczniów, studentów i nauczycieli.

Ważne jest też aktywne uczestnictwo sektora edukacyjnego i naukowego w procesie identyfikacji trendów i prognozowanie zapotrzebowania na kompetencje w perspektywie średnio- i długoterminowej. Pozwoli to na opracowywanie programów nauczania,

które nie tylko odpowiadają bieżącym potrzebom rynku pracy, lecz również przygotowują do przyszłych wyzwań związanych z rozwojem technologii i ewolucją cyfrowych zagrożeń.

Istotne znaczenie powinien mieć także rozwój regionalnych i branżowych partnerstw na rzecz kompetencji cyfrowych, które mogą stanowić podstawę do tworzenia lokalnych sieci współpracy dostosowanych do specyfiki danego obszaru lub sektora gospodarki. Takie inicjatywy mogą być uzupełnieniem ogólnokrajowych działań strategicznych i przyczyniać się do wyrównywania dysproporcji terytorialnych.

Współpraca międzysektorowa w obszarze cyberbezpieczeństwa sprzyja większej spójności działań edukacyjnych i szkoleniowych, lepszemu wykorzystaniu zasobów, a także szybszemu wdrażaniu innowacyjnych rozwiązań. Jest również warunkiem niezbędnym dla stworzenia środowiska sprzyjającego trwałemu podnoszeniu kompetencji cyfrowych społeczeństwa oraz zwiększaniu bezpieczeństwa cyfrowego w warunkach szybko postępującej transformacji technologicznej.

10. Rozszerzenie współpracy międzynarodowej w zakresie rozwoju kompetencji

Rozwój kompetencji cyfrowych i cyberbezpieczeństwa w Polsce powinien być też wspierany poprzez intensyfikację działań na płaszczyźnie międzynarodowej. Współpraca międzynarodowa umożliwia dostęp do najnowszych badań, standardów, narzędzi edukacyjnych oraz praktyk stosowanych w innych państwach, a także stwarza warunki do integracji z europejską i globalną społecznością specjalistów ds. bezpieczeństwa cyfrowego. Tego rodzaju działania są szczególnie istotne w kontekście transgranicznego charakteru zagrożeń cybernetycznych, które wymagają koordynacji odpowiedzi na poziomie ponadnarodowym.

Jednym z kierunków rozwoju powinno być pogłębianie udziału Polski w takich inicjatywach Unii Europejskiej, jak działania prowadzone w ramach Europejskiej Akademii ds. Umiejętności Cyberbezpieczeństwa (European Cybersecurity Skills Academy), programu Cyfrowa Europa czy wspólnych przedsięwzięć badawczo-rozwojowych realizowanych przez Europejską Organizację ds. Cyberbezpieczeństwa. Udział w tych inicjatywach pozwala nie tylko na pozyskiwanie środków finansowych i wiedzy (*know-how*), lecz również na współtworzenie europejskich standardów edukacyjnych i zawodowych w obszarze cyberbezpieczeństwa.

Istotne jest także dalsze rozwijanie współpracy w ramach międzynarodowej sieci edukacyjnej, ze szczególnym uwzględnieniem obszaru kompetencji cyfrowych i cyberbezpieczeństwa. Programy wymiany studentów i kadry akademickiej, wspólne projekty badawcze oraz partnerstwa szkół wyższych z uczelniami zagranicznymi mogą znacząco podnieść jakość kształcenia i zwiększyć jego spójność z międzynarodowymi standardami. Korzyścią z takich działań jest też budowanie długoterminowych relacji i sieci eksperckich, które mogą wspierać polskie instytucje w działaniach prewencyjnych,

reagowaniu na incydenty oraz w tworzeniu innowacyjnych rozwiązań w zakresie ochrony infrastruktury cyfrowej.

Współpraca międzynarodowa wpływa także na usprawnienie transferu wiedzy dotyczącej skutecznych modeli kształcenia i certyfikacji, a tym samym przyczynia się do zwiększenia spójności działań Polski z europejskim systemem bezpieczeństwa cyfrowego.

11. Opracowanie systemu finansowania wspierającego rozwój kompetencji

Rozwój kompetencji w zakresie cyberbezpieczeństwa nie jest możliwy bez stworzenia trwałych i stabilnych mechanizmów finansowania, które będą wspierać zarówno inicjatywy instytucjonalne, jak i indywidualne ścieżki kształcenia. W tym celu konieczne jest opracowanie zintegrowanego systemu finansowania, który będzie łączył środki publiczne, prywatne oraz instrumenty zachęt fiskalnych i regulacyjnych. Spójny system wsparcia finansowego umożliwi osiągnięcie trwałych efektów w zakresie budowy kompetencji społeczeństwa informacyjnego oraz zwiększenia liczby specjalistów i rozwoju rynku pracy w sektorze cyberbezpieczeństwa.

Środki publiczne, zarówno krajowe, jak i unijne, powinny być wykorzystywane przede wszystkim do wspierania systemowych działań edukacyjnych, takich jak tworzenie programów nauczania, finansowanie infrastruktury dydaktycznej, szkolenia nauczycieli, rozwój zasobów otwartych oraz prowadzenie badań nad kompetencjami i zagrożeniami cyfrowymi. Fundusze unijne w ramach takich programów, jak Fundusze Europejskie dla Rozwoju Społecznego (FERS), Horyzont Europa, Cyfrowa Europa czy Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), mogą stanowić istotne źródło finansowania projektów o zasięgu regionalnym i krajowym, w tym także partnerstw międzysektorowych.

Obok wykorzystania środków publicznych niezbędny jest rozwój mechanizmów współfinansowania przez sektor prywatny działań w zakresie rozwoju kompetencji swoich pracowników oraz wspierania inicjatyw edukacyjnych, stażowych i mentoringowych. W tym kontekście niezbędne wydaje się wprowadzenie odpowiednich zachęt – np. ulg podatkowych dla firm finansujących szkolenia w obszarze cyberbezpieczeństwa, grantów partnerskich czy preferencyjnych warunków współpracy z instytucjami edukacyjnymi i badawczymi.

Aby zwiększyć efektywność wykorzystania dostępnych zasobów, konieczne jest ułatwienie dostępu do informacji o potencjalnych źródłach finansowania oraz zapewnienie ich lepszej koordynacji. W tym celu uzasadnione jest utworzenie repozytorium, które gromadziłoby dane na temat aktualnych naborów, zasad ubiegania się o środki, przykładów dobrych praktyk oraz mechanizmów wsparcia dostępnych dla instytucji edukacyjnych, administracji, sektora prywatnego i osób indywidualnych. Zbierane w ten sposób informacje mogłyby stanowić jeden z elementów platformy koordynującej działania

edukacyjne, wskazanej w ramach rekomendacji nr 2, i tym samym ułatwić wymianę informacji pomiędzy instytucjami zarządzającymi poszczególnymi programami finansowymi oraz beneficjentami, co w konsekwencji pozwoliłoby na lepsze planowanie i efektywne wykorzystanie zasobów.

System finansowania powinien być zaprojektowany w sposób elastyczny i długofalowy, umożliwiający szybkie reagowanie na zmieniające się potrzeby rynku pracy, rozwój technologii oraz nowe zagrożenia w cyberprzestrzeni. Jego skuteczność będzie zależeć od przejrzystych zasad dystrybucji środków, efektywnego monitorowania efektów oraz spójności z celami krajowej strategii rozwoju kompetencji cyfrowych.

Przedstawione rekomendacje mają na celu wzmocnienie kompetencji społeczeństwa oraz zwiększenie liczby specjalistów w dziedzinie cyberbezpieczeństwa w Polsce. Obejmują one zarówno modernizację strategii krajowych, poprawę zarządzania i koordynacji, jak i rozwój nowoczesnych programów edukacyjnych, wspieranie talentów, edukację nieformalną oraz certyfikację umiejętności. Uwzględniona została również konieczność prowadzenia badań nad motywacjami specjalistów, rozwijania współpracy międzysektorowej i międzynarodowej, prowadzenia kampanii informacyjnych oraz stworzenia systemu monitorowania poziomu kompetencji. Istotnym elementem powinna stać się także poprawa dostępu do informacji o możliwych źródłach finansowania oraz ich lepsza koordynacja.

Wprowadzenie tych działań pozwoli na zbudowanie spójnego i elastycznego ekosystemu kompetencji, odpowiadającego na rosnące potrzeby gospodarki, administracji i społeczeństwa w warunkach dynamicznych zmian technologicznych. Rezultatem będzie zwiększenie poziomu bezpieczeństwa cyfrowego państwa, wzrost konkurencyjności na rynku pracy, skuteczniejsza ochrona obywateli przed zagrożeniami w sieci oraz większa odporność instytucji publicznych na incydenty cybernetyczne. Rekomendacje te powinny stanowić fundament długofalowej polityki rozwoju kompetencji w obszarze kluczowym dla współczesnego państwa i jego obywateli.

Podsumowanie

Współczesne państwa, społeczeństwa i organizacje coraz bardziej polegają na technologiach cyfrowych, co powoduje, że cyberbezpieczeństwo staje się jednym z kluczowych wyzwań naszych czasów. Z postępującą cyfryzacją związanych jest wiele korzyści, jednak jej rozwój niesie ze sobą nowe zagrożenia, które dotyczą nie tylko sfery technologicznej, ale również informacyjnej, społecznej i politycznej. W ostatnich latach znacząco wzrosła liczba incydentów, cyberataków, naruszeń danych, a także przypadków dezinformacji wykorzystywanej do wywierania wpływu na opinię publiczną. Międzynarodowe konflikty i napięcia powodują, że coraz częstsze są przypadki sponsorowanych przez państwa ataków, które wymierzone są w infrastrukturę krytyczną, instytucje publiczne czy systemy wyborcze. Zjawiska te pokazują, że cyberprzestrzeń stała się nie tylko środowiskiem, w którym prowadzona jest aktywność przestępcza, ale również areną konfliktów geopolitycznych.

W dobie coraz bardziej wyrafinowanych i zautomatyzowanych ataków niezbędna staje się zmiana podejścia do ochrony systemów informatycznych. Tradycyjne działania polegające głównie na zapobieganiu atakom okazują się niewystarczające, ponieważ jak pokazują doświadczenia, nie można uniknąć wszystkich incydentów ani całkowicie wyeliminować ryzyka cyberataków.

Z tego powodu, równoległe do zapewnienia cyberbezpieczeństwa, konieczne jest rozwijanie cyberodporności, czyli zdolności do szybkiego reagowania na incydenty, ograniczania ich skutków oraz przywracania sprawności systemów po zakłóceniach. Podejście to obejmuje identyfikację zagrożeń, stosowanie zabezpieczeń, monitorowanie, skuteczne reagowanie oraz odbudowę i ciągłe doskonalenie narzędzi, systemów i procedur.

Rozwój systemów ochrony opiera się obecnie nie tylko na technologiach i procedurach, ale też na regulacjach prawnych oraz współpracy między państwami. W ostatnich latach w systemie prawnym Unii Europejskiej i krajów członkowskich zaimplementowano wiele regulacji, których celem jest podniesienie poziomu cyberbezpieczeństwa i cyberodporności. Przykładem są takie akty prawne, jak dyrektywa NIS2, Akt o cyberbezpieczeństwie, Akt o cybersolidarności, DORA, Akt o odporności cyfrowej oraz Akt o sztucznej inteligencji. Polska wdraża te regulacje do krajowego porządku prawnego, dostosowując systemy zarządzania cyberbezpieczeństwem do nowych wymagań i zmieniającego się krajobrazu zagrożeń. Wzmacniana jest rola instytucji odpowiedzialnych

za cyberbezpieczeństwo, w tym zespołów reagowania na incydenty (CSIRT), a także zwiększany jest zakres obowiązków najważniejszych podmiotów i organizacji w obszarach dotyczących oceny ryzyka, wdrażania zabezpieczeń, raportowania incydentów oraz szkoleń pracowników. Równocześnie rozwijane są systemy certyfikacji, które pozwalają na weryfikację poziomu zabezpieczeń produktów cyfrowych i usług.

Zagrożenia, z jakimi mierzy się współczesna cyberprzestrzeń, zmieniają się w szybkim tempie. Rozwój sztucznej inteligencji, Internetu Rzeczy i systemów automatyzacji sprawia, że pojawiają się nowe metody ataków i podatności. Rośnie zagrożenie i skutki ataków na łańcuchy dostaw, infrastrukturę przemysłową i usługi cyfrowe. Wraz z rozwojem elektronicznych środków komunikacji coraz poważniejszym zagrożeniem staje się dezinformacja, która może być wykorzystywana do manipulowania opinią publiczną, osłabiania zaufania do instytucji publicznych i destabilizacji systemów demokratycznych. Nowe zagrożenia wymagają nieustannej adaptacji środków ochronnych oraz aktualizacji polityk i procedur bezpieczeństwa.

Obok rozwiązań technicznych, regulacji prawnych i procedur kluczowym elementem skutecznego systemu cyberbezpieczeństwa stają się kompetencje cyfrowe społeczeństwa. Umiejętność bezpiecznego korzystania z technologii, rozpoznawania zagrożeń i stosowania podstawowych zasad ochrony danych jest niezbędna nie tylko dla jednostek, ale również dla instytucji i gospodarki. Wysoki poziom kompetencji w tym zakresie przyczynia się do zwiększenia odporności na wszystkich poziomach funkcjonowania państwa. Szczególnie istotne jest podnoszenie świadomości zagrożeń oraz rozwijanie umiejętności technicznych wśród pracowników sektora publicznego, edukacyjnego oraz małych i średnich przedsiębiorstw. Niezbędna jest też integracja działań edukacyjnych prowadzonych w różnych obszarach systemu kształcenia, w tym edukacji formalnej, szkoleń zawodowych oraz platform edukacyjnych umożliwiających samokształcenie.

W celu określenia poziomu wiedzy i umiejętności mieszkańców Polski w zakresie cyberbezpieczeństwa autor monografii przeprowadził badanie ankietowe na ogólnopolskiej próbie dorosłych osób w wieku produkcyjnym. Objęło ono różnorodne grupy społeczne i zawodowe, a jego celem było zdiagnozowanie poziomu świadomości, źródeł wiedzy oraz umiejętności praktycznych w zakresie cyberbezpieczeństwa.

Z uzyskanych danych wynika, że zdecydowana większość Polaków ma świadomość zagrożeń i jest przekonana, że liczba zagrożeń cyfrowych rośnie. Jednocześnie znaczna część respondentów deklaruje niewystarczający poziom wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. Problem ten w znacznym stopniu wynika z faktu, że system edukacji nie dostarcza wystarczającej wiedzy w zakresie cyberbezpieczeństwa, a respondenci w przeważającej większości czerpali wiedzę na temat cyberbezpieczeństwa z popularnych, łatwo dostępnych, lecz niekoniecznie wiarygodnych źródeł, takich jak media społecznościowe czy rozmowy z innymi osobami.

Wielu uczestników badania zadeklarowało stosowanie podstawowych środków ochrony, jak uwierzytelnianie dwuskładnikowe, aktualizacje oprogramowania czy

korzystanie z oprogramowania antywirusowego, jednak wiedza na temat bardziej zaawansowanych narzędzi i zagrożeń pozostaje niska.

W badaniu uwzględniono także pytanie o chęć poszerzenia wiedzy z zakresu cyberbezpieczeństwa. Znaczna część respondentów zadeklarowała chęć poszerzania wiedzy, co wskazuje na istotny potencjał społeczny do rozwoju kompetencji cyberbezpieczeństwa.

Należy zwrócić uwagę, że niski poziom kompetencji cyfrowych i specjalistycznych przekłada się bezpośrednio na rynek pracy. W Polsce brakuje obecnie tysięcy specjalistów z zakresu cyberbezpieczeństwa, co utrudnia rozwój nowoczesnych sektorów gospodarki, osłabia bezpieczeństwo instytucji publicznych i obniża konkurencyjność kraju na tle innych państw Unii Europejskiej. Deficyt kadr jest zauważalny zarówno w sektorze prywatnym, jak i publicznym, a luka kompetencyjna powiększa się z roku na rok.

W oparciu o przeprowadzone badanie, analizę danych obrazujących aktualny poziom kompetencji cyfrowych i kompetencji cyberbezpieczeństwa oraz przegląd prowadzonych w Polsce i w Unii Europejskiej działań edukacyjnych autor przedstawił szereg rekomendacji mających na celu poprawę sytuacji. Zalecenia te zawierają m.in. konieczność budowy systemu certyfikacji kompetencji w zakresie cyberbezpieczeństwa, wsparcia szkół i uczelni w kształceniu specjalistów, rozwijania współpracy publiczno-prywatnej oraz tworzenia zachęt do podnoszenia kwalifikacji przez pracowników i obywateli. Jako istotne wskazano również regularne badanie poziomu kompetencji oraz ocenę skuteczności wdrażanych programów edukacyjnych. W ramach podejmowanych działań niezbędne jest uwzględnienie specyfiki różnych grup demograficznych i zawodowych, a także wsparcie dla samorządów i podejmowanych lokalnie inicjatyw edukacyjnych.

Wobec szybko zmieniającego się środowiska technologicznego i rosnących zagrożeń, konieczne jest kontynuowanie badań nad kompetencjami cyfrowymi, ich wpływem na poziom cyberbezpieczeństwa oraz skutecznością wdrażanych polityk publicznych. Uzyskane wyniki takich badań pozwolą na zaprojektowanie skutecznych strategii i działań operacyjnych, które w efekcie podniosą poziom bezpieczeństwa i odporności cyfrowej państwa i społeczeństwa. Badania takie powinny być prowadzone systematycznie, obejmując nie tylko poziom wiedzy i umiejętności, ale również zmiany postaw i zachowań użytkowników w przestrzeni cyfrowej.

Spis rysunków i tabel

Rysunek 1. Filary cyberodporności.....	30
Rysunek 2. Liczba incydentów zarejestrowanych przez ENISA w latach 2012–2024	88
Rysunek 3. Liczba incydentów zarejestrowanych przez CERT Polska w latach 2012–2024	89
Rysunek 4. Struktura respondentów ze względu na płeć	110
Rysunek 5. Struktura respondentów pod względem województwa.....	110
Rysunek 6. Struktura respondentów pod względem wykształcenia	111
Rysunek 7. Struktura respondentów pod względem wieku.....	111
Rysunek 8. Struktura respondentów pod względem wielkości miejsca zamieszkania (liczba mieszkańców)	111
 Tabela 1. Systematyka incydentów komputerowych eCSIRT.net mkVI.....	 27
Tabela 2. Porównanie zakresu i charakteru różnych dokumentów tworzących formalne ramy cyberbezpieczeństwa.....	59

Bibliografia

Pozycje zwarte i artykuły w czasopismach

- Adams A., Sasse M.A., *Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures*, „Communications of the ACM” 1999, no. 42(12).
- Aldhamer M., *The Impact of Artificial Intelligence on the Future of Cybersecurity*, „Multi-Knowledge Electronic Comprehensive Journal for Education & Science Publications” 2024, no. 71.
- AlSalem T.S., Almaiah M.A., Lutfi A., *Cybersecurity Risk Analysis in the IoT: A Systematic Review*, „Electronics” 2023, no. 12(18).
- Antczak J., Kos M., *Cybersecurity of ICT systems in the era of widespread digitization*, „Nowoczesne Systemy Zarządzania” 2022, nr 17(3).
- Arroyabe M.F., Arranz C.F.A., Fernandez de Arroyabe I., Fernandez de Arroyabe J.C., *The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges*, „Technological Forecasting and Social Change” 2023, no. 199.
- Brundage M., Avin S., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., Scharre P., Zeitzoff T., Filar B., Roff H., Allen G., Steinhardt J., Flynn C., O’Heigeartaigh S., Beard S., Belfield H., Farquhar S., Amodei D., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018.
- Budziewicz-Guźlecka A., *Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych*, Szczecin 2019.
- Chen P., Desmet L., Huygens C., *A Study on Advanced Persistent Threats* [w:] *Communications and Multimedia Security*, red. B. De Decker, A. Zúquete, Berlin–Heidelberg 2014.
- Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej” 2016, t. 3, nr 2(10).
- Clarke R., *Big Data, Big Risks*, „Information Systems Journal” 2016, no. 26(1).
- Cornish P. (red.), *The Oxford Handbook of Cyber Security*, 2021.
- Craig D., Diakun-Thibault N., Purse R., *Defining Cybersecurity*, „Technology Innovation Management Review” 2014.
- Drab-Kurowska A., Budziewicz-Guźlecka A., *The Digital Post Ecosystem – Example of Poland in the Context of Research*, „Sustainability” 2021, no. 13(5).

- Fricker R.D., Schonlau M., *Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature*, „Field Methods” 2002, no. 14(4).
- Gawkowski K., *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka Komisji Politologii i Stosunków Międzynarodowych” 2018, nr 2.
- Górka M., *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, „Przegląd Geopolityczny” 2018, nr 25.
- Gwebu K.L., Wang J., Wang L., *The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management*, „Journal of Management Information Systems” 2018, no. 35.
- Hansman S., Hunt R., *A taxonomy of network and computer attacks*, „Computers & Security” 2005, no. 24.
- Herley C., *So long, and no thanks for the externalities: the rational rejection of security advice by users. Proceedings of the New Security Paradigms Workshop (NSPW)*, ACM 2009.
- Horváth D., Szabó R.Z., *Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?*, „Technological Forecasting and Social Change” 2019, no. 146.
- Jouini M., Ben Arfa Rabai L., Ben Aissa A., Ben L., *Classification of security threats in information systems*, „Procedia Computer Science” 2014, vol. 32.
- Kaiser F., Wiens M., Schultmann F., *Motivation-based Attacker Modelling for Cyber Risk Management: A Quantitative Content: Analysis and a Natural Experiment*, „Journal of Information Security and Cybercrimes Research” 2021, no. 4.
- Kamiya S., Jun-Koo K., Jungmin K., Milidonis A., Stulz R.M., *Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms*, „Journal of Financial Economics” 2021, no. 139(3).
- Krapp P., *Terror and Play, or What was Hacktivism?*, „Grey Room” 2015, no. 21.
- Lemay A., Calvet J., Menet F., Fernandez J.M., *Survey of publicly available reports on advanced persistent threat actors*, „Computers & Security” 2018, no. 72.
- Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce: Wybrane zagadnienia*, „European Association for Security” 2016.
- Mazhar A., Khan S.U., Vasilakos A.V., *Security in cloud computing: Opportunities and challenges*, „Information Sciences” 2015, no. 305.
- Meneghello F., Matteo C., Zucchetto D., Polese M., Zanella A., *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*, „Internet of Things Journal” 2019, vol. 6, issue 1.
- Mulder M., *Conceptions of Professional Competence [w:] International Handbook of Research in Professional and Practice Based Learning*, red. S. Billett, C. Harteis, H. Gruber, Springer 2014.
- Olszewski B., Rot A., *Advanced Persistent Threat attacks as a new cybersecurity threat*, „Informatyka Ekonomiczna – Business Informatics” 2016, nr 2(40).
- Rabitti G., Khorrami Chokami A., Coyle P., Cohen R.D., *A taxonomy of cyber risk taxonomies*, „Risk Analysis” 2014.

- Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R., *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, „National Institute of Standards and Technology” 2021.
- Sajdak M. (red.), *Wprowadzenie do bezpieczeństwa IT*, t. 1, Kraków 2023.
- Saltier J.H., Schroeder M.D., *Protection of information in computer systems*, „IEEE” 1975, no. 3(12).
- Stallings W., Brown L., *Computer security: Principles and practice*, Pearson 2018.
- Stoddart K., *Russia's Cyber Campaigns and the Ukraine War: From the Gray Zone to the Red Zone*, „Applied Cybersecurity & Internet Governance” 2024.
- Syafrizal M., Selamat S.R., Zakaria N.A., *AVOIDITALS: Enhanced Cyber-attack Taxonomy in Securing Information Technology Infrastructure*, „International Journal of Computer Science and Network Security” 2021, vol. 21, no. 8.
- Vial G., *Understanding Digital Transformation: A Review and a Research Agenda*, „The Journal of Strategic Information Systems” 2019, no. 28(2).
- Vogel E., Dyka E.Z., Klann D., Langendörfer P., *Resilience in the Cyberworld: Definitions, Features and Models*, „Future Internet” 2021, no. 13(11).
- Von Solms R., *Information security management (3): the Code of Practice for Information Security Management (BS 7799)*, „Information Management & Computer Security” 1998, vol. 6, no. 5.
- Von Solms R., Van Niekerk J., *From information security to cyber security*, „Computers & Security” 2013, no. 38.
- Vuorikari R., Kluzer S., Punie Y., *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg 2022.
- Whitten A., Tygar D., *Why Johnny can't encrypt: A usability evaluation of pgp 5.0* [w:] *Proceedings of the 8th conference on USENIX Security Symposium*, vol. 8, USENIX Association, USA 1999.
- Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary. Automatyka. Robotyka” 2013, R. 17, nr 2.

Akty prawne

- Dyrektywa 2002/58/WE parlamentu europejskiego i rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), 13, 029 DD § (2002). <http://data.europa.eu/eli/dir/2002/58/oj/pol>.
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, 13, 015 DD § (1995). <http://data.europa.eu/eli/dir/1995/46/oj/pol>.

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, 194 OJ L § (2016). <http://data.europa.eu/eli/dir/2016/1148/oj/pol>.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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 uchylającą dyrektywę (UE) 2016/1148, OJ L (2022). <http://data.europa.eu/eli/dir/2022/2555/oj/pol>.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającą dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG). <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/pol>.
- Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji Tekst mający znaczenie dla EOG., 01, 005 DD § (2004). <http://data.europa.eu/eli/reg/2004/460/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2025/38 z 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (2024). <http://data.europa.eu/eli/reg/2025/38/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Tekst mający znaczenie dla EOG), 119 OJ L § (2016). <http://data.europa.eu/eli/reg/2016/679/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, 151 OJ L (2019). <http://data.europa.eu/eli/reg/2019/881/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, 333 OJ L § (2022). <http://data.europa.eu/eli/reg/2022/2554/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Tekst mający znaczenie dla EOG), 152 OJ L § (2022). <http://data.europa.eu/eli/reg/2022/868/oj/pol>.

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Tekst mający znaczenie dla EOG) (2023). <http://data.europa.eu/eli/reg/2023/2854/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (2024). <http://data.europa.eu/eli/reg/2024/1689/oj/pol>.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Tekst mający znaczenie dla EOG) (2024). <http://data.europa.eu/eli/reg/2024/2847/oj/pol>.
- 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. 2024 poz. 773. <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240000773>.
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037>.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000>.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, nr 64, poz. 565). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20050640565>.
- Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. 2023, poz. 1703). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001703>.
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2022, poz. 1863 ze zm.).
- Ustawa z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz.U. 2023, poz. 1394). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001394>.
- Zalecenie Rady w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, 22 maja 2018 r., ST 9009 2018 INIT. [https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018H0604(01)).

Inne źródła

- #CyberMagazyn: *Gdzie można studiować cyberbezpieczeństwo?*, <https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-gdzie-mozna-studiowac-cyberbezpieczenstwo> (25.04.2025).
- 100 Chilling Malware Statistics & Trends (2023–2025), <https://controld.com/blog/malware-statistics-trends/> (7.01.2025).
- 2024 rokiem ransomware. Polskie instytucje na celowniku, <https://businessjournal.pl/2024-rokiem-ransomware-polskie-instytucje-na-celowniku/> (19.03.2025).
- 2025 Identity Theft Facts and Statistics, <https://identitytheft.org/statistics/> (27.03.2025).
- Advanced Persistent Threats (Ataki APT), <https://www.comcert.pl/slownik/advanced-persistent-threats-apt/> (7.03.2025).
- Adyen Retail Report Poland 2024, https://www.adyen.com/pl_PL/index-reports/retail (17.03.2025).
- Ataki DDoS coraz groźniejsze, 2021, <https://biznes.t-mobile.pl/pl/ataki-ddos-coraz-grozniesze> (17.03.2025).
- Bezpieczeństwo w sieci – Co to jest, główne zagrożenia, szyfrowanie, segmentacja sieci i polityka bezpieczeństwa, <https://nflo.pl/baza-wiedzy/bezpieczenstwo-w-sieci/#dlaczego-segmentacja-sieci-jest-wazna-dla-bezpieczenstwa> (13.04.2025).
- Boosting your Organization's Cyber resilience – Joint Publication, 2022, <https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience> (8.03.2025).
- Britain lands at the top of global identity theft, <https://thepaypers.com/payments-general/britain-lands-at-the-top-of-global-identity-theft--1265445> (2.02.2025).
- Check Point, *Cloud Security Report 2024*, <https://engage.checkpoint.com/2024-cloud-security-report/> (6.04.2025).
- Closing The Cybersecurity Skills Gap: Strategies for Employers and Aspiring Professionals, <https://www.cybrary.it/blog/closing-cybersecurity-skills-gap> (10.04.2025).
- Cloud Security Guide for SMEs, 2015, <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes> (8.03.2025).
- CNSS, *National Information Assurance Glossary*, 2010, https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf (3.12.2024).
- Co NIS2 mówi o tworzeniu kopii zapasowych?, <https://arkanet.pl/baza-wiedzy/co-nis2-mowi-o-tworzeniu-kopii-zapasowych/> (15.04.2025).
- Co to jest SIEM – Security Information and Event Management? Definicja, komponenty, korzyści i wyzwania, <https://nflo.pl/baza-wiedzy/co-to-jest-siem-security-information-and-event-management-definicja-komponenty-korzysci-i-wyzwania/> (13.04.2025).
- Co to jest tworzenie kopii zapasowych?, <https://nflo.pl/slownik/tworzenie-kopii-zapasowych/> (13.04.2025).
- Co wybrać: SOAR czy SIEM? Różnice i czynniki ważne podczas wyboru, <https://nflo.pl/baza-wiedzy/co-wybrac-soar-czy-siem-roznice-i-czynniki-wazne-podczas-wyboru/> (13.04.2025).

- Co z podatkiem cyfrowym i strategią cyberbezpieczeństwa?*, <https://cyberdefence24.pl/cyberbezpieczenstwo/co-z-podatkiem-cyfrowym-i-strategia-cyberbezpieczenstwa> (23.04.2025).
- CompTIA Certifications*, <https://www.comptia.org/certifications> (19.04.2025).
- Current developments on DigComp (2024–2025)*, https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/current-developments-digcomp-2024-2025_en (19.04.2025).
- Cyber Safety Tips for Small Business Owners*, <https://www.sba.gov/blog/2023/2023-09/cyber-safety-tips-small-business-owners> (12.02.2025).
- Cyberataki na infrastrukturę krytyczną w Polsce – zagrożenia dla systemów ICS/OT, 2025*, <https://aspolska.pl/ataki-i-cyberataki-na-infrastrukture-krytyczna-w-polsce-zagrozenia-dla-systemow-ics-ot/> (21.03.2025).
- Cyberbezpieczeństwo w 2025 roku: kluczowe wsparcie dla samorządów*, <https://samorząd.pap.pl/kategoria/e-urząd/cyberbezpieczenstwo-w-2025-roku-kluczowe-wsparcie-dla-samorzadow> (26.04.2025).
- Cyberbezpieczeństwo w szkole*, <https://www.rodosfera.pl/post/cyberbezpieczenstwo-w-szkole> (23.04.2025).
- Cybersecurity History: Hacking & Data Breaches*, <https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches> (29.10.2024).
- Cyfrowa dekada Europy: cele cyfrowe na 2030 r.*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl (19.04.2025).
- Czym jest CVE (Common Vulnerabilities and Exposures)? – kluczowe informacje*, <https://nflo.pl/baza-wiedzy/czym-jest-cve/#jaka-jest-relacja-miedzy-cve-a-cvss> (2.04.2025).
- Czym jest ochrona przed utratą danych (DLP)?*, <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-data-loss-prevention-dlp> (15.04.2025).
- Czym jest zarządzanie podatnościami IT (Vulnerability Management) i dlaczego jest kluczowe dla cyberbezpieczeństwa?*, <https://nflo.pl/baza-wiedzy/czym-jest-zarzadzanie-podatnosciami-it-vulnerability-management-i-dlaczego-jest-kluczowe-dla-cyberbezpieczenstwa/> (13.04.2025).
- Dezinformacja oczami Polaków, 2024*, <https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a32-02a26c324f18> (26.03.2025).
- Digital Competence Framework for Citizens (DigComp)*, https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en (19.04.2025).
- Domańska E., *Dezinformacja – czym jest i jak ją zweryfikować*, https://cyberprofilaktyka.pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html (24.03.2025).
- Edukacja cyfrowa dzieci. Co planuje rząd?*, <https://cyberdefence24.pl/cyberbezpieczenstwo/edukacja-cyfrowa-dzieci-co-planuje-rzad> (23.04.2025).

- EITM, *The Rise of Quantum Computing: What It Means for Cybersecurity*, 2024, <https://www.eimt.edu.eu/the-rise-of-quantum-computing-what-it-means-for-cybersecurity> (7.04.2025).
- ENISA, *2024 Report on the State of Cybersecurity in the Union. European Union Agency for Cybersecurity*, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (28.04.2025).
- ENISA, *2024 Report on the State of the Cybersecurity in the Union*, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (12.03.2025).
- ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2019, <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity> (15.04.2025).
- ENISA, *Cybersecurity Education Maturity Assessment*, 2024, <https://www.enisa.europa.eu/publications/cybersecurity-education-maturity-assessment> (22.04.2025).
- ENISA, *Threat Landscape 2024*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (15.03.2025).
- ENISA, *Threat Landscape for Supply Chain Attacks*, 2021, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks> (24.03.2025).
- Eurobarometr, *Cyberskills*, 2024, https://data.europa.eu/data/datasets/s3176_fl547_eng?locale=en (28.04.2025).
- European Commission, *Digital skills initiatives*, <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-initiatives> (22.04.2025).
- European Cybersecurity Skills Framework (ECSF), <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf> (22.04.2025).
- Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC), <https://www.gov.pl/web/cyber-nccpl/eccc> (22.04.2025).
- Europol, *Internet Organised Crime Threat Assessment*, 2023, <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023> (10.04.2025).
- Eurostat, 2024, https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/bar?lang=en (28.04.2025).
- Eurostat, *Cloud computing – statistics on the use by enterprises*, 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises (4.04.2025).
- Eurostat, *How many people verified online information in 2021?*, <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211216-3> (26.03.2025).
- EY Future Consumer Index 2023, https://www.ey.com/pl_pl/newsroom/2023/07/ey-fci-bezpieczenstwo-danych (19.03.2025).
- FIDO Authentication, *A passwordless vision*, <https://fidoalliance.org/fido2/> (12.04.2025).

- Fundusze Europejskie na Rozwój Cyfrowy 2021–2027*, <https://www.polskacyfrowa.gov.pl/strony/o-programie/fundusze-europejskie-na-rozwoj-cyfrowy-2021-2027-2028/> (26.04.2025).
- Gartner Forecasts Worldwide Public Cloud End-User Spending to Total \$723 Billion in 2025*, <https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025> (4.04.2025).
- Group-IB, *High-Tech Crime Trends Report 2025*, <https://www.group-ib.com/landing/high-tech-crime-trends-2025/> (22.03.2025).
- History of Cybersecurity: An Overview*, <https://keepnetlabs.com/blog/cybersecurity-breaches-lessons-from-history> (17.11.2024).
- Incident Classification/Incident Taxonomy according to eCSIRT.net – adapted*, <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf> (20.02.2025).
- ITRC, *2023 Annual Data Breach Report*, <https://www.idtheftcenter.org/publication/2023-data-breach-report/> (24.03.2025).
- Jakie zasady wprowadza DORA? – Kompletny przegląd regulacji*, <https://nflo.pl/baza-wiedzy/jakie-zasady-wprowadza-dora-kompletny-przegląd-regulacji/> (10.03.2025).
- Jesteśmy coraz bardziej świadomi zagrożeń w sieci*, 2022, <https://polska.googleblog.com/2022/11/jestesmy-coraz-bardziej-swiadomi.html/> (28.04.2025).
- Joint Declaration on EU-NATO Cooperation*, https://www.nato.int/cps/en/natohq/official_texts_156626.htm (16.03.2025).
- Kompendium wiedzy – IDS i IPS*, <https://whitehats.pwr.edu.pl/research/kompendium-ids-ips/> (13.04.2025).
- Kompetencje cyfrowe*, 2020, <https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe> (18.04.2025).
- Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa ws. ataków na przemysłowe systemy sterowania, <https://www.gov.pl/web/cyfryzacja/komunikat-pełnomocnika-rządu-do-spraw-cyberbezpieczeństwa-ws-ataków-na-przemysłowe-systemy-sterowania3> (15.04.2025).
- Konwencja Rady Europy o Cyberprzestępczości, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4656911> (15.03.2025).
- KPMG, *Barometr cyberbezpieczeństwa*, 2024, <https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpieczeństwa-2024.pdf> (27.04.2025).
- KPMG, *Quantum is coming – and bringing new cybersecurity threats with it*, <https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html> (7.04.2025).
- Krajobraz bezpieczeństwa polskiego Internetu w 2024 roku*, 2025, https://cert.pl/uploads/docs/Raport_CP_2024.pdf (25.04.2025).

- Kulas T., *Komputery kwantowe zmienią świat biznesu. Jak przygotować firmę?*, „MIT Sloan Management Review Polska”, 19 sierpnia 2019, <https://mitsmr.pl/b/komputery-quantowe-zmienia-swiat-biznesu-jak-przygotowac-firme/P11m4TmHH> (7.04.2025).
- Lewis J.A., *Cybersecurity and Critical Infrastructure Protection*. Washington, D.C. 2006, <http://csis.org/publication/cybersecurity-and-criticalinfrastructure-protection> (22.11.2024).
- Makosz I., *Jakie przedsiębiorstwa obejmie nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa*, 2025, <https://www.prawo.pl/podatki/jakie-przedsiębiorstwa-objemie-nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa,531171.html> (19.01.2025).
- Microsoft *Digital Defense Report 2024*, <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024> (19.03.2025).
- Ministerstwo Cyfryzacji zamierza wydać 10 mld zł na cyberbezpieczeństwo, https://www.pap.pl/aktualnosci/ministerstwo-cyfryzacji-zamierza-wydac-10-mld-zl-na-cyberbezpieczenstwo?utm_source=chatgpt.com (26.04.2025).
- Najważniejsze cyberzagrożenia na 2025 r. Wyzwaniem komputery kwantowe, <https://businessinsider.com.pl/technologie/nowe-technologie/najwazniejsze-cyberzagrozenia-na-2025-r-wyzwaniem-komputery-quantowe/ph05lhe> (12.04.2025).
- NASK, *Dezinformacja, fake newsy i cyberzagrożenia – czy nasze wybory są bezpieczne?*, <https://nask.pl/aktualnosci/dezinformacja-fake-newsy-i-cyberzagrozenia-czy-nasze-wybory-sa-bezpieczne/> (26.03.2025).
- National Institute of Standards and Technology – glossary, <https://csrc.nist.gov/glossary/term/threat> (14.01.2025).
- National Institute of Standards and Technology, *Framework for improving critical infrastructure cybersecurity: Version 1.0*, 2014, <https://www.nist.gov/document/cybersecurity-framework-021214pdf> (12.12.2024).
- Nieles M., Dempsey K., Pillitteri V.Y., *An introduction to information security*, NIST SP 800-12r1, National Institute of Standards and Technology 2017, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> (5.04.2025).
- Niemal ćwierć miliona Europejczyków przeszkolonych przez Cisco w dziedzinie cyberbezpieczeństwa w ciągu ostatniego roku, <https://brief.pl/niemal-cwierc-miliona-europejczykow-przeszkolonych-przez-cisco-w-dziedzinie-cyberbezpieczenstwa-w-ciagu-ostatniego-roku/> (26.04.2025).
- NIK, *Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa*, 2022, <https://www.nik.gov.pl/kontrola/P/21/003/KAP/> (27.04.2025).
- NIST, *SP 800-63 Digital Identity Guidelines*, 2017, <https://doi.org/10.6028/NIST.SP.800-63-3> (12.04.2025).
- O certyfikacji ECDL/ICDL, <https://pti.org.pl/polskie-biuro-ecd/> (19.04.2025).
- OECD, *Learning to Change: ICT in Schools*, 2001, https://www.oecd.org/en/publications/learning-to-change-ict-in-schools_9789264195714-en.html (18.04.2025).

- Ofir Geveye M., *Protecting Endpoints in an Evolving Threat Landscape*, 2024, <https://www.centraleyes.com/protecting-endpoints-in-an-evolving-threat-landscape/> (15.04.2025).
- Oszustwa na szkodę gmin. Akt oskarżenia trafił do sądu, 2024, https://www.rmf24.pl/regiony/lodz/news-oszustwa-na-szkode-gmin-akt-oskarzenia-trafil-do-sadu,nId,7471466#crp_state=1 (18.03.2025).
- Pawlak M., *Zarządzanie incydentami cyberbezpieczeństwa w praktyce*, PTI 2024, <https://pti.org.pl/zarzadzanie-incydentami-cyberbezpieczenstwa-w-praktyce/> (5.04.2025).
- Polska cierpi na brak specjalistów od cyberbezpieczeństwa. Luka kompetencyjna jest spora, <https://www.bankier.pl/wiadomosc/Polska-cierpi-na-brak-specjalistow-od-cyberbezpieczenstwa-Luka-kompetencyjna-jest-spora-8641461.html> (28.04.2025).
- Prawie 400 mln zł na rozwój umiejętności cyfrowych Polaków, <https://www.gov.pl/web/cyfryzacja/prawie-400-mln-zl-na-rozwoj-umiejtnosci-cyfrowych-polakow> (25.04.2025).
- Program Współpracy w Cyberbezpieczeństwie (PWCyber), <https://www.gov.pl/web/baza-wiedzy/o-programie> (25.04.2025).
- Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, <https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw3> (19.01.2025).
- Quantum of Lies*, <https://www.kaspersky.com/blog/quantum-cryptography-2024-hype/52884/> (7.04.2025).
- Ransomware Landscape in Europe*, 2023, <https://www.digitalsme.eu/57-surge-of-cyberattacks-in-europe-flagged-by-digital-sme-report/> (19.02.2025).
- Raport o dokumentach infoDOK – IV kwartał 2024, <https://dokumentyzastrzezone.pl/raport-infodok/> (5.02.2025).
- Recommendation X.1205 – Overview of cybersecurity*, <https://www.itu.int/rec/t-rec-x.1205-200804-i> (9.12.2024).
- Reza A., *Cyber Threat Profiling: Understanding the Different Threat Actors*, <https://www.linkedin.com/pulse/cyber-threat-profiling-understanding-different-actors-reza-adineh> (5.02.2025).
- Rodseth R., Mayer M., Rothkugel J., *IIoT at a Tipping Point*, 2024, <https://activantcapital.com/research/iiot-at-a-tipping-point> (12.04.2025).
- Rośnie liczba ataków na polskie firmy. W tym roku przeskoczy ważny próg, 2024, <https://www.money.pl/gospodarka/co-grozi-firmom-w-cyberatakach-co-mozna-stracic-7075406726208352a.html> (17.03.2025).
- Ruf L., Thorn A., Christen T., Gruber B., Portmann R., *Threat Modeling in Security Architecture – The Nature of Threats*, 2008, https://www.iss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf (5.11.2024).
- Security Orchestration, Automation and Response (SOAR)*, <https://www.oneidentity.com/learn/what-is-soar.aspx> (13.04.2025).

- Segmentacja sieci – podstawy podstaw*, <https://www.grupae.pl/segmentacja-sieci-podstawy-podstaw/> (13.04.2025).
- Shirey R., *Internet Security Glossary*. Internet Engineering Task Force, 2000, doi:10.17487/RFC2828, <https://datatracker.ietf.org/doc/html/rfc2828> (9.03.2025).
- Simmons C., Ellis C., Shiva S., Dasgupta D., Wu C., *AVOIDIT: A Cyber Attack Taxonomy*. CTIT technical reports series, 2009, https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy (22.03.2025).
- Sophos, *The State of Ransomware 2024*, <https://www.sophos.com/en-us/whitepaper/state-of-ransomware> (22.03.2025).
- Spear Phishing – Top Threats and Trends*, <https://www.barracudamsp.com/resources/reports/spear-phishing-threats-and-trends> (8.04.2025).
- State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*, <https://iot-analytics.com/number-connected-iot-devices/> (12.04.2025).
- The EU's Cybersecurity Strategy for the Digital Decade*, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> (3.03.2025).
- The Global Financial Stability Report*, 2024, <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024> (18.02.2025).
- The Impact of Remote Work on Security and Compliance*, <https://360advanced.com/the-impact-of-remote-work-on-security-and-compliance/> (10.04.2025).
- The State of Cyber Security 2025 Report*, <https://www.checkpoint.com/security-report/> (25.02.2025).
- Total amount of malware and PUA*, <https://portal.av-atlas.org/malware> (18.03.2025).
- Trend Micro, *Cloud Security Report 2024*, <https://www.trendmicro.com/explore/cloud-security-eu> (6.04.2025).
- Understanding Cybersecurity Throughout the Electoral Process: A Reference Document An Overview of Cyber Threats and Vulnerabilities in Elections*, https://www.usaid.gov/sites/default/files/2023-01/Understanding-Cybersecurity-Throughout-the-Electoral-Process_1.pdf (11.01.2025).
- UODO, *Jedno deklarujemy, drugie robimy. Jak nie chronić danych osobowych*, <https://uodo.gov.pl/pl/138/2558> (26.03.2025).
- USAID, *Economic Growth Briefer*, <https://www.usaid.gov/digital-development/cybersecurity/economic-growth-briefer> (5.09.2024).
- Value of the Polish cloud computing market increased by 1 billion PLN in 2023*, <https://www.pmrmarketexperts.com/en/news/value-of-the-polish-cloud-computing-market-increased-by-1-billion-pln-in-2023/> (4.04.2025).
- Veridas, *Cybersecurity in 2025: Navigating the Identity Fraud Landscape*, <https://www.linkedin.com/pulse/cybersecurity-2025-navigating-identity-fraud-landscape-veridas-pbdhf> (27.03.2025).
- Wachowska A., Basaj K., *Dyrektywa NIS 2 – obowiązki w zakresie zgłaszania incydentów*, 2024, <https://www.traple.pl/dyrektywa-nis-2-obowiazki-w-zakresie-zglaszania-incydentow/> (11.03.2025).

- Wardle C., Derakhshan H., *Information disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe 2017, <https://rm.coe.int/information-disorder-report-november-2017/1680764666> (10.04.2025).
- Waszczuk P., *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, <https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance/> (4.04.2025).
- What is a cyber attack? How they work and how to stop them*, <https://www.techtarget.com/searchsecurity/definition/cyber-attack> (19.02.2025).
- What is a Disaster Recovery Plan?*, <https://cloud.google.com/learn/what-is-disaster-recovery> (15.04.2025).
- Wrzosek M., *Dyrektywa NIS 2 – jakie zmiany w zakresie cyberbezpieczeństwa proponuje Komisja Europejska?*, 2020, <https://cyberpolicy.nask.pl/dyrektywa-nis-2-jakie-zmiany-w-zakresie-cyberbezpieczenstwa-proponuje-komisja-europejska/> (22.02.2025).
- Wspólny komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, 2013, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52013JC0001> (3.02.2025).
- Zarządzanie podatnościami*, <https://csirt-mon.wp.mil.pl/aktualnosci/zarzadzanie-podatnosciami/> (13.04.2025).

Formularz ankiety

Pytania ankietowe – Świadomość i kompetencje Polaków w zakresie cyberbezpieczeństwa

P1. Czy podczas korzystania z Internetu odczuwasz obawy dotyczące swojego bezpieczeństwa?

- ☐ Tak, czasami
- ☐ Tak, często
- ☐ Nie, nigdy
- ☐ Nie wiem

P2. Czy uważasz, że liczba zagrożeń cyfrowych obecnie...

- ☐ Zdecydowanie rośnie
- ☐ Raczej rośnie
- ☐ Raczej maleje
- ☐ Zdecydowanie maleje
- ☐ Nie wiem / trudno powiedzieć

P3. Czy doświadczyłeś/doświadczyłaś jakiegóż cyberataku?

- ☐ Tak, doświadczyłem/łam osobiście, ale bez straty pieniędzy
- ☐ Tak, doświadczyłem/łam osobiście i straciłem/łam pieniądze
- ☐ Ktoś z moich bliskich/znajomych doświadczył cyberataku, ale bez straty pieniędzy
- ☐ Ktoś z moich bliskich/znajomych doświadczył cyberataku i stracił pieniądze
- ☐ Nie, ani ja, ani nikt z moich znajomych nie doświadczył takiej sytuacji
- ☐ Nie wiem/trudno powiedzieć

P4. Skąd czerpiesz wiedzę na temat cyberbezpieczeństwa? (można wybrać wiele odpowiedzi)

- ☐ Od znajomych i członków rodziny
☐ Z mediów społecznościowych
☐ Z tradycyjnych mediów (TV, prasa, radio)
☐ Z internetowych portali informacyjnych
☐ Ze specjalistycznych stron i portali zajmujących się cyberbezpieczeństwem
☐ Ze szkoleń w miejscu pracy
☐ Z zajęć w szkole/uczelni
☐ Inne
☐ Nie interesuje mnie ten temat

P5. Czy chciałbyś zdobyć (poszerzyć) wiedzę na temat cyberbezpieczeństwa?

- ☐ Tak, obecnie jestem w trakcie zdobywania lub poszerzania takiej wiedzy
☐ Tak, planuję w najbliższym czasie zdobyć (poszerzyć) taką wiedzę
☐ Tak, ale nie wiem, jak to zrobić ani gdzie szukać informacji
☐ Tak, ale nie ma na to czasu
☐ Nie, taka wiedza nie jest mi potrzebna
☐ Nie, wiem już wystarczająco dużo na ten temat

P6. Jak oceniasz swoją wiedzę na temat poniższych zagrożeń?

	Nie mam w ogóle wiedzy	Bardzo słabo	Słabo	Dobrze	Bardzo dobrze
<i>Phishing</i>					
<i>Ransomware</i>					
<i>Spoofing</i>					
<i>Malware</i> (złośliwe oprogramowanie)					
<i>SIM Swap</i>					
Kradzież tożsamości					
Ogólna wiedza na temat cyberbezpieczeństwa					

P7. Jak oceniasz informacje/wiedzę na temat cyberbezpieczeństwa, które uzyskałeś:

	Nie uzyskałem/am wiedzy o cyberbezpieczeństwie w tym miejscu	Bardzo słabo	Słabo	Dobrze	Bardzo dobrze
W szkole (szkoła podstawowa/ średnia)					
W czasie studiów					
Od swojego pracodawcy					

	Nie uzyskałem/am wiedzy o cyberbezpieczeństwie w tym miejscu	Bardzo słabo	Słabo	Dobrze	Bardzo dobrze
Od sprzedawców w Internecie					
Od banku, z którego korzystasz					
W telewizji					
W mediach społecznościowych					
Na portalach informacyjnych					
Z innych źródeł					

P8. Jak oceniasz swoją wiedzę i umiejętności obrony przed poniższymi zagrożeniami (czy wiesz jak się przed nimi bronić?)

	W ogóle nie mam takiej wiedzy	Bardzo słabo	Słabo	Dobrze	Bardzo dobrze
<i>Phishing</i>					
Oszustwa w czasie zakupów internetowych					
Złośliwe oprogramowanie					
Przejęcie (kradzież) przez przestępców danych Twojej karty płatniczej					
Przejęcie przez przestępców loginu i hasła do serwisów internetowych, z których korzystasz					
Utrata dostępu do informacji przechowywanych w telefonie, tablecie lub komputerze (w wyniku ataku lub awarii)					
Fałszywe informacje publikowane w Internecie					
Podszywanie się pod inne osoby lub instytucje					

P9. Czy stosujesz poniższe rozwiązania?

	Tak, zawsze	Nie	Częściowo/ czasami
Mam inne hasło do każdego serwisu, z którego korzystam			
Stosuję hasła o długości 12 znaków lub więcej			
Zapisuję hasła w przeglądarce internetowej			
Stosuję logowanie (uwierzytelnianie) dwuskładnikowe			
Posiadam program antywirusowy na komputerze			
Robię kopie zapasowe (bezpieczeństwa) swoich danych			
Korzystam z menedżera haseł w telefonie			
Sprawdzam okresowo, czy moje hasło/hasła nie wyciekły			

Pytania metryczkowe

M1. Proszę wskazać płeć:

- ☐ kobieta
- ☐ mężczyzna
- ☐ inna
- ☐ nie chcę podawać

M2. Podaj swój wiek:

- ☐ 18–25 lat
- ☐ 26–40 lat
- ☐ 41–55 lat
- ☐ 56–65 lat
- ☐ 66 lat i więcej

M3. Zaznacz wielkość miejscowości, w której mieszkasz:

- ☐ wieś
- ☐ miasto do 19 tys. mieszkańców
- ☐ miasto 20–49 tys. mieszkańców
- ☐ miasto 50–99 tys. mieszkańców
- ☐ miasto 100–199 tys. mieszkańców
- ☐ miasto 200–499 tys. mieszkańców
- ☐ miasto 500 tys. lub więcej mieszkańców

M4. W jakim województwie mieszkasz?

- ☐ dolnośląskie
- ☐ kujawsko-pomorskie
- ☐ lubelskie
- ☐ lubuskie
- ☐ łódzkie
- ☐ małopolskie
- ☐ mazowieckie
- ☐ opolskie
- ☐ podkarpackie
- ☐ podlaskie
- ☐ pomorskie
- ☐ śląskie

- ☐ świętokrzyskie
- ☐ warmińsko-mazurskie
- ☐ wielkopolskie
- ☐ zachodniopomorskie

M5. Jakie wykształcenie uzyskałeś/uzyskałaś do tej pory?

- ☐ podstawowe/gimnazjalne
- ☐ zasadnicze zawodowe
- ☐ uczę się w szkole średniej
- ☐ średnie
- ☐ policealne
- ☐ studiuję w szkole wyższej
- ☐ licencjat, inżynier
- ☐ wyższe magisterskie/podyplomowe/stopień naukowy

ME4. Jaki jest Twój obecny status zawodowy?

- ☐ uczeń
- ☐ student
- ☐ pracownik fizyczny
- ☐ pracownik umysłowy
- ☐ emeryt/rencista nieaktywny zawodowo
- ☐ emeryt/rencista aktywny zawodowo
- ☐ bezrobotny
- ☐ inny
- ☐ nie chcę podawać

ME5. Oszacuj dochody netto (na rękę) na 1 osobę w gospodarstwie domowym (zł):

- ☐ Poniżej 1000
- ☐ 1000 do 2000
- ☐ 2001 do 4000
- ☐ 4001 do 6000
- ☐ 6001 do 8000
- ☐ 8001 do 10000
- ☐ Powyżej 10000
- ☐ Nie chcę podawać

Streszczenie

Niniejsza monografia zawiera omówienie i analizę zagadnień związanych z cyberbezpieczeństwem i cyberodpornością w kontekście funkcjonowania współczesnych społeczeństw, instytucji oraz państw. Szczególną uwagę poświęcono sytuacji Polski na tle innych państw Unii Europejskiej, uwzględniając zarówno aspekty systemowe, jak i społeczne. Głównym celem opracowania było zidentyfikowanie i ocena kluczowych wyzwań w zakresie bezpieczeństwa cyfrowego oraz wskazanie kierunków działań niezbędnych do budowy skutecznego i odpornego systemu cyberbezpieczeństwa.

W monografii dokonano identyfikacji najważniejszych zagrożeń obecnych w cyberprzestrzeni oraz przeglądu technik i narzędzi służących przeciwdziałaniu tym zagrożeniom. Przeanalizowano obowiązujące regulacje prawne i dokumenty strategiczne w obszarze cyberbezpieczeństwa, zarówno na poziomie krajowym, jak i unijnym, z uwzględnieniem ich spójności oraz komplementarności. Szczególne miejsce zajmuje w opracowaniu problematyka świadomości społecznej oraz kompetencji cyfrowych obywateli Polski jako kluczowych czynników wpływających na skuteczność działań w zakresie ochrony zasobów cyfrowych. W oparciu o wyniki autorskiego badania empirycznego, przeprowadzonego na reprezentatywnej próbie dorosłych Polaków, dokonano oceny poziomu wiedzy, źródeł informacji oraz umiejętności praktycznych z zakresu cyberbezpieczeństwa. Wnioski z badań wskazują na potrzebę intensyfikacji działań edukacyjnych oraz systemowego wspierania rozwoju kompetencji cyfrowych w społeczeństwie. Opracowanie zawiera również propozycje rekomendacji mających na celu zwiększenie skuteczności polityk publicznych w zakresie cyberbezpieczeństwa, a także wzmocnienie potencjału kadrowego i instytucjonalnego w tej dziedzinie.

Słowa kluczowe: cyberbezpieczeństwo, cyberodporność, kompetencje cyfrowe, świadomość cyberbezpieczeństwa

Abstract

This monograph provides a comprehensive discussion and analysis of issues related to cybersecurity and cyber resilience in the context of the functioning of contemporary societies, institutions, and states. Particular attention is devoted to the situation in Poland compared to other European Union member states, taking into account both systemic and societal dimensions. The main objective of the study is to identify and assess key challenges in the field of digital security and to propose strategic directions essential for the development of an effective and resilient cybersecurity system.

The analysis identifies major threats present in cyberspace and reviews techniques and tools used to mitigate them. It also examines current legal regulations and strategic documents on cybersecurity at both national and EU levels, with particular emphasis on their coherence and complementarity. A key focus of the monograph is the issue of public awareness and the digital competencies of Polish citizens, which are crucial to the effectiveness of efforts aimed at protecting digital assets. Based on the results of an original empirical study conducted on a representative sample of adult Poles, the monograph assesses the level of knowledge, information sources, and practical cybersecurity skills. The findings highlight the need for intensified educational efforts and systemic support for the development of digital competencies within society. The study also presents a set of recommendations aimed at enhancing the effectiveness of public cybersecurity policies and strengthening human and institutional capacity in this field.

Keywords: cybersecurity, cyber resilience, digital competencies, cyberawareness



71-101 Szczecin, ul. Mickiewicza 64
tel. 91 444 20 06, 91 444 20 09
e-mail: wydawnictwo@usz.edu.pl
www.wn.usz.edu.pl

ISBN 978-83-8419-046-3 (online)
ISBN 978-83-8419-045-6 (print)



9 788384 190456