Akademia Bialska im. Jana Pawła II

BEZPIECZEŃSTWO CYFROWE PAŃSTWA I ADMINISTRACJI PUBLICZNEJ

Redakcja naukowa
Marta Chodyka
Tomasz Grudniewski
Zbigniew Ciekanowski



Biała Podlaska 2026

Akademia Bialska im. Jana Pawła II

BEZPIECZEŃSTWO CYFROWE PAŃSTWA I ADMINISTRACJI PUBLICZNEJ

Redakcja naukowa
Marta Chodyka
Tomasz Grudniewski
Zbigniew Ciekanowski

Biała Podlaska 2026

Wydawca
Akademia Bialska im. Jana Pawła II

Recenzenci
dr hab. Dariusz Artur Bogusz, prof. LAW
prof. dr hab. inż. Jan Posobiec

Redaktor techniczny
mgr inż. Ewelina Melaniuk

© Copyright by Akademia Bialska im. Jana Pawła II

Książka jest udostępniana na licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne – Bez utworów zależnych 4.0 Międzynarodowa

ISBN 978-83-68103-35-9
https://doi.org/10.29316/9788368103359

Nakład: 50 egzemplarzy

Wydawnictwo AB JPII
ul. Sidorska 95/97
21-500 Biała Podlaska
wydawnictwo.akademiabialska.pl

Projekt okładki, skład i druk:

druk-24h.com.pl
DRUKARNIA CYFROWA
Hurtowa 21, 15-399 Białystok
tel. 535 500 898
e-mail: studio@druk-24h.com.pl

Spis treści

Wprowadzenie 5

Waldemar Jagodziński

Aksjologiczne uwarunkowania transformacji cyfrowej administracji publicznej w Polsce – perspektywa metodologiczna 9

Adrian Szatkiewicz

Informatyzacja usług administracji publicznej – blaski i cienie 25

Sławomir Żurawski

Zarządzanie cyberbezpieczeństwem jako wyzwanie dla administracji publicznej – porównanie i rekomendacje dla systemów Polski i Słowacji 39

Barbara Drapikowska, Sylwia Borawska

Rola użytkownika w kształtowaniu cyberbezpieczeństwa organizacji 59

Małgorzata Wilczyńska, Justyna Wilczyńska-Baraniak

Audyt bezpieczeństwa informacji 79

Waldemar Perdion

Ochrona danych osobowych w cyberprzestrzeni 127

Tomasz Grudniewski, Karol Zygo, Sławomir Żurawski

Cyberterroryzm w erze zagrożeń hybrydowych 147

Marta Chodyka, Sławomir Żurawski, Marcin Oskierko

Cyberterroryzm jako zagrożenie bezpieczeństwa państwa w środowisku cyfrowym 161

Patryk Ochyra, Mariusz Kubisz, Bartosz Tarnowski

Cyberterroryzm jako wyzwanie dla bezpieczeństwa państwa – ewolucja form, struktur organizacyjnych i implikacje dla Polski 175

Kamil Jaszczuk

Mechanizmy dezinformacji w mediach społecznościowych i ich wpływ na bezpieczeństwo narodowe 189

Zuzanna Jordan

Prawo a dezinformacja – analiza regulacji dotyczących bezpieczeństwa informacyjnego w Polsce i UE 211

Justyna Wilczyńska-Baraniak, Małgorzata Wilczyńska

Deepfake jako strukturalne zagrożenie dla bezpieczeństwa informacji 223

Zuzanna Jordan, Wojciech Kołakowski

Prawna odpowiedzialność podmiotów za naruszenia cyberbezpieczeństwa 253

Barbara Drapikowska, Sylwia Borawska

Odporność informacyjna pokolenia Z – czynniki kształtujące świadomość i podatność na dezinformację w erze cyfrowej 271

Katarzyna Bakalarczyk-Burakowska, Marcin Mazurek

Dezinformacja jako narzędzie współczesnej wojny hybrydowej 293

Mateusz Rudaś

Cyfrowe platformy e-commerce a bezpieczeństwo finansów publicznych – wybrane problemy systemowe 317

Łukasz Stelmaszczyk

Wirtualny pieniądz – nowe możliwości i zagrożenia 337

Ewelina Melaniuk

Rola wirtualnego pieniądza w rozwoju gospodarki cyfrowej 357

Wprowadzenie

Transformacja cyfrowa państwa i administracji publicznej jest dziś jednym z kluczowych procesów modernizacyjnych: porządkuje relacje obywatel-państwo, przyspiesza świadczenie usług, usprawnia zarządzanie informacją i podnosi efektywność działania instytucji. Jednocześnie jednak cyfryzacja zmienia profil ryzyka w sposób fundamentalny. Rozszerza powierzchnię ataku, zwiększa zależność od infrastruktury teleinformatycznej i dostawców technologii, a także przenosi istotną część sporów, konfliktów i presji politycznej do środowiska informacyjnego. W konsekwencji bezpieczeństwo cyfrowe przestaje być wyłącznie zagadnieniem technicznym – staje się warunkiem ciągłości realizacji zadań publicznych, ochrony praw jednostki, utrzymania zaufania społecznego oraz odporności państwa na oddziaływania wrogie i destabilizujące.

Niniejsza monografia została przygotowana z myślą o ujęciu bezpieczeństwa cyfrowego w sposób możliwie pełny i interdyscyplinarny. Proponujemy perspektywę, w której bezpieczeństwo nie jest „dodatkiem" do informatyzacji administracji, lecz jej integralną częścią – komponentem projektowania usług, zarządzania instytucjami, kształtowania kultury organizacyjnej i tworzenia rozwiązań prawnych. W praktyce oznacza to konieczność równoległego prowadzenia działań modernizacyjnych i zabezpieczających, a także stałego bilansowania wartości: dostępności i wygody usług publicznych z prywatnością, legalnością przetwarzania danych oraz odpornością systemów na incydenty i nadużycia.

W tomie podejmujemy zarówno zagadnienia „twarde" – związane z zarządzaniem cyberbezpieczeństwem, ochroną danych, odpowiedzialnością prawną czy bezpieczeństwem infrastruktury – jak i „miękkie", obejmujące rolę użytkownika, świadomość ryzyka, podatność na manipulację oraz odporność informacyjną. Takie połączenie jest celowe. Współczesne zagrożenia cyfrowe wykorzystują bowiem nie tylko luki technologiczne, lecz także

słabości proceduralne, deficyty kompetencyjne i napięcia społeczne. Atak na system informatyczny może zaczynać się od błędu człowieka, a destabilizacja instytucji publicznej – od dezinformacji podważającej wiarygodność procedur, danych i decyzji. Układ rozdziałów odzwierciedla logikę przechodzenia od podstaw koncepcyjnych i instytucjonalnych do zagadnień operacyjnych, prawnych i społecznych. Tom otwierają rozważania poświęcone aksjologicznym podstawom transformacji cyfrowej administracji publicznej oraz analizie informatyzacji usług administracyjnych, ukazujące cyfryzację jako proces jednocześnie organizacyjny, prawny i wartościujący. To ważny punkt wyjścia, ponieważ pytania o cele cyfryzacji, jej społeczną funkcję oraz kryteria oceny skuteczności przesądzają o tym, czy bezpieczeństwo będzie traktowane jako element jakości państwa, czy jedynie jako koszt towarzyszący modernizacji. Kolejna część monografii koncentruje się na bezpieczeństwie organizacyjnym i ochronie informacji. Obejmuje zagadnienia zarządzania cyberbezpieczeństwem w administracji publicznej, roli użytkownika w kształtowaniu bezpieczeństwa organizacji, audytu bezpieczeństwa informacji oraz ochrony danych osobowych w cyberprzestrzeni. Zestawienie tych problemów pozwala uchwycić istotę współczesnego bezpieczeństwa cyfrowego: nie jest ono wyłącznie sumą rozwiązań technicznych, lecz efektem współdziałania procedur, kompetencji, nadzoru, kultury organizacyjnej i zgodności z prawem. W dalszej części tomu szczególne miejsce zajmuje problematyka cyberterroryzmu i zagrożeń hybrydowych. Trzy kolejne rozdziały analizują to zjawisko z różnych perspektyw: jako element szerszej architektury zagrożeń hybrydowych, jako zagrożenie bezpieczeństwa państwa w środowisku cyfrowym oraz jako wyzwanie związane z ewolucją form działania, struktur organizacyjnych i konsekwencji dla Polski. Łącznie tworzą one spójny obraz zagrożenia, które przekracza tradycyjne granice między bezpieczeństwem narodowym, cyberprzestrzenią i oddziaływaniami polityczno-informacyjnymi. Rozbudowany blok tematyczny poświęcono bezpieczeństwu informacyjnemu i dezinformacji. Otwiera go analiza mechanizmów dezinformacji w mediach społecznościowych oraz ich wpływu na bezpieczeństwo narodowe. Następnie omówione zostały regulacje prawne dotyczące bezpieczeństwa informacyjnego w Polsce i Unii Europejskiej, problem deepfake jako strukturalnego zagrożenia dla bezpieczeństwa informacji, a także prawna odpowiedzialność podmiotów za naruszenia cyberbezpieczeństwa. Ważnym dopełnieniem tej części są

rozważania nad odpornością informacyjną pokolenia Z oraz nad dezinformacją jako narzędziem współczesnej wojny hybrydowej. Taki układ pokazuje, że bezpieczeństwo informacyjne wymaga dziś równoczesnego namysłu nad technologią, prawem, psychologią odbioru informacji i strategicznym wykorzystaniem narracji. Końcowa część monografii przenosi uwagę na wymiar gospodarczy i finansowy bezpieczeństwa cyfrowego. Przedmiotem analizy są cyfrowe platformy e-commerce w kontekście bezpieczeństwa finansów publicznych, zjawisko wirtualnego pieniądza jako źródła zarówno nowych możliwości, jak i nowych zagrożeń, a także rola wirtualnego pieniądza w rozwoju gospodarki cyfrowej. Rozdziały te unaoczniają, że bezpieczeństwo państwa w środowisku cyfrowym obejmuje również stabilność i przejrzystość ekosystemów finansowych, odporność na nadużycia oraz zdolność instytucji do reagowania na innowacje wyprzedzające klasyczne modele regulacyjne.

Monografia ma charakter problemowy i praktyczny. Autorzy posługują się analizą literatury i dokumentów, podejściami porównawczymi, argumentacją prawną, a także perspektywą zarządczą i społeczną. Wspólnym mianownikiem pozostaje dążenie do zrozumienia mechanizmów ryzyka oraz do formułowania wniosków możliwych do zastosowania w projektowaniu usług publicznych, budowie systemów zarządzania bezpieczeństwem, edukacji użytkowników, kształtowaniu polityk instytucjonalnych i doskonaleniu ram prawnych. Adresatami tomu są przedstawiciele administracji publicznej i instytucji odpowiedzialnych za bezpieczeństwo, prawnicy i osoby zajmujące się compliance, specjaliści IT i cyberbezpieczeństwa, badacze oraz studenci kierunków związanych z bezpieczeństwem i zarządzaniem publicznym. Mamy nadzieję, że przedstawione analizy i rekomendacje pomogą lepiej rozumieć złożoność współczesnego środowiska cyfrowego oraz wspierać decyzje, które wzmacniają odporność państwa i zaufanie do instytucji.

Miłej lektury – Redaktorzy

Waldemar Jagodziński[1]
Ministerstwo Klimatu i Środowiska

https://doi.org/10.29316/9788368103359_1

AKSJOLOGICZNE UWARUNKOWANIA TRANSFORMACJI CYFROWEJ ADMINISTRACJI PUBLICZNEJ W POLSCE – PERSPEKTYWA METODOLOGICZNA

VALUE-BASED DETERMINANTS OF THE DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION IN POLAND – A METHODOLOGICAL PERSPECTIVE

Streszczenie

Rozdział analizuje metodologiczne podstawy badań nad aksjologicznymi uwarunkowaniami transformacji cyfrowej administracji publicznej w Polsce. Autor wskazuje na potrzebę odejścia od redukcjonistycznych, technokratycznych ujęć cyfryzacji, które pomijają wymiar wartości i norm konstytuujących funkcjonowanie instytucji publicznych. Proponuje zintegrowane podejście badawcze łączące perspektywę prawną, organizacyjną i aksjologiczną, umożliwiające rekonstrukcję hierarchii

[1] https://orcid.org/0000-0002-6148-8703, e-mail: waldek_jagodzinski@wp.pl

i dynamiki wartości w procesie cyfrowych przemian. Refleksja ma charakter metateoretyczny – dotyczy sposobów konceptualizacji pojęć, doboru metod oraz relacji między poziomem deklaratywnym a praktycznym realizacji wartości w administracji cyfrowej. Autor podkreśla, że aksjologia administracji publicznej stanowi system otwarty i zmienny, kształtowany przez kontekst społeczny i technologiczny. Wskazuje potrzebę dalszych badań nad tworzeniem spójnych narzędzi metodologicznych pozwalających na analizę wartości w środowisku cyfrowym.

Słowa kluczowe: aksjologia, aksjologiczne uwarunkowania transformacji cyfrowej, metodologia badań, administracja cyfrowa, wartości

Abstract

The chapter examines the methodological foundations for studying the axiological determinants of digital transformation in Poland's public administration. The author highlights the limitations of technocratic approaches that overlook the normative and ethical dimensions of digital governance. A comprehensive research framework is proposed, integrating legal, organizational, and axiological perspectives to reconstruct the hierarchy and evolution of values shaping digital change. The study adopts a metatheoretical orientation, focusing on the conceptualization of key notions, methodological design, and the relationship between declared and practiced values in digital administration. Axiology is presented as a dynamic, open system influenced by social and technological contexts. The chapter calls for the development of consistent methodological tools that can capture the interplay between technology, law, and public values, thus enabling a more holistic understanding of digital transformation processes in public institutions.

Keywords: axiology, axiological determinants of digital transformation, research methodology, digital administration, values

Wstęp

Transformacja cyfrowa administracji publicznej stanowi jeden z fundamentalnych procesów modernizacyjnych zachodzących we współczesnych państwach, który redefiniuje relacje między władzą publiczną a obywatelami oraz sposób realizacji zadań administracyjnych. W dotychczasowym dyskursie naukowym dominuje perspektywa techniczno-organizacyjna, która ujmuje transformację cyfrową administracji publicznej w kategoriach operacyjnych i wdrożeniowych. Prowadzone analizy koncentrują się

przede wszystkim na problematyce normatywnych i organizacyjnych podstaw transformacji – w szczególności na regulacjach prawnych umożliwiających wdrażanie zmian instytucjonalnych (Dudzik, 2022; Puczko, 2025; Romaniuk, 2017), implementacji narzędzi cyfrowych (Błażewski, 2022; Grzybowski, 2022; Hysa, 2013), doskonaleniu procedur administracyjnych (Lewańska, Sokołowska, Stróżyna, 2016; Świtał, 2020) oraz dostępności usług publicznych w środowisku elektronicznym (Miłek, Nowak, 2021). W relatywnie niewielkim stopniu podejmowana jest natomiast refleksja nad aksjologicznymi uwarunkowaniami i konsekwencjami tych procesów, które w istocie determinują ich kierunek, zakres oraz społeczny odbiór[2]. Ten brak zainteresowania wydaje się wynikać przede wszystkim z ograniczonej refleksji metodologicznej dotyczącej sposobów konceptualizacji i prowadzenia badań w tym obszarze[3]. Przeważająca w większości prac orientacja pragmatyczno-efektywnościowa, choć niewątpliwie cenna z punktu widzenia optymalizacji procesów administracyjnych, prowadzi do marginalizacji wymiaru wartości i znaczeń konstytutywnych dla działania cyfrowej administracji publicznej jako instytucji służącej realizacji dobra wspólnego. Zjawisko to jest o tyle znamienne, że w literaturze przedmiotu od dłuższego czasu rozwijane są badania nad aksjologią prawa administracyjnego oraz tradycyjnej administracji publicznej (Zimmermann, 2017; Cieślak 2000; Frańczuk 2016), które obejmują zarówno rekonstrukcję wartości normatywnych konstytuujących określone instytucje prawa administracyjnego (Chlipała, 2017; Zając, 2022), jak i badania nad ich funkcjonalnym przejawianiem się

[2] W tym kontekście warto odnotować pracę Ejdys (2018). Choć już sam tytuł sugeruje podjęcie problematyki aksjologicznej, to – jak wskazuje autorka – „(c)elem utylitarnym pracy było pozyskanie wiedzy niezbędnej w procesach doskonalenia stosowanych rozwiązań w zakresie e-administracji, umożliwiających adaptację rozwiązań technologicznych w większym zakresie" (s. 9). Tym samym potencjał tej pracy w zakresie pogłębionej refleksji nad aksjologią e-administracji został podporządkowany celom aplikacyjnym i doskonaleniu praktyk wdrożeniowych, co dobrze ilustruje dominację podejścia instrumentalnego w polskich badaniach nad cyfryzacją administracji publicznej.

[3] Zob. np. opracowanie M. Błażewskiego (2017), w którym autor formułuje wniosek, że „dwoma podstawowymi wartościami wyrażonymi w przepisach prawa dotyczących e-administracji są powszechność oraz bezpieczeństwo" (s. 206). Pomimo że we wstępie podkreślono interdyscyplinarny charakter analizowanych wartości, wskazując ich powiązanie zarówno z ujęciem ekonomicznym – odnoszącym się do redukcji kosztów realizacji zadań publicznych lub interakcji z organami administracji – jak i psychologicznym – odnoszącym się do zmian w zachowaniach pracowników administracji i obywateli – w pracy całkowicie pominięto jakiekolwiek założenia metodologiczne, które pozwalałyby ocenić trafność i spójność wnioskowania.

w praktyce stosowania prawa, rozumianym jako sposób ich implementacji i operacjonalizacji w działalności organów administracji (Chlipała, 2023) oraz sądów administracyjnych (Kułak-Krzysiak, 2017), jak również w sposobie ich organizacji[4]. Można w tym kontekście wnioskować, że naturalnym kierunkiem badań nad aksjologią administracji publicznej będzie analiza wartości, które determinują proces cyfrowej transformacji administracji publicznej w Polsce.

Rozdział podejmuje refleksję nad potrzebą wypracowania nowego paradygmatu badań nad administracją cyfrową, integrującego perspektywę techniczną, normatywną, organizacyjną i aksjologiczną. Ma on charakter metodologiczny i wskazuje główne kierunki oraz kryteria, na które należy zwracać uwagę w badaniach nad wartościami determinującymi transformację cyfrową administracji publicznej.

Cyfrowa administracja publiczna – kwestie terminologiczne

Jednym z zasadniczych wyzwań stojących przed badaczem podejmującym analizę aksjologicznych uwarunkowań transformacji cyfrowej administracji publicznej jest konieczność precyzyjnego zdefiniowania przedmiotu badań. Choć pojęcie e-administracji weszło już na stałe do dyskursu naukowego i praktyki funkcjonowania instytucji publicznych, jego znaczenie wciąż pozostaje niejednoznaczne. W literaturze przedmiotu spotkać można liczne ujęcia, które akcentują odmienne aspekty tego zjawiska – od technicznego wymiaru informatyzacji procedur administracyjnych, poprzez zarządcze koncepcje modernizacji sektora publicznego, aż po szersze interpretacje ujmujące e-administrację jako element transformacji społeczno-kulturowej współczesnego państwa. Tak szerokie spektrum interpretacyjne sprawia, że badacz musi prawidłowo zdefiniować przedmiot analiz. Od sposobu ujęcia

[4] Kwestię organizacji organu i jego wpływu na wartość, jaką jest zaufanie jednostki do organu administracji w ciekawy sposób wyjaśnia J. Korczak (2015, s. 105), pisząc: „Wydaje się, że szczególne znaczenie w pozyskiwaniu zaufania może mieć prostota tak struktur organizacyjnych, jak i procedur postępowania (oczywiście z poszanowaniem obowiązujących przepisów prawa), które prowadzą do przejrzystości tych struktur i procedur, o co współcześnie tak bardzo się zabiega. Nie ulega wątpliwości, iż już sama zagmatwana struktura organizacyjna urzędu nie budzi zaufania, zwłaszcza gdy załatwiający w nim sprawę interesant nie jest w stanie ustalić właściwości poszczególnych komórek organizacyjnych i stanowisk pracy".

pojęcia e-administracji zależy bowiem identyfikacja kluczowych wartości, które konstytuują i legitymizują proces jej rozwoju. W wąskim, technokratycznym rozumieniu, akcentującym funkcjonalne aspekty cyfryzacji, centralne miejsce zajmują wartości instrumentalne – takie jak efektywność, szybkość działania, racjonalizacja kosztów czy standaryzacja procedur. Natomiast w podejściu szerszym, ujmującym transformację cyfrową jako zmianę relacji między państwem a obywatelem, w centrum zainteresowania znajdują się wartości o charakterze normatywnym: przejrzystość, równość dostępu, partycypacja obywatelska, odpowiedzialność instytucji publicznych oraz ochrona prywatności i danych osobowych.

Nie bez znaczenia jest również fakt, że e-administracja stanowi zjawisko dynamiczne, pozostające w ścisłym związku z rozwojem technologii informacyjno-komunikacyjnych, zmianami społecznymi oraz ewolucją oczekiwań wobec państwa. Z tej perspektywy badacz nie może traktować e-administracji jako konstruktu o ustalonej treści, lecz raczej jako proces, którego granice i znaczenia ulegają ciągłej renegocjacji. Każda próba definicyjna ma zatem charakter sytuacyjny i aksjologicznie zdeterminowany – odzwierciedla nie tylko stan rozwoju technologicznego, lecz również dominujące w danym momencie rozumienie roli państwa, obywatela i dobra wspólnego.

Z tych powodów refleksja nad aksjologicznymi podstawami transformacji cyfrowej administracji publicznej wymaga nie tylko deskrypcji zjawiska, ale także metateoretycznej świadomości przyjętego sposobu jego konceptualizacji. Jasne określenie, czy przedmiotem badań jest e-administracja rozumiana jako zestaw narzędzi technicznych, jako nowy paradygmat zarządzania publicznego, jako zbiór regulacji prawnych czy też jako zjawisko o wymiarze społecznym i kulturowym, stanowi warunek konieczny do prowadzenia spójnej i pogłębionej analizy aksjologicznej. Dopiero takie ujęcie pozwala na identyfikację wartości, które nie tylko towarzyszą procesowi cyfryzacji, ale również nadają mu kierunek i sens w perspektywie etycznej oraz społecznej legitymizacji działań administracji publicznej.

Błędem jest także postrzeganie administracji jako zjawiska jednolitego, niezależnego od szczebla organizacyjnego i rodzaju realizowanych zadań. Takie podejście prowadzi do uproszczeń metodologicznych, ponieważ zakłada, że narzędzia cyfrowe, zasady działania i wartości aksjologiczne administracji publicznej mają charakter uniwersalny. Tymczasem

analiza struktury i funkcji administracji wskazuje na istotne różnice między administracją centralną i samorządową. O ile administracja rządowa pełni funkcje regulacyjne, kontrolne i strategiczne, o tyle administracja samorządowa realizuje przede wszystkim zadania o charakterze usługowym, wspólnotowym i lokalnym. Oznacza to, że e-administracja w samorządzie terytorialnym musi być interpretowana przez pryzmat odmiennych wartości, co wynika z odmiennych funkcji przez nią realizowanych i relacji społecznych, w które jest uwikłana. Różnica ta przekłada się na sposób wdrażania rozwiązań cyfrowych: w administracji rządowej dominują systemy integrujące dane i procedury w skali ogólnokrajowej, takie jak rejestry centralne, elektroniczne dzienniki urzędowe, systemy kontroli czy platforma legislacyjna. W samorządzie administracja przybiera formę interaktywnych usług publicznych, takich jak elektroniczne wnioski, lokalne portale obywatelskie czy platformy konsultacji społecznych. Już na etapie konceptualizacji badań widać, że administracja centralna posługuje się technologią informacyjną jako narzędziem urzeczywistniania takich wartości jak racjonalizacja i koordynacja, natomiast administracja samorządowa wykorzystuje ją w celu zwiększenia dostępności i partycypacji. Funkcja technologii różni się zatem zasadniczo: w jednym przypadku służy optymalizacji systemu, w drugim – wzmocnieniu relacji z obywatelem. Prawidłowa konceptualizacja przedmiotu badań stanowi warunek *sine qua non* operacjonalizacji działań badawczych.

Konsekwencją powyższych ustaleń jest rozważenie, jakie modele powiązań będą stanowiły przedmiot analizy. Nie ulega bowiem wątpliwości, że inne są uwarunkowania aksjologiczne w przypadku relacji e-administracji z obywatelem (typowej dla administracji samorządowej), inne zaś w przypadku relacji między organami administracji (charakterystycznej dla administracji rządowej). Mając tę refleksję na uwadze, rozróżnić należy trzy modele komunikacji prowadzonej przez organy (Haręża, 2011):

- G to C / G2C (ang. Government to Citizens – relacja e-administracja – obywatele),
- G to B / G2B (ang. Government to Business – relacja e-administracja – przedsiębiorcy),
- G to G / G2G (ang. Government to Government – relacja między organami administracji).

Zróżnicowanie modeli funkcjonowania administracji cyfrowej implikuje konieczność stosowania odmiennych metod badawczych oraz wykorzystania zróżnicowanych narzędzi analitycznych. Dla przykładu, ze względu na bezpośredni charakter relacji między administracją a obywatelem, analiza modelu G2C wymaga podejścia socjologiczno-prawnego, które uwzględnia problematykę praw człowieka, zasadę zaufania do władzy publicznej oraz reguły dobrej administracji. W tym ujęciu szczególnego znaczenia nabiera pytanie o sposób, w jaki narzędzia cyfrowe wpływają na realizację podstawowych wartości administracyjnych, takich jak dostępność, równość w dostępie do usług i przejrzystość działania organów.

W relacjach typu G2B centralne miejsce zajmują wartości ekonomiczne i organizacyjne, determinujące kierunek działań administracji publicznej ukierunkowanej na tworzenie otoczenia instytucjonalnego sprzyjającego rozwojowi przedsiębiorczości. Takie wartości jak efektywność, interoperacyjność czy szybkość działania zyskują tu wymiar gospodarczy, ponieważ równocześnie wzmacniają konkurencyjność rynku.

Z kolei model G2G odnosi się do wewnętrznego wymiaru funkcjonowania administracji publicznej. Jego istotą jest współdziałanie między organami władzy publicznej, wymiana informacji, koordynacja zadań oraz tworzenie wspólnych standardów technologicznych i proceduralnych. Analiza tego modelu powinna pozwolić odpowiedzieć na pytanie, czy cyfryzacja przyczynia się do realnego podniesienia jakości zarządzania publicznego, czy jedynie rekonfiguruje tradycyjne mechanizmy biurokratyczne w środowisku elektronicznym.

Wspólnym obszarem badań dla wszystkich wymienionych modeli są aspekty organizacyjno-instytucjonalne funkcjonowania administracji cyfrowej, obejmujące aksjologiczne uwarunkowania zarówno formalnych, jak i nieformalnych procedur, rozwój kompetencji urzędników, przepływ informacji między instytucjami oraz kwestie regulacyjne. Warto podkreślić, że przepisy prawa dotyczące rozwoju administracji cyfrowej są wytwarzane przez organy administracji, które w procesie tym korzystają z nowoczesnych technologii informacyjnych (Araszkiewicz, Ciurak, 2025; Deminet, Godlewska, 2025), co wprowadza istotny element sprzężenia zwrotnego między regulacją a praktyką wdrażania innowacji technologicznych.

Na podstawie wyróżnionych modeli funkcjonowania administracji cyfrowej przedmiotem badań można uczynić także napięcia aksjologiczne

występujące między różnymi podmiotami wchodzącymi w interakcję z e-administracją, co zostanie ukazane na przykładzie relacji G2B.

Napięcia aksjologiczne w relacji G2B wynikają przede wszystkim z odmiennego ukierunkowania celów działania administracji publicznej i podmiotów gospodarczych. Podczas gdy administracja działa w imię interesu publicznego, przedsiębiorcy kierują się racjonalnością ekonomiczną i dążeniem do maksymalizacji korzyści. Te dwie logiki, choć mogą się uzupełniać, nie zawsze pozostają w pełnej harmonii. Pierwszy obszar potencjalnych napięć dotyczy relacji między efektywnością a równością dostępu. Cyfryzacja procesów administracyjnych często zwiększa szybkość i ekonomiczność działania, jednak może prowadzić do wykluczenia mniejszych podmiotów, które nie dysponują odpowiednim zapleczem technologicznym lub kompetencjami cyfrowymi. W tym kontekście wartości efektywności i ekonomiczności muszą być równoważone przez wartości inkluzywności i równości szans w dostępie do e-usług administracyjnych. Pod kątem badań aksjologicznych metodologicznie doniosłe jest zatem nie tylko sprawdzenie, jak dobrze system działa, lecz także dla kogo działa dobrze, a kogo może wykluczać, co na dalszym etapie badawczym umożliwi identyfikację antywartości cyfrowej administracji. Drugi obszar napięcia może ujawniać się między transparentnością a ochroną tajemnicy przedsiębiorstwa oraz prywatności danych. E-administracja, realizując wartości jawności i przejrzystości działania instytucji publicznych, generuje jednocześnie ryzyko nadmiernej ekspozycji informacji gospodarczych lub danych wrażliwych. Wymaga to wyważenia między dążeniem do otwartego państwa a koniecznością zapewnienia bezpieczeństwa informacyjnego uczestników obrotu gospodarczego. Trzeci obszar napięć ma charakter systemowy i dotyczy relacji między automatyzacją procesów administracyjnych a zachowaniem gwarancji proceduralnych. Uproszczenie i przyspieszenie postępowań administracyjnych poprzez narzędzia cyfrowe niewątpliwie wspiera przedsiębiorców, ale może równocześnie osłabiać możliwość indywidualnej oceny sprawy, co w konsekwencji prowadzi do ograniczenia realizacji wartości sprawiedliwości proceduralnej i prawa do wysłuchania strony (Kaszubowski, 2024).

E-administracja jako narzędzie wspierania rozwoju przedsiębiorczości funkcjonuje w przestrzeni kompromisów aksjologicznych, które wymagają od badaczy identyfikacji**,** interpretacji i weryfikacji aksjologicznej. Skuteczne prowadzenie takich badań wymaga opracowania spójnych narzędzi

metodologicznych, pozwalających nie tylko na ocenę realizacji wartości konstytutywnych, lecz również na wykrywanie antywartości ograniczających dostępność i równość szans w korzystaniu z e-usług administracyjnych. Tylko dzięki takiemu podejściu możliwe staje się formułowanie weryfikowalnych wniosków naukowych oraz projektowanie e-administracji zgodnie z aksjologicznymi priorytetami państwa i społeczeństwa.

Różnorodność działań mieszczących się w obszarze e-administracji – od wdrażania systemów informatycznych, przez automatyzację procedur urzędowych i procesów legislacyjnych, po rozwój usług publicznych świadczonych online – wymusza na badaczu konieczność precyzyjnego rozróżnienia między technologicznym, organizacyjnym a normatywnym wymiarem analizowanego zjawiska.

Aksjologia jako dynamiczny system wartości

Aksjologia transformacji administracji publicznej nie powinna być ujmowana jedynie jako abstrakcyjny zbiór zasad normatywnych, lecz jako dynamiczny system wartości urzeczywistnianych w określonym kontekście społecznym, instytucjonalnym i czasowym. Dynamikę tę można rozpatrywać dwutorowo – jako proces ewolucji aksjologicznej oraz jako zjawisko reinterpretacji zastanych wartości w zmieniających się technologicznych i społecznych warunkach funkcjonowania administracji publicznej (Wronkowska-Jaśkiewicz, 2017).

Z perspektywy nauk administracyjnych szczególnego znaczenia nabiera zatem napięcie pomiędzy aksjologiczną ciągłością a zmiennością, stanowiące o tożsamości instytucji administracyjnych. Ciągłość ta wyraża się w zachowaniu fundamentalnych wartości, takich jak legalizm, bezstronność, służba publiczna czy odpowiedzialność, które konstytuują etos administracji. Zmienność natomiast odzwierciedla zdolność administracji do reagowania na nowe wyzwania społeczne i technologiczne, a tym samym do redefiniowania sposobów urzeczywistniania tych samych wartości w odmiennych warunkach funkcjonowania państwa. W tym sensie aksjologia administracji publicznej pozostaje nie tylko kategorią teoretyczną, lecz również praktycznym narzędziem interpretacji i oceny procesów transformacyjnych zachodzących w strukturach administracyjnych.

Traktując aksjologię jako dynamiczny system wartości, można dostrzec, że wartości administracyjne nie funkcjonują w izolacji, lecz są kształtowane w ciągłej interakcji z uwarunkowaniami historycznymi, kulturowymi, politycznymi, ekonomicznymi oraz – w kontekście e-administracji – technologicznymi. Przyjęcie powyższego założenia prowadzi do wniosku, że „system (zbiór) wartości jest otwarty, stale uzupełniany i modyfikowany. Wartości istnieją tylko w sensie relatywnym i subiektywnym, nie ma wobec tego żadnej z góry założonej hierarchii" (Stelmach, 2017, s. 40)[5]. W praktyce oznacza to, że zarówno identyfikacja wartości, jak i ocena ich znaczenia zależą od wielu czynników, takich jak kontekst interpretacyjny, przyjęta metoda badawcza, indywidualne przyzwyczajenia interpretatora, dziedzina prawa, a także stopień złożoności analizowanego przypadku (Stelmach, 2017). Takie zróżnicowanie w podejściu do wartości skutkuje tym, że różni autorzy przypisują najwyższy priorytet odmiennej wartości (posługując się przy tym zróżnicowaną nomenklaturą).

Zróżnicowanie hierarchii wartości a potrzeba pogłębienia metodologii badań aksjologicznych

Ilustracją zjawiska relatywizmu wartości w prawie administracyjnym mogą być teksty opublikowane w pierwszym tomie monografii pod redakcją J. Zimmermanna (2017) (Tabela 1). Zawarte w nim opracowania ujawniają znaczną różnorodność podejść do rozumienia oraz hierarchizacji wartości,

[5] Oczywiście będąc świadomym problemu nadmiernego subiektywizmu w ustalaniu katalogu wartości prawnych można starać się mu przeciwdziałać, przykładowo operując „tylko tymi wartościami, które wysłowił sam ustawodawca, co z reguły następuje poprzez określenie w treści aktu prawnego (w tym w treści ewentualnej preambuły) jego celów. (…) Szczególnie istotne są właśnie tzw. wartości-cele, czyli te, dla których realizacji podejmowane są odpowiednie decyzje prawne" (Nałęcz, 2017, s. 671). Niewątpliwie jednak podejście takie ogranicza badania w zakresie, w jakim nie może objąć wszystkich rzeczywistych wartości, które faktycznie determinują działalność prawodawcy, co wynika z faktu, że katalog wartości wyrażonych *explicite* w treści aktów normatywnych - nawet jeśli jest precyzyjnie zrekonstruowany – odzwierciedla jedynie deklaratywny, a nie zawsze rzeczywisty system aksjologiczny ustawodawcy. Ograniczenie analizy wyłącznie do wartości ujawnionych w tekstach prawnych prowadzi zatem do zawężenia perspektywy badawczej – pomija bowiem te elementy aksjologiczne, które działają niejako w tle procesu legislacyjnego, ale w istocie mogą w iększym stopniu determinować kierunek decyzji prawnych niż same deklaracje zawarte w preambułach czy uzasadnieniach projektów ustaw.

co wskazuje na brak jednolitych kryteriów ich identyfikacji i klasyfikacji. Istotność poszczególnych wartości bywa często sygnalizowana już w tytułach opracowań, jednak zestawienie ze sobą tych ujęć prowadzi do wniosku, że autorzy – kierując się odmiennymi przesłankami interpretacyjnymi – nadają priorytet różnym wartościom, traktując je jako nadrzędne dla systemu prawa administracyjnego (Tabela 1).

Tabela 1. Pluralizm aksjologiczny w prawie administracyjnym

Autor	Wartość	Określenie istotności wartości
Dominik J. Kościuk (2017)	prawda obiektywna	wartość realizowana w prawie administracji elektronicznej
Magdalena Małecka-Łyszczek (2017)	inkluzja społeczna	wartość w stanowieniu prawa administracyjnego na szczeblu centralnym
Katarzyna Mełgieś, Katarzyna Miaskowska-Daszkiewicz (2017)	zdrowie ludzkie	wartość determinująca zadania administracji publicznej
Alina Miruć (2017)	godność człowieka	wyznacznik prawa administracyjnego stanowionego na szczeblu centralnym
Katarzyna Wlaźlak (2017)	racjonalność	wartość prawa miejscowego
Lidia Zacharko, Barbara Wartenberg-Kempka (2017)	dobro dziecka	wartość najwyższa w prawie administracyjnym

Źródło: opracowanie własne.

Warto podkreślić, że wymienienie określonej wartości w tytule opracowania naukowego nie jest aktem neutralnym poznawczo. Pod względem metodologicznym sam wybór wartości jako centralnej kategorii analizy oznacza jej wyróżnienie spośród innych kategorii oraz przypisanie jej szczególnego znaczenia w systemie aksjologicznym, który badacz rekonstruuje lub postuluje. W tym sensie już sam fakt nadania wartości statusu kategorii tytułowej stanowi formę hierarchizacji, poprzez którą autor sugeruje, że dana wartość zajmuje pozycję nadrzędną wobec innych – czy to w strukturze teoretycznej, czy w praktyce funkcjonowania administracji publicznej. Tytuł, jako najbardziej ekspresyjny element tekstu naukowego, pełni ważną funkcję informacyjną: ukierunkowuje uwagę odbiorcy, określa punkt ciężkości analizy i wskazuje ramy interpretacyjne całego wywodu. W efekcie nazwanie

wartości w tytule jest nie tylko wyborem terminologicznym, ale również aktem interpretacyjnym, który ma konsekwencje dla sposobu postrzegania hierarchii wartości w danej dziedzinie prawa. Z perspektywy metodologicznej oznacza to, że już na poziomie formułowania problemu badawczego dochodzi do wstępnej hierarchizacji aksjologicznej, która kształtuje dalszy tok rozważań i determinuje konstrukcję argumentacji.

Przedstawione zróżnicowanie wartości zasadniczych w prawie administracyjnym nie ma charakteru czysto deskryptywnego, lecz ujawnia ograniczenia współczesnych badań aksjologicznych, wynikające w znacznej mierze z niedostatków metodologicznych, które niewątpliwie swe piętno odcisną również nad badaniami nad e-administracją. Brak spójnych, powszechnie akceptowanych narzędzi badawczych uniemożliwia porównywalność wyników analiz oraz weryfikowalność formułowanych wniosków. W konsekwencji prowadzi to do istotnych rozbieżności w proponowanych hierarchiach wartości i utrudnia formułowanie jednoznacznych, metodologicznie uzasadnionych konkluzji naukowych[6].

Z metodologicznego punktu widzenia w badaniach nad aksjologią e-administracji ujawnia się konieczność wyraźnego rozgraniczenia dwóch poziomów analizy:

- poziomu *de iure* (normatywnego), rekonstruującego wartości na podstawie źródeł prawa, polityk publicznych oraz dokumentów strategicznych;
- poziomu *de facto*, ukazującego sposób, w jaki wartości z poziomu pierwszego są realizowane i reinterpretowane w konkretnych działaniach organów administracji (rządowej i samorządowej, przy uwzględnieniu różnych modeli relacji).

[6] Z drugiej strony przytoczone tytuły prac dowodzą pluralizmu naukowego wyrażającego się w relatywizmie interpretacyjnym. Wyłania się tu zatem potencjalnie inspirujący obszar badań komparatystycznych. Analizy porównawcze, obejmujące różne tradycje interpretacyjne i metodologiczne, mogą bowiem przyczynić się do lepszego zrozumienia wspólnych elementów aksjologicznych oraz odmienności wynikających z uwarunkowań kulturowych, historycznych i doktrynalnych w rozwoju e-administracji.

Podsumowanie

Refleksja nad aksjologią transformacji cyfrowej administracji publicznej ujawnia, że proces cyfryzacji nie jest jedynie zjawiskiem technologicznym, lecz stanowi głęboką zmianę kulturową i normatywną, która wpływa na samą tożsamość instytucji publicznych. Z perspektywy metodologicznej kluczowe jest zatem przyjęcie podejścia, które pozwala uchwycić zarówno wartości deklarowane (w dyskursie normatywnym i strategicznym), jak i wartości realizowane (w praktykach organizacyjnych, technologicznych i komunikacyjnych).

W świetle przeprowadzonych rozważań można wskazać kilka wniosków syntetycznych:

1. Badania nad aksjologią e-administracji wymagają precyzyjnego zdefiniowania przedmiotu badań w celu uniknięcia redukcjonizmu metodologicznego i błędnego utożsamiania wartości z ich technicznymi lub organizacyjnymi przejawami oraz zagwarantowania rzetelności i porównywalności wyników analiz.
2. Aksjologia administracji cyfrowej stanowi interdyscyplinarne pole badawcze, które wymaga stworzenia metod analizy wartości w kontekście relacji między prawem, technologią i społeczeństwem.
3. Proces cyfryzacji administracji publicznej generuje nowe wartości (takie jak interoperacyjność, transparentność algorytmiczna czy bezpieczeństwo informacyjne), które współistnieją z klasycznymi wartościami administracyjnymi, tworząc obszar napięć aksjologicznych.
4. Aksjologia administracji cyfrowej ma charakter dynamiczny, co oznacza, że hierarchie wartości podlegają nieustannej reinterpretacji w odpowiedzi na zmiany technologiczne, społeczne i kulturowe.

Refleksja metodologiczna nad aksjologią administracji cyfrowej otwiera nowy kierunek badań, w którym prawo i technologia nie są już odrębnymi sferami, lecz wzajemnie się warunkują. Zrozumienie tego sprzężenia zwrotnego między rozwojem technologicznym i aksjologicznym fundamentem administracji publicznej pozwoli nie tylko lepiej opisać proces cyfrowej transformacji, lecz także świadomie nim kierować – tak, by służył on realizacji dobra wspólnego i wzmacniał zaufanie obywateli do instytucji publicznych.

Literatura

1. Araszkiewicz, M., Ciurak, P. (2025). Stosowanie systemów sztucznej inteligencji w e-legislacji. Wprowadzenie do problematyki. *Przegląd Legislacyjny*, *1*(129), 1-46.
2. Błażewski, M. (2022). Automatyzacja pozyskiwania i analizowania danych jako przejaw informatyzacji czynności materialno-technicznych organów administracji publicznej podejmowanych w toku postępowania administracyjnego. W: M. Kruś, L. Staniszewska, M. Szewczyk (red.), *Kierunki rozwoju jurysdykcji administracyjnej* (s. 289-296). Wolters Kluwer.
3. Błażewski, M. (2017). Wartości w e-administracji i ich wyważenie. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 197-206). Wolters Kluwer.
4. Chlipała, M. (2017). Zaufanie do administracji publicznej a normatywizacja przyrzeczenia administracyjnego. *Przegląd Prawa Publicznego*, *12*, 42-52.
5. Chlipała, M. (2023). Zaufanie jako wartość w procesie tworzenia prawa w gminie. W: A. Kaźmierczyk, K. Michałowska, M. Szaraniec (red.), *Verba volant, scripta manet. Księga jubileuszowa dedykowana Pani Profesor Bogusławie Gneli* (s. 125-135). Wolters Kluwer.
6. Cieślak, Z. (2000). Podstawy aksjologiczne administracji publicznej w Polsce – próba oceny. *Studia Iuridica*, *XXXVIII*, 59-64.
7. Deminet, J., Godlewska, M. (2025). *Kierunki modernizacji i rozwoju systemu informatycznego obsługującego proces legislacyjny. Przegląd Legislacyjny*, *1*(129), 1-55.
8. Dudzik, S. (2022). Podstawy prawne działania e-administracji a ochrona danych osobowych. W: S. Dudzik, I. Kawka, R. Śliwa (red.), *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej* (s. 13-28). Wydawnictwo Księgarnia Akademicka.
9. Ejdys, J. (2018). *Zaufanie do technologii w e-administracji.* Politechnika Białostocka.
10. Frańczuk, M. (2016). Podstawy aksjologiczne współczesnej administracji. *Zeszyty Naukowe UEK*, *3*(951), 17-32.

11. Grzybowski, T. (2022). Granice cyfrowej kontroli podatnika na przykładzie zmian uszczelniających w VAT. W: S. Dudzik, I. Kawka, R. Śliwa (red.), *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej* (s. 203-220). Wydawnictwo Księgarnia Akademicka. https://doi.org/10.12797/9788381386739
12. Haręża, A. (2011). Wprowadzenie do problematyki elektronicznej administracji publicznej. *Prawo Mediów Elektronicznych*, *1*, 26-31.
13. Hysa, B. (2013). E-usługi i inne narzędzia informatyczne wspomagające pracę urzędów administracji samorządowej. *Roczniki Kolegium Analiz Ekonomicznych*, *29*, 91-100.
14. Kaszubowski, K. (2024). *O zagrożeniach procesowych związanych z automatyzacją czynności w ogólnym postępowaniu administracyjnym. Dyskurs Prawniczy i Administracyjny, 3,* 75-86.
15. Korczak, J. (2015). Pozyskiwanie i umacnianie zaufania do władz publicznych przez współadministrowanie. W: M. Kasiński, M. Stahl, K. Wlaźlak (red.), *Sprawiedliwość i zaufanie do władz publicznych w prawie administracyjnym*, (s. 98-114). Wolters Kluwer.
16. Kościuk, D. J. (2017). Prawda obiektywna jako wartość realizowana w prawie administracji elektronicznej. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I.* Wolters Kluwer.
17. Kułak-Krzysiak, K. (2017). *Efektywność jako wartość w postępowaniu sądowoadministracyjnym.* W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom II* (s. 127-140). Wolters Kluwer.
18. Lewańska, E., Sokołowska, W., Stróżyna, M. (2016). Projektowanie e-usług dla administracji publicznej w podejściu procesowym – studium przypadku. *Roczniki Kolegium Analiz Ekonomicznych*, *42*, 103-112.
19. Małecka-Łyszczek, M. (2017). Inkluzja społeczna jako wartość w stanowieniu prawa administracyjnego na szczeblu centralnym. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 405-418). Wolters Kluwer.
20. Mełgieś, K., Miaskowska-Daszkiewicz, K. (2017). Zdrowie ludzkie jako wartość determinująca zadania administracji publicznej. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 257-272). Wolters Kluwer.

21. Miłek, D., Nowak, P. (2021). Rozwój usług elektronicznej administracji publicznej w Polsce na tle Unii Europejskiej. *Nierówności Społeczne a Wzrost Gospodarczy*, *65*, 47-73.
22. Miruć, A. (2017). Godność człowieka jako wyznacznik prawa administracyjnego stanowionego na szczeblu centralnym. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 419-434). Wolters Kluwer.
23. Nałęcz, A. (2017). *Aksjologia gminnych projektów bezpłatnego dostępu do Internetu*. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 671-679). Wolters Kluwer.
24. Romaniuk, P. (2017). Rozwój elektronicznej administracji czynnikiem wspierającym nurt zarządzania humanistycznego. *Journal of Modern Science, 2*(33), 305-323.
25. Skoczylasz, D., Puczko, A. (2025). Komunikacja elektroniczna w administracji publicznej a kwestia cyberbezpieczeństwa. *Studia Administracji i Bezpieczeństwa*, *18*, 11-25. https://doi.org/10.5604/01.3001.0055.2274
26. Stelmach, J. (2017). Spór o wartości podstawowe w prawie. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 37-43). Wolters Kluwer.
27. Świtał, P. (2020). Standaryzacja usług w administracji elektronicznej. W: B. Jaworska-Dębska, P. Kledzik, J. Sługocki (red.), *Wzorce i zasady działania współczesnej administracji publicznej*. (s. 956-968). Wolters Kluwer.
28. Wlaźlak, K. (2017). Racjonalność jako wartość prawa miejscowego. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 541-555). Wolters Kluwer.
29. Wronkowska-Jaśkiewicz, S. (2017). *Uwagi o instrumentalności, instrumentalizacji i autonomii prawa.* W: J. Zimmermann (red.) *Aksjologia prawa administracyjnego. Tom I* (s. 25-36). Wolters Kluwer.
30. Zimmermann, J. (red.), (2017). *Aksjologia prawa administracyjnego. Tom I*. Wolters Kluwer.
31. Zacharko, L., Wartenberg-Kempka, B. (2017). Dobro dziecka jako wartość najwyższa w prawie administracyjnym. W: J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I* (s. 281-292). Wolters Kluwer.
32. Zając, K. (2022). Sądowa korekta aksjologiczna prawa podatkowego – uwagi w kontekście zwolnienia dla osób najbliższych w podatku od spadków i darowizn. *International Journal of Legal Studies*, *1,* 23-59. https://doi.org/10.5281/zenodo.6891868

Adrian Szatkiewicz[1]
Uniwersytet Warszawski

https://doi.org/10.29316/9788368103359_2

INFORMATYZACJA USŁUG ADMINISTRACJI PUBLICZNEJ – BLASKI I CIENIE

THE DIGITALIZATION OF PUBLIC ADMINISTRATION SERVICES – THE PROS AND CONS

Streszczenie

Proces informatyzacji usług administracji publicznej jest w realiach XXI w., bezwzględnie konieczny, czego w jakikolwiek sposób nikt nie kwestionuje i absolutnie uważa za kluczowy dla prospektywnego rozwoju całego kraju. Generuje on bowiem szereg zalet, które immanentnie przenikają strukturę funkcjonowania administracji, jednocześnie kształtując korelację występującą pomiędzy organem a obywatelem. Jednakże w ramach globalnej elektronizacji należy a posteriori pamiętać o jej wadach generujących ryzyko intencjonalnego wykorzystania modelu zarządzania aparatem państwa przeciwko Naszemu państwu. Perspektywa ataków hybrydowych, względnie cyberataków ukierunkowanych dyrektywnie na krajową architekturę bezpieczeństwa, czy też infrastrukturę organizacyjną jest nie tylko realna, ale zwyczajnie prawdopodobna. Wiąże się to bowiem ściśle z rolą Polski w obecnej

[1] https://orcid.org/0000-0003-4963-0313, e-mail: a.szatkiewicz@wpia.uw.edu.pl

sytuacji geopolitycznej panującej w Europie Środkowo-Wschodniej, a także niekwestionowanym niebezpieczeństwem dalszej ewolucji konfliktu zbrojnego na Ukrainie. Równocześnie ustawodawca winien w dalekosiężnym modelu rozwoju usług administracji publicznej uwzględnić uwarunkowania osób zaawansowanych wiekowo, których naturalne inklinacje do obsługi aplikacji elektronicznych są radykalnie ograniczone. Konkretyzując, potencjalna globalna informatyzacja nie może naruszać powszechnej równości stanowiącej swoisty fundament cywilizacji zachodniej, w związku z czym oceniając krytycznie całokształt wad badanego procesu należy rozważyć zastosowanie dualnego (elastycznego) układu zarządzania sferą publiczną.

Słowa kluczowe: administracja, informatyzacja, sfera publiczna, obywatel, organ administracji publicznej

Abstract

The process of computerising public administration services is absolutely necessary in the 21st century, which no one questions in any way and is considered crucial for the prospective development of the entire country. It generates a number of advantages that inherently permeate the structure of the administration, while shaping the correlation between the authority and the citizen. However, in the context of global computerisation, it is important to remember its disadvantages, which generate the risk of intentional use of the state apparatus management model against our country. The prospect of hybrid attacks or cyberattacks directed at national security architecture or organisational infrastructure is not only real, but simply probable. This is closely related to Poland's role in the current geopolitical situation in Central and Eastern Europe, as well as the unquestionable danger of further escalation of the armed conflict in Ukraine. At the same time, the legislator should take into account the circumstances of elderly people, whose natural inclination to use electronic applications is radically limited, in a long-term model for the development of public administration services. To be specific, potential global computerisation must not violate universal equality, which is a fundamental principle of Western civilisation. Therefore, when critically assessing the overall disadvantages of the process under consideration, the use of a dual (flexible) public sector management system should be considered.

Keywords: administration, computerisation, public sphere, citizen, public administration agency

Wstęp

Newralgiczny proces informatyzacji usług administracji publicznej jest bez wątpienia konieczny dla interdyscyplinarnego rozwoju całego kraju, gdyż korelacja występująca na linii obywatele – państwo stanowi fundament dla wspólnej pracy sfery publicznej i prywatnej. Można zatem stwierdzić, iż sposób oraz szybkość działania organów władzy determinują sytuację poszczególnych osób i podmiotów zainteresowanych aktywnością wymagającą urzędowej aprobaty. Konkretyzując przystępna forma obsługi spraw publicznych z pewnością sprawia, że obywatele zmieniają utarty dotąd stosunek do administracji, jednakże w praktyce zdarzają się również przypadki, w ramach których powszechna informatyzacja marginalizuje, czy też nawet dyskryminuje określone grupy społeczne. Z kolei w ujęciu docelowym administracja publiczna winna obsługiwać sprawy poszczególnych obywateli wyłącznie w formie elektronicznej, co wzbudza liczne wątpliwości związane zwłaszcza z zaawansowanymi wiekowo grupami społecznymi. Mianowicie czy wówczas kontakty z organami państwowymi stanowić będą dla szeregu przeciętnych 60-latków wyzwanie, czy też może niemożliwe do zrealizowania zadanie skutkujące negatywnymi implikacjami? W ramach interdyscyplinarnej analizy procesu informatyzacji usług administracji publicznej nie można bowiem koncentrować się tylko na zaletach tegoż projektu, gdyż bezspornie konieczna jest również eliminacja jego wad (Kuzionko-Ochrymiuk, 2018).

Zalety procesu informatyzacji usług administracji publicznej

Sukcesywny rozwój wszelkich dziedzin życia społecznego generuje liczne możliwości, które dostrzec można również w sferze publicznej, czego wyrazem jest chociażby perspektywa złożenia dokumentu w kilka chwil. Otóż obecnie kontakt z organami państwowymi w dalszym ciągu posiada charakter podporządkowania, co przenika wprost istotę postępowania jurysdykcyjnego, jednakże sposób wymiany informacji uległ radykalnej modyfikacji. Obywatele mogą bowiem permanentnie korzystać z przystępnych w obsłudze elektronicznych kanałów komunikacji takich jak Elektroniczna Platforma Usług Administracji Publicznej (ePUAP), czy też e-Urząd Skarbowy (e-US). Dodatkowo od 1 stycznia 2025 r., dysponują oni szeregiem innych form komunikacji elektronicznej, gdyż ustawodawca wprowadził do obrotu prawnego zarówno Publiczną Usługę Hybrydową (PUH), jak również

Publiczną Usługę Rejestrowanego Doręczenia Elektronicznego (PURDE). Co prawda PUH nie generuje obywatelom zasadniczych różnic w zakresie formy doręczenia korespondencji, niemniej jednak faktem kluczowym jest odstąpienie od papierowej formy sporządzania dokumentów. Jest to zatem kolejny krok w sukcesywnie realizowanym procesie pełnego informatyzowania usług administracji publicznej, zaś w 2029 r., do grona stosownych instytucji powinny dołączyć również sądy[2].

Tak więc przed obywatelami kreśli się perspektywa zdalnego prowadzenia komunikacji z organami państwowymi, która *a natura rei* jest mniej absorbująca i przede wszystkim bardziej mobilna dla przeciętnych osób lub podmiotów. Nadto modyfikuje tempo korespondencji, paralelnie eliminując potencjalne wady związane z koniecznością doręczenia przesyłki za pośrednictwem operatora pocztowego. Nie dotyczy to jeszcze alternatywy wykorzystania PUH, jednakże w ujęciu finalnym całokształt działań administracji publicznej powinien dysponować charakterem elektronicznym. W związku z czym podatnicy korzystając, np. ze ścieżki e-US dedykowanej *stricte* kontaktom z organami Krajowej Administracji Skarbowej, czy też obywatele preferujący ePUAP nie będą ponosili dodatkowych obciążeń finansowych związanych z obsługą korespondencji. Elektroniczne kontakty z administracją publiczną stały się bowiem swoistym standardem, który *nolens volens* wyznacza zupełnie inną korelację pomiędzy obywatelem a organem państwowym. Możliwość stopniowego odstąpienia od obecnego charakteru postępowania przewidziano również w projekcie Nowej Ordynacji Podatkowej (Rozporządzenie w sprawie utworzenia, organizacji i trybu działania Komisji Kodyfikacyjnej Ogólnego Prawa Podatkowego, 2014; Rozporządzenie w sprawie zniesienia Komisji Kodyfikacyjnej Ogólnego Prawa Podatkowego, 2024), który uwzględniał chociażby instytucję mediacji pomiędzy

[2] Należy zwrócić uwagę, że od 1.01.2025 r., wdrażana jest w sposób sukcesywny metoda e-Doręczeń marginalizująca wykorzystanie operatora pocztowego – postanowienie Sądu Najwyższego – Izby Cywilnej z 28.03.2024 r., III CZ 42/23, Legalis nr 3063259; Komunikat Ministra Cyfryzacji z 29 maja 2023 r., w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym (Dz.U. z 2023 r. poz. 1077); Warto również zwrócić uwagę na uwarunkowania sfery e-government, a także jego kalendarium w Polsce – Kaczorowska, A. (2013). *E-usługi administracji publicznej w warunkach zarządzania projektami*, Wydawnictwo Uniwersytetu Łódzkiego, s. 17-32.

podatnikiem a organem podatkowym, co dotychczas w ogólnym prawie daninowym było swoistą abstrakcją. Konkretyzując póki co potencjalna perspektywa stworzenia substytutu dla żmudnych i często nieefektywnych procedur wyjaśniających (dowodowych) *a priori* generuje inklinacje sytuującej model krajowego prawodawstwa nieco bliżej systemu common law typowego dla krajów anglosaskich.

Zatem warto zastanowić się, czy pełna informatyzacja usług administracji publicznej nie stanowi asumptu do głębszej refleksji w zakresie toku postępowań jurysdykcyjnych, gdyż wraz z modernizacją wzajemnej komunikacji można dokonać również stopniowej reorganizacji procesowej. Konkretyzując z pewnością organy państwowe wielokrotnie nie są w stanie ustalić stanu faktycznego w sposób niebudzący jakichkolwiek wątpliwości, zaś poszczególne, bezproduktywne i kosztowne działania można ustalić w drodze mediacji, *ergo* przy pomocy wzajemnych ustępstw. Nadto poszczególne kategorie spraw *ad exemplum* o charakterze podatkowych ukierunkowane dyrektywnie na ustalenie dochodu z nieujawnionych źródeł przychodów ograniczają perspektywę stwierdzenia na podstawie dokumentów okoliczności wymaganych dla podjęcia należytego rozstrzygnięcia. Zatem wówczas wątpliwa jest bezwzględna konieczność wyjaśniania węzłowych kwestii merytorycznych w sposób permanentny, ponieważ podatnicy nie tylko fabrykują dowody, lecz także cynicznie wykorzystują aktywności organów celem uzyskania konkretnych korzyści. Mianowicie w praktyce występują sytuacje, w ramach których wszczęcie postępowania podatkowego stanowi wyłączny motyw dla przygotowania dokumentacji rachunkowej (Kuzionko-Ochrymiuk, 2018).

Wady procesu informatyzacji usług administracji publicznej

Newralgiczny proces informatyzacji usług administracji publicznej wiąże się paralelnie z wadami, które generują liczne wątpliwości, gdyż poszczególne grupy społeczne dysponują ograniczonymi zdolnościami w zakresie obsługi aplikacji elektronicznych. Tak więc godnym zastanowienia jest, czy perspektywa rezygnacji z tradycyjnej formy komunikacji jest rozwiązaniem uwzględniającym interesy wszystkich obywateli. Mianowicie obecnie aplikacja Twój e-PIT umożliwiająca złożenie deklaracji podatkowej do właściwego urzędu skarbowego w sposób elektroniczny korzysta

z tzw. mechanizmu automatycznego rozliczenia daninowego, w przypadku gdy podatnik nie dokona tego samodzielnie (Zarządzenie w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów, 2022). Tak więc w ujęciu hipotetycznym obywatele, którzy nie dysponują możliwością zweryfikowania danych przygotowanych przez aplikację Twój e-PIT zostaną pozbawieni prawa do przedstawienia indywidualnego wyniku finansowego. Obecnie mogą oni bowiem złożyć *ad exemplum* formularz zeznania podatkowego PIT-37 w sposób tradycyjny, a więc posiadają alternatywę, której w przyszłości może zabraknąć. Co wówczas powinny zrobić wszystkie te osoby? Zdać się na jakość funkcjonowania aplikacji Twój e-PIT, czy też zwyczajnie udać się na szkolenie z obsługi całego szeregu systemów elektronicznych wymaganych przy kontaktach z administracją publiczną (Kuzionko-Ochrymiuk, 2018).

Poza tym pełna elektronizacja usług sfery publicznej generuje również inne wątpliwości związane m.in. z potencjalnymi przerwami w dostawie prądu, czy też coraz częściej obserwowanymi atakami hakerskimi, które *nolens volens* stymulują rozwój cyberbezpieczeństwa. Mianowicie już obecnie incydentalne deficyty energii elektrycznej generują uzasadniony brak świadczenia pracy przez pracowników merytorycznych, ponieważ ich realizacja ich obowiązków zawodowych warunkowana jest dostępem do funkcjonalnego komputera stacjonarnego, albo mobilnego. Niemniej jednak zasadnicza część jednostek pracuje w sposób tradycyjny, w związku z czym brak jest ryzyka zupełnego paraliżu organizacyjnego, co zwłaszcza w kontekście możliwych kryzysów jest bardzo istotne. Aktualnie obserwujemy bowiem swoistą, polityczną wojnę hybrydową, która immanentnie penetruje interdyscyplinarną sferę ryzyka wzbudzenia sytuacji skrajnych wymagających wystarczającej odporności na konotacje zewnętrzne. Zatem warto rozważyć, czy perspektywa globalnej informatyzacji usług administracji publicznej nie powinna paralelnie uwzględniać swoistego „konserwatywnego buforu bezpieczeństwa", który pozwoliłby zachować ciągłość pracy w przypadkach krytycznych. Względy obiektywne, *ergo* dotyczące zarówno uwarunkowań społecznych, jak również infrastruktury bezpieczeństwa przemawiają za dywersyfikacją form działania organów państwowych. Stwarza to bowiem fundamentalną alternatywę dla permanentnej – nieprzerwanej aktywności zwłaszcza w czasach powszechnego ryzyka, którego z jednej strony nikt nie

deprecjonuje, jednakże z drugiej strony momentami nie traktuje wystarczająco poważnie[3].

Kolejną wadą badanego procesu jest mnogość elektronicznych form komunikacji funkcjonujących w obrocie prawnym od 1 stycznia 2025 r., co mimowolnie generuje liczne kontrowersje również na gruncie judykatury. Otóż szereg aplikacji takich jak PURDE, e-US, ePUAP i PUH samoistnie wzbudzają niejasność dla przeciętnego obywatela, zaś perspektywa zastosowania dwóch ścieżek kontaktowych (PURDE i e-US) w jednej, konkretnej sytuacji *a priori* generuje asumpt do głębszej refleksji, który powinien zostać niezwłocznie rozwiązany. Oddziałuje to bowiem negatywnie na newralgiczny proces wykładni oraz stosowania prawa daninowego, jednocześnie rozpoczynając niepotrzebne spory na linii organy podatkowe – podatnicy. Konkretyzując nakaz zawarty w art. 144 § 1a ustawy Ordynacja podatkowa (1997; dalej jako: O.p.), stwarza liczne problemy interpretacyjne, które w praktyce oczekują dopiero na ugruntowane stanowisko sądów administracyjnych[4]. Jednoznaczne brzmienie powyższego przepisu teoretycznie nie powinno budzić jakichkolwiek wątpliwości, jednakże mnogość form komunikacji elektronicznej sprawia, iż pełnomocnicy mogą dysponować paralelnie zarówno adresem do doręczeń elektronicznych, jak również kontem w systemie e-US. W związku z czym w formularzu pełnomocnictwa szczególnego PPS-1 intencjonalnie deklarują oni gotowość do prowadzenia korespondencji za pośrednictwem kanału PURDE. Natomiast równolegle wyrażają zgodę na wykorzystywanie przez organy skarbowe systemu e-US, co *a natura rei* wprowadza niepotrzebny dualizm elektronicznych form komunikacji. Z kolei to stwarza perspektywę potencjalnego naruszenia norm procesowych przez administrację publiczną, która postępując zgodnie z literalnym brzmieniem art. 144 § 1a O.p., rzekomo kontestuje wolę profesjonal-

[3] Analizując strukturę ewolucji procesu informatyzacji usług administracji publicznej warto zwrócić uwagę na pozycję Polski w Europie, gdyż *a posteriori* generuje to pozytywny asumpt na przyszłość – Kaczorowska, A. (2013). *E-usługi...op. cit.*, s. 17-32; Nadto dotyczy to również uwarunkowań światowych – Ibidem, s. 53-57.

[4] W tym zakresie przywołać można zasadniczo akty judykacyjne sądów administracyjnych, np. wyrok WSA w Gliwicach z 15.02.2024 r., I SA/Gl 794/23, Legalis nr 3049761, czy też wyrok NSA z 3.04.2025 r., III FSK 1578/23, Legalis nr 3225567. Należy bowiem podkreślić, że stosownie do art. 144 § 5 O.p., doręczanie pism pełnomocnikowi będącemu adwokatem, radcą prawnym lub doradcą podatkowym oraz organom administracji publicznej, następuje za pomocą środków komunikacji elektronicznej albo w siedzibie organu podatkowego.

nego pełnomocnika wyrażoną w formularzu pełnomocnictwa (wyrok WSA w Olsztynie z 9.04.2025 r., I SA/Ol 118/25). Jednakże jednocześnie należy dokonać wnikliwej analizy norm art. 35b ust. 1 pkt 2 lit. b) oraz art. 35d ust. 1 ustawy o Krajowej Administracji Skarbowej (2016).

Zatem gdzie leży istota nie tylko prawa, ale fundamentów praworządności, jeżeli uczestnicy postępowania podatkowego mogą cynicznie wykorzystywać model alternatywnego układu komunikacji elektronicznej celem uzyskania partykularnych korzyści prawnych? Jednostronne oddziaływanie na newralgiczny proces doręczania korespondencji stanowi bowiem apodyktyczną i niedopuszczalną ingerencję w standardy demokratycznego państwa prawa. Czemu miało służyć wprowadzenie do krajowego prawodawstwa daninowego systematyki PURDE, w przypadku gdy zdecydowanie wcześniej ustawodawca wdrożył do obrotu normatywnego aplikację e-US? Czy w danym zakresie nie zachodzi konieczność uregulowania występujących już sytuacji kolizyjnych celem wyeliminowania zbędnych sporów sądowych ogniskujących wyłącznie wokół analizowanej kwestii procesowej? Tak więc można *a posteriori* stwierdzić, że przygotowywana od dłuższego czasu radykalna reorganizacja posiada istotne wadliwości, które bezwzględnie winny zostać niezwłocznie zmodyfikowane. Po raz kolejny dochodzi bowiem do sytuacji, gdy pryncypialne *ratio legis* oraz literalna treść przepisu wydają się posiadać charakter wtórny wobec irrelewantnych interesów lobbystycznych uczestników postępowania podatkowego, *ergo* zrzeszeń korporacyjnych. Warto zatem postulować wdrożenie do porządku prawnego norm statuujących pierwszeństwo wykorzystywania w przypadkach kolizyjnych systemu e-US, który ze swej istoty jest dedykowany w kontaktach z organami skarbowymi. Rozwieje to bowiem wszelkie występujące wątpliwości po raz kolejny uwłaczające legislacyjnym standardom państwa członkowskiego UE, paralelnie gwarantując należytą pewność prawodawstwa daninowego[5].

[5] Dodatkowo należy zwrócić uwagę na dynamiczne tempo rozwoju struktury informatyzacji w Polsce, którą na gruncie publicznym dobitnie obrazują zarówno wprowadzenie systemu Elektronicznego Zarządzania Dokumentami (EZD), jak również wdrożenie systemu e-Doręczeń (1.01.2025 r.) – Kuzionko-Ochrymiuk, E. (2018). *Informatyzacja…op. cit.*, s. 165-166; s. 169-172; Lewańska, E., Sokołowska, W., Stróżyna, M. (2016). Projektowanie e-usług dla administracji publicznej w podejściu procesowym – studium przypadku. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42*, 97-102; Goliński, M. (2016). Rozwój e-administracji a rozwój gospodarczy w krajach Unii Europejskiej – próba analizy. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna*

Dodatkowo warto zastanowić się nad sensem dalszego utrzymywania dualizmu elektronicznych form komunikacji pomiędzy alternatywą PURDE a systemem e-US, gdyż jest nie tylko niekonieczne, ale raczej zbędne zarówno dla organów podatkowych, jak również podatników, względnie pełnomocników. Otóż uniwersalny model zastosowania PURDE można porównać do funkcjonalności ePUAP, który znajdował zastosowanie w sposób niezależny od dziedziny. Może zatem perspektywą substytucyjną dla konieczności przygotowania i wdrożenia wymaganych regulacji kolizyjnych będzie modyfikacja systemu e-US, który powinien posiadać pierwszeństwo w kontaktach prowadzonych w toku jurysdykcyjnego postępowania podatkowego. Potencjalne zastrzeżenie sfery użytkowej systemu e-US wyłącznie do indywidualnie oznaczonych czynności procesowych *ad exemplum* doręczenia rozstrzygnięcia kończącego postępowanie, może również stanowić realną alternatywę merytoryczną dla występującej obecnie problematyki interpretacyjnej. Zadaniem krajowego legislatora jest bowiem przygotowanie literalnego brzmienia art. 144 § 1a O.p., w taki sposób, aby nie zachodziła potrzeba wykorzystywania wtórnych metod wykładni, gdyż ta sytuacja praktycznie zawsze generuje spory sądowe. Nadto warto w sposób perspektywiczny zaplanować wykorzystanie zarówno PURDE, jak również systemu e-US chociażby do czasu wiążących decyzji politycznych w badanym przedmiocie, gdyż *quasi* konkurencyjność nie jest potrzebna na gruncie kanałów komunikacji elektronicznej (wyroki WSA w Gliwicach z: 6.04.2023 r., I SA/Gl 870/22; 12.04.2022 r., I SA/Gl 81/22).

Tym samym rozwiązanie swoistego impasu występującego pomiędzy organami skarbowymi a podatnikami i ich pełnomocnikami jest warunkowane przede wszystkim ideą ustawodawcy co do dalszego, prospektywnego rozwoju prawodawstwa daninowego. Alternatywy wdrożenia norm kolizyjnych, czy też normatywnego przypisania poszczególnych czynności procesowych do konkretnych kanałów komunikacji elektronicznej stanowią bowiem merytoryczne propozycje dla dalszej ewolucji struktury

Handlowa w Warszawie, 42, 27; Ludzia, M. (2016). Wybrane aspekty związane z realizacją strategii informatyzacji w urzędach miejskich w Polsce w kontekście koncepcji inteligentnych miast. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42*, 149-150; Szyjewski, Z. (2016). Kwalifikacje informatyczne w administracji. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42*, 227.

e-doręczeń w Polsce. Z kolei to jest zasadniczo pewne, gdyż stopniowa asymilacja wszystkich instytucji publicznych *nolens volens* generuje perspektywę potencjalnych, wtórnych modyfikacji mających na celu dostosowanie uwarunkowań obiektywnych do stanu pożądanego (Kuzionko-Ochrymiuk, 2018; Horbaczewski, 2025).

Podsumowanie

W ujęciu globalnym proces informatyzacji usług administracji publicznej ocenić należy jako bezwzględnie konieczny dla interdyscyplinarnej funkcjonalności nie tylko aparatu państwowego, ale także sfery prywatnej. Permanentna dostępność w kontaktach z organami, czy też sposobność udzielenia odpowiedzi w ciągu kilku minut kreuje bowiem zupełnie inną rzeczywistość w porównaniu do uwarunkowań występujących jeszcze w latach 90 XX w. Nadto na gruncie szeroko rozumianej elektronizacji możemy oczekiwać dalszego, dynamicznego rozwoju, co rodzi nadzieję na kolejne kroki w procesie sukcesywnego upraszczania wzajemnej komunikacji. Zatem wszelkie zalety badanego mechanizmu kwalifikować należy wyłącznie jako konstruktywną podstawę warunkującą sposobność przygotowania modelu wieloletniej ewolucji. Informatyzacja usług administracji publicznej winna bowiem stanowić swoisty punkt zwrotny dla zaawansowania struktury państwowej zwłaszcza w dobie trzeciej dekady XXI w.

Niemniej jednak nie można paralelnie deprecjonować szeregu istotnych niebezpieczeństw, które *nolens volens* wiążą się z procesem sukcesywnego rozwoju administracji publicznej. Problematyka potencjalnych ataków hybrydowych, czy też wykluczenia określonych grup społecznych generuje bowiem perspektywę uwłaczającą standardom nie tylko kraju członkowskiego UE, lecz także uwarunkowaniom demokratycznego państwa prawa. Mianowicie przeciętni przedstawiciele pokolenia Baby boomers mogą posiadać zasadnicze trudności z adaptacją do pełnej informatyzacji usług administracji publicznej, co *per se* zmusza ustawodawcę do zagwarantowania alternatywnych form komunikacji nieelektronicznej. W świetle wynikającej z art. 32 Konstytucji Rzeczypospolitej Polskiej (1997) zasady równości wszystkich wobec prawa każdy obywatel bez względu na wiek, czy też zdolności intelektualne musi dysponować analogicznymi uprawnieniami również w zakresie dostępu do usług struktury państwowej.

Paralelnie krajowy legislator powinien należycie zakwalifikować realną perspektywę intencjonalnego wykorzystania modelu obsługi spraw publicznych do organizacji ataków hybrydowych. Otóż w kontekście permanentnego konfliktu zbrojnego na Ukrainie oraz obserwowanych sukcesywnie działań destabilizacyjnych, które z jednej strony nie stanowią asumptu do pełnoskalowych operacji wojskowych, jednakże z drugiej strony negatywnie oddziałują na autonomię i bezpieczeństwo państwa, należy rozważyć dywersyfikację metodologiczną w danym obszarze. Przechodząc *ad rem* alternatywa dualnego – wymiennego zastosowania formy elektronicznej oraz konwencjonalnej, *ergo* tradycyjnej z pewnością wzmocni architekturę bezpieczeństwa całego regionu Europy Środkowo-Wschodniej, gdyż Polska jest bezspornie krajem pośredniczącym w organizacji pomocy Ukrainie. Dotyczy to zwłaszcza obserwowanych relatywnie często wydarzeń krytycznych takich jak niewyjaśnione pożary poszczególnych budynków, czy też utraty kontroli nad koleją publiczną, których bez wątpienia można było uniknąć przy zastosowaniu wymaganych form wysokiej ostrożności. Nie tylko krajowa klasa polityczna, ale także polskie społeczeństwo muszą bowiem dokonać świadomej transformacji mentalnej zakładającej wzmocnienie profilaktycznych aktywności zaradczych. Sytuacje związane z rojem rosyjskich dronów na terytorium Rzeczypospolitej z pewnością stanowią wyłącznie incydent generujący wysokie prawdopodobieństwo powtarzalności. Niezależnie od jej przypadkowego, czy też radykalnie intencjonalnego charakteru powinniśmy analogicznie jak, np. Finlandia uwzględnić badane ryzyko w ujęciu prospektywnym, a więc obejmującym rozwój w najbliższych co najmniej 10 latach.

Podsumowując, należy postulować wdrożenie sukcesywnego rozwoju elastycznego (dualnego) modelu zarządzania sferą publiczną, gdyż tylko on generuje swoistą, konstruktywną odpowiedź na obiektywne uwarunkowania występujące w rejonie konfliktu zbrojnego. Powszechna informatyzacja rodzi bowiem nie tylko liczne zalety, ale także potencjalną sferę krytyczną dla agresora, który może ją cynicznie wykorzystać bez względu na alternatywne zabezpieczenia. Nadto stabilizacja warunkowana pewnością zarządzania sprawami przeciętnych obywateli pełni niebagatelną rolę w dobie permanentnych napięć politycznych ogniskujących nawet na gruncie militarnym.

Literatura

1. Goliński, M. (2016). Rozwój e-administracji a rozwój gospodarczy w krajach Unii Europejskiej – próba analizy. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie*, *42*.
2. Horbaczewski, R. (2025). *Nowa ustawa o informatyzacji – kluczowe zmiany w cyfryzacji administracji publicznej*. Pobrano z: https://www.prawo.pl/samorzad/zmiany-w-cyfryzacji-administracji-publicznej-nowe-przepisy,534544.html (dostęp: 13.10.2025).
3. Kaczorowska, A. (2013). *E-usługi administracji publicznej w warunkach zarządzania projektami*. Wydawnictwo Uniwersytetu Łódzkiego.
4. Ministerstwo Cyfryzacji. (2023). *Komunikat Ministra Cyfryzacji z 29 maja 2023 r., w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym* (Dz. U. z 2023 r. poz. 1077).
5. Kuzionko-Ochrymiuk, E. (2018). Informatyzacja administracji publicznej w województwach Polski. *Optimum. Economic Studies, 1*(91), 160.
6. Lewańska, E., Sokołowska, W., Stróżyna, M. (2016). Projektowanie e-usług dla administracji publicznej w podejściu procesowym – studium przypadku. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42.*
7. Ludzia, M. (2016). Wybrane aspekty związane z realizacją strategii informatyzacji w urzędach miejskich w Polsce w kontekście koncepcji inteligentnych miast. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42*.
8. Szyjewski, Z. (2016). Kwalifikacje informatyczne w administracji. *Rocznik Kolegium Analiz Ekonomicznych Szkoła Główna Handlowa w Warszawie, 42*.

Akty prawne

1. Postanowienie Sądu Najwyższego – Izby Cywilnej z 28.03.2024 r., III CZ 42/23.

2. Postanowienie WSA w Olsztynie z 9.04.2025 r., I SA/Ol 118/25.
3. Rozporządzenie Rady Ministrów z 21 października 2014 r. w sprawie utworzenia, organizacji i trybu działania Komisji Kodyfikacyjnej Ogólnego Prawa Podatkowego (Dz. U. z 2014 r. poz. 1471).
4. Rozporządzenie Rady Ministrów z 27 maja 2024 r. w sprawie zniesienia Komisji Kodyfikacyjnej Ogólnego Prawa Podatkowego (Dz. U. z 2024 r. poz. 818).
5. Ustawa z 16 listopada 2016 r. o Krajowej Administracji Skarbowej (j.t. Dz. U. z 2025 r. poz. 1131 ze zm.).
6. Ustawa z 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.).
7. Ustawa z 29 sierpnia 1997 r. Ordynacja podatkowa (j.t. Dz. U. z 2025 r. poz. 111 ze zm.).
8. Wyrok NSA z 3.04.2025 r., III FSK 1578/23.
9. Wyrok WSA w Gliwicach z 12.04.2022 r., I SA/Gl 81/22.
10. Wyrok WSA w Gliwicach z 15.02.2024 r., I SA/Gl 794/23.
11. Wyrok WSA w Gliwicach z 6.04.2023 r., I SA/Gl 870/22.
12. Zarządzenie Ministra Finansów z 31 stycznia 2022 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (j.t. Dz. Urz. MF z 2025 r. poz. 7 ze zm.).

Sławomir Żurawski[1]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

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

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

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

Streszczenie

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

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

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

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

Abstract

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

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

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

Wstęp

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

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

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

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

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

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

Definicja i znaczenie cyberbezpieczeństwa

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

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

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

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

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

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

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

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

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

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

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

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

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

Rozwoju i ewolucja cyberzagrożeń

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

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

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

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

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

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

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

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

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

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

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

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

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

Tabela 1. Najskuteczniejsza metoda w ochronie przed cyberzagrożeniami według respondentów

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

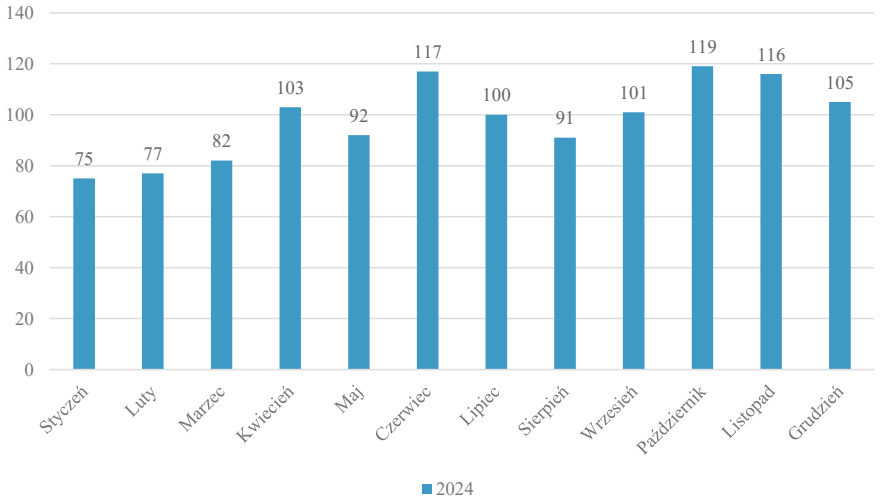
Źródło: opracowanie własne na podstawie: Vecto Sp. z o.o. (2023). *Cyberbezpieczeństwo w polskich firmach 2023*, s. 10-12 (dostęp: 27.09.2025 r.).

Wnioski dotyczącej tabeli o najskuteczniejszych metodach ochrony przed cyberzagrożeniami:

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

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

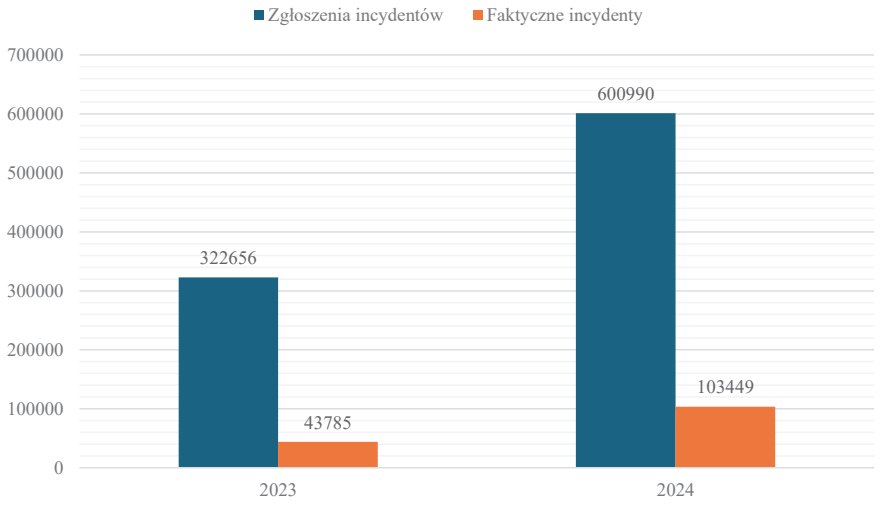
W 2024 roku w Słowacji większość zgłoszeń o incydentach cyberbezpieczeństwa wpłynęła w drugiej połowie roku. W 2024 roku SK-CERT otrzymał o 204 zgłoszenia więcej niż w roku poprzednim. Wzrost liczby zgłaszanych incydentów można przypisać procesowi legislacyjnemu transpozycji dyrektywy NIS2, która rozszerza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



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

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

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

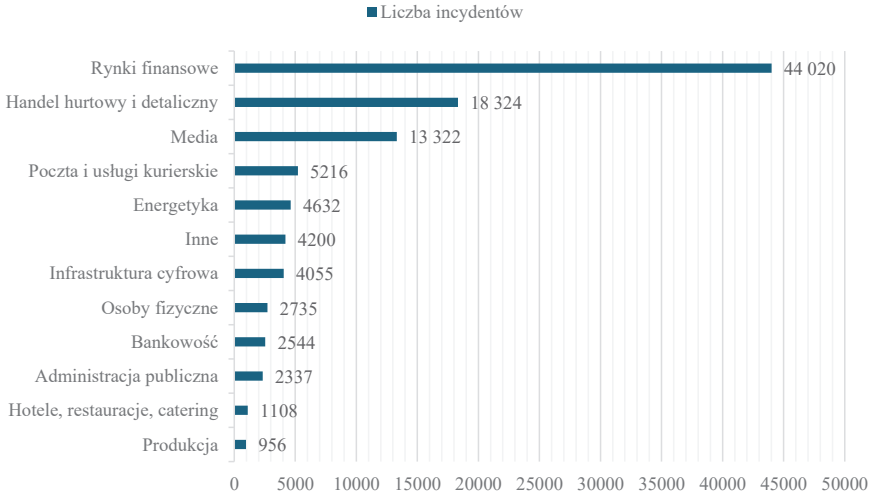


Rysunek 2. Liczba zarejestrowanych zgłoszeń oraz incydentów cyberbezpieczeństwa w latach 2023-2024

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

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

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



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

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

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

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

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

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

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

Poprawa systemu cyberbezpieczeństwa – praktyczne rekomendacje dla Polski i Słowacji

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

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

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

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

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

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

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

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

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

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

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

Podsumowanie

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

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

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

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

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

Literatura

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

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

Barbara Drapikowska[1], Sylwia Borawska[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103359_4

ROLA UŻYTKOWNIKA W KSZTAŁTOWANIU CYBERBEZPIECZEŃSTWA ORGANIZACJI

THE USER'S ROLE IN SHAPING AN ORGANIZATION'S CYBERSECURITY

Streszczenie

Rozdział poświęcono analizie roli użytkownika w kształtowaniu cyberbezpieczeństwa organizacji, ze szczególnym uwzględnieniem znaczenia kompetencji cyfrowych jako czynnika warunkującego odporność na zagrożenia cybernetyczne. Problem badawczy sformułowano w postaci pytania: w jakim stopniu kompetencje cyfrowe użytkowników warunkują odporność organizacji na cyberataki? Celem rozdziału było określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na zagrożenia w cyberprzestrzeni. Przyjęto hipotezę badawczą, zgodnie z którą wyższy poziom kompetencji cyfrowych użytkowników istotnie zwiększa zdolność organizacji do zapobiegania, wykrywania oraz reagowania

[1] https://orcid.org/0000-0002-6852-2791, e-mail: b.drapikowska@akademia.mil.pl
[2] https://orcid.org/0009-0006-6851-9492, e-mail: borawska.sylwia@o2.pl

na incydenty cyberbezpieczeństwa. W rozdziale zastosowano teoretyczne metody badawcze, obejmujące analizę i ocenę literatury przedmiotu, analizę dokumentów strategicznych i raportów instytucjonalnych (m.in. ENISA, CERT Polska, IBM Security), a także metodę syntezy i porównania istniejących ujęć kompetencji cyfrowych w kontekście bezpieczeństwa informacji. Przeprowadzone rozważania wykazały, że kompetencje cyfrowe obejmujące wiedzę, umiejętności oraz postawy użytkowników w znacznym stopniu determinują poziom cyberodporności organizacji. W konsekwencji kompetencje cyfrowe należy traktować jako jeden z kluczowych czynników kształtujących poziom bezpieczeństwa informacji oraz stabilność funkcjonowania organizacji we współczesnym środowisku cyfrowym.

Słowa kluczowe: kompetencje cyfrowe, cyberbezpieczeństwo, odporność, edukacja

Abstract

The chapter is devoted to the analysis of the role of the user in shaping the cybersecurity of the organization, with particular emphasis on the importance of digital competences as a factor determining resilience to cyber threats. The research problem was formulated in the form of a question: to what extent do users' digital competencies determine the resilience of an organization to cyberattacks? The aim of the chapter was to determine the role of digital competences of users in building the organization's resilience to threats in cyberspace. The research hypothesis was adopted, according to which a higher level of digital competence of users significantly increases the organization's ability to prevent, detect and respond to cybersecurity incidents. The chapter uses theoretical research methods, including analysis and critical evaluation of the literature on the subject, analysis of strategic documents and institutional reports (m.in. ENISA, CERT Polska, IBM Security), as well as a method of synthesizing and comparing existing approaches to digital competences in the context of information security. The conducted considerations have shown that digital competencies, including the knowledge, skills and attitudes of users, significantly determine the level of cyber resilience of an organization. As a consequence, digital competences should be treated as one of the key factors shaping the level of information security and the stability of the organization's functioning in the modern digital environment.

Keywords: digital competences, cybersecurity, resilience, education

Wstęp

Dynamiczny rozwój technologii informacyjno-komunikacyjnych sprawił, że cyberbezpieczeństwo stało się jednym z kluczowych obszarów funkcjonowania współczesnych organizacji. Złożoność środowiska cyfrowego, rosnąca liczba zagrożeń oraz powszechne wykorzystywanie narzędzi sieciowych powodują, że ochrona informacji przestaje być wyłącznie zagadnieniem technicznym. W raportach branżowych wskazuje się, iż znaczna część incydentów bezpieczeństwa ma swoje źródło w działaniach użytkowników, a nie w niedoskonałości samych systemów informatycznych (Verizon, 2024).

Jednocześnie obserwuje się wyraźne zróżnicowanie poziomu przygotowania pracowników do funkcjonowania w środowisku zagrożeń cyfrowych. Europejska Agencja ds. Cyberbezpieczeństwa zwraca uwagę, że kompetencje użytkowników w zakresie bezpiecznego korzystania z technologii nie zawsze nadążają za tempem cyfryzacji procesów organizacyjnych (ENISA, 2020). Z kolei raport IBM Security (2024) podkreśla, że organizacje charakteryzujące się wyższym poziomem przygotowania personelu skuteczniej ograniczają skutki incydentów.

W tym kontekście zasadne staje się podjęcie refleksji nad zależnością pomiędzy poziomem kompetencji cyfrowych użytkowników a zdolnością organizacji do funkcjonowania w warunkach rosnących zagrożeń. Rozważania te prowadzą do sformułowania problemu badawczego dotyczącego tego, w jakim stopniu kompetencje cyfrowe warunkują odporność organizacji na cyberataki? a także do wyznaczenia celu niniejszego rozdziału, którym jest określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na cyberataki.

Znaczenie kompetencji cyfrowych użytkowników

Współczesne cyberbezpieczeństwo nie może być rozpatrywane wyłącznie przez pryzmat technologii – coraz więcej badań wskazuje, że czynnik ludzki jest kluczowym determinantem sukcesu lub porażki systemów ochrony informacji. Tradycyjne modele ochrony koncentrowały się na rozwiązaniach technicznych tj. zapory sieciowe, systemy wykrywania włamań czy zaawansowane algorytmy kryptograficzne, jednak praktyka

pokazuje, że najczęstsze naruszenia bezpieczeństwa wynikają z błędów lub niewłaściwych zachowań samych użytkowników.

W literaturze zjawisko to jest intensywnie analizowane jako zagadnienie interdyscyplinarne, łączące aspekty psychologii, organizacji i technologii – co pokazuje najnowsza przeglądowa analiza literatury w dziedzinie „human factors in cybersecurity" (Khadka, Barkat Ullah, 2025). Takie spojrzenie znajduje odzwierciedlenie w literaturze i praktyce: organizacje, które traktują bezpieczeństwo jako wspólną odpowiedzialność, osiągają lepsze wyniki w ograniczaniu incydentów niż te, które koncentrują się jedynie na technologii i procedurach formalnych (Verizon, 2024).

W tym kontekście rola pojedynczego użytkownika jest szczególnie istotna – to on codziennie podejmuje decyzje, które albo wzmacniają bariery ochronne, albo je osłabiają. W tak złożonym dzisiejszym środowisku same zabezpieczenie techniczne bez wsparcia odpowiednich zachowań użytkowników nie wystarczają. Tak więc użytkownicy systemów organizacyjnych pełnią dziś wiele ról: są operatorami, decydentami, klientami wewnętrznymi i pierwszą linią kontaktu z potencjalnymi zagrożeniami. W praktyce oznacza to, że każda interakcja użytkownika z systemem komputerowym może stać się momentem podatności lub przeciwnie, wzmocnienia bezpieczeństwa. Procesy tj. rozpoznawanie phishingu, stosowanie zasad haseł, aktualizowanie oprogramowania czy reagowanie na podejrzane zdarzenia stanowią integralne elementy organizacyjnej odporności.

W literaturze termin „human firewall" (Włodarczyk, 2020) został użyty właśnie po to, aby podkreślić, że świadome i kompetentne działania personelu mogą działać jak uzupełniający, aktywny element systemu ochrony, redukując zależność od pasywnych narzędzi IT.

Aby właściwie zrozumieć uwarunkowania omawianego problemu badawczego, konieczne jest doprecyzowanie pojęcia kompetencji cyfrowych. Zgodnie ze stanowiskiem Ministerstwa Cyfryzacji (2020) są one definiowane jako „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".

W kontekście funkcjonowania organizacji kompetencje te warunkują zdolność użytkowników do efektywnego i bezpiecznego wykonywania obowiązków zawodowych w środowisku opartym na technologiach cyfrowych.

Oznacza to, że pracownik nie tylko potrafi posługiwać się narzędziami informatycznymi, lecz również rozumie konsekwencje swoich działań w cyberprzestrzeni, potrafi rozpoznawać sytuacje ryzykowne oraz świadomie stosuje zasady bezpieczeństwa informacji.

Vademecum Bezpieczeństwa Informacyjnego (2020) wydane przez Uniwersytet Komisji Edukacji Narodowej (UKEN) kompetencje cyfrowe należy postrzegać jako „zespół umiejętności, wiedzy i postaw umożliwiających świadome i krytyczne korzystanie z technologii cyfrowych (w tym z Internetu) w celu uczenia się, pracy i aktywnego udziału w społeczeństwie informacyjnym". Takie ujęcie akcentuje wielowymiarowy charakter kompetencji cyfrowych i wskazuje, że ich istotą nie jest jedynie biegłość techniczna, lecz zdolność do refleksyjnego funkcjonowania w środowisku cyfrowym.

Pierwszym komponentem, który wskazał UKEN jest wiedza, obejmująca rozumienie sposobu, w jaki technologie cyfrowe wspierają komunikację, kreatywność oraz innowacyjność, a także świadomość ich ograniczeń, potencjalnych konsekwencji i zagrożeń. Obejmuje ona znajomość podstawowych zasad działania technologii, rozumienie mechanizmów leżących u podstaw ich rozwoju oraz umiejętność krytycznej oceny wiarygodności informacji i danych rozpowszechnianych w środowisku cyfrowym, z uwzględnieniem aspektów prawnych i etycznych.

Drugim obszarem są umiejętności, które pozwalają użytkownikom nie tylko na bierne korzystanie z narzędzi cyfrowych, lecz także na aktywne uczestnictwo w procesach komunikacji, współpracy i tworzenia treści. Obejmują one zdolność do wyszukiwania, filtrowania, oceny i przetwarzania informacji, tworzenia i udostępniania zasobów cyfrowych, a także zarządzania własną tożsamością cyfrową oraz ochrony danych. W tym wymiarze istotne staje się również rozpoznawanie możliwości zastosowania nowych technologii, w tym rozwiązań opartych na sztucznej inteligencji, w sposób efektywny i bezpieczny.

Trzecim elementem są postawy, rozumiane jako refleksyjne, krytyczne i odpowiedzialne podejście do korzystania z technologii cyfrowych. Obejmują one otwartość na zmiany technologiczne, gotowość do uczenia się, a także etyczne i bezpieczne korzystanie z narzędzi cyfrowych, z poszanowaniem zasad ochrony prywatności, danych oraz innych użytkowników. Postawy te decydują o tym, czy posiadana wiedza i umiejętności zostaną

wykorzystane w sposób sprzyjający zarówno rozwojowi jednostki, jak i bezpieczeństwu organizacji.

Wskazane składowe kompetencji cyfrowych stanowią dziś nie tylko element indywidualnego rozwoju użytkowników, lecz również istotny zasób organizacyjny. Ich poziom wpływa na sposób realizacji codziennych procesów, jakość podejmowanych decyzji oraz zdolność organizacji do reagowania na sytuacje kryzysowe w cyberprzestrzeni. W praktyce oznacza to, że kompetencje cyfrowe pracowników przestają być wyłącznie kwestią sprawności obsługi narzędzi, a stają się jednym z filarów bezpieczeństwa. Warto podkreślić, że „umiejętności cyfrowe mają kluczowe znaczenie dla strategii cyfrowej UE na rzecz zapewnienia suwerenności technologicznej, zniwelowania przepaści cyfrowej i promowania środowiska cyfrowego skoncentrowanego na człowieku w całej UE" (Komisja Europejska, 2025).

Podstawowe kompetencje cyfrowe stanowią fundament aktywnego uczestnictwa w życiu społecznym oraz na rynku pracy. Dynamiczny rozwój przełomowych technologii – tj. sztuczna inteligencja, środowiska wirtualne, robotyka, technologie kwantowe czy sieci 6G – powoduje rosnące zapotrzebowanie na nowy zestaw zaawansowanych kwalifikacji cyfrowych.

Tak jak zostało już wskazane, współczesny użytkownik nie jest jedynie odbiorcą technologii, lecz aktywnym uczestnikiem procesów bezpieczeństwa, którego postawy i decyzje bezpośrednio wpływają na poziom ochrony zasobów informacyjnych. Według raportu Polskiej Agencji Rozwoju Przedsiębiorczości (PARP) kompetencje cyfrowe stały się jednym z kluczowych trendów rynku pracy, a ich brak jest często wymieniany jako bariera dla efektywnego wykonywania zadań w nowoczesnym środowisku cyfrowym (PARP, 2024).

Jednocześnie krajowe programy rozwoju kompetencji, tj. Poland Digital Competence Development Programme 2020-2030, podkreślają strategiczne znaczenie umiejętności cyfrowych nie tylko dla osób pracujących w sektorze IT, ale dla całej społeczności w różnych branżach (Digital Skills and Jobs Platform, 2020). Komisja Europejska wskazuje, że w ponad 90% miejsc pracy w UE wymagane są co najmniej podstawowe umiejętności cyfrowe. W perspektywie do 2030 roku takie kompetencje wymagane będą w 9 na 10 miejsc pracy. Ich znaczenie rośnie również w Polsce (Rogacka, 2022).

Użytkownik powinien posiadać zestaw pożądanych cech, które są pożądne, należy do nich przede wszystkim zdolność do szybkiego uczenia się technologii i narzędzi cyfrowych. Pracodawcy coraz częściej oczekują, że nowi pracownicy nie tylko będą potrafili korzystać z obecnych rozwiązań, lecz także będą gotowi do szybkiej adaptacji w obliczu nowych technologii oraz zagrożeń. Co idzie za tym do dalszych etapów rekrutacji będą przechodzi osoby, które właśnie ten zestaw cech posiadają, a pracodawca ewentualnie będzie dawał możliwości ich rozwoju. Ten rodzaj elastyczności i otwartości na rozwój jest kluczowy w środowisku, gdzie narzędzia, protokoły i standardy bezpieczeństwa zmieniają się bardzo dynamicznie (Pawłowska-Cyprysiak, Hildt-Ciupińska, 2024).

Równie istotna jest umiejętność oceniania informacji cyfrowych, co wiąże się bezpośrednio z rozpoznawaniem prób manipulacji, deepfake, phishingu czy dezinformacji. W kulturze organizacyjnej, w której cyberzagrożenia są coraz bardziej wyrafinowane, użytkownik musi umieć ocenić wiarygodność źródeł, komunikatów czy plików, zanim podejmie działania mogące mieć konsekwencje dla bezpieczeństwa sieciowego. Stworzenie automatycznego nawyku sprawdzania rzetelności informacji nie jest łatwe jednak jak mówi przysłowie „praktyka czyni mistrza", ilekroć znajdzie się informację należy najpierw ją zweryfikować.

Kolejną pożądaną kwalifikacją jest znajomość zasad bezpiecznego korzystania z technologii, obejmująca m.in. świadome zarządzanie hasłami, stosowanie uwierzytelniania wieloskładnikowego czy umiejętność właściwego reagowania na incydenty cybernetyczne. Tego rodzaju kompetencje nie są typowymi „umiejętnościami twardymi" jak programowanie, lecz należą do obszaru cyberhigieny (Ministerstwo Cyfryzacji, 2022) – codziennych praktyk, które znacząco ograniczają ryzyko naruszeń.

Nie mniej ważna jest umiejętność komunikacji i współpracy cyfrowej w zespole, co staje się kluczowe w sytuacjach wymagających szybkiej wymiany informacji i koordynacji działań reagowania na zagrożenia. Najważniejszym zasobem organizacji są ludzie, a jak ludzie to i komunikacja, która musi być jasna i zrozumiała dla każdego elementu tworzącego zespół. W pracy zespołowej kompetencje te umożliwiają nie tylko wydajną pracę, lecz także skuteczne wdrażanie procedur bezpieczeństwa i wymianę wiedzy.

Wreszcie, cechą coraz częściej wymienianą w kontekście rynku pracy jest odpowiedzialność cyfrowa – postawa zakładająca aktywne dbanie

o bezpieczeństwo własne i organizacji, zgodnie z zasadami etycznego i świadomego korzystania z technologii. Ta postawa obejmuje refleksję nad konsekwencjami własnych działań w cyberprzestrzeni oraz gotowość do stałego doskonalenia swoich kwalifikacji w odpowiedzi na nowe wyzwania. Tak rozumiane cechy i kwalifikacje użytkownika nie tylko zwiększają jego wartość jako pracownika cyfrowego, lecz również dają wartość dodatnią dla całej organizacji.

Warto również wskazać, że użytkownik tak jak wcześniej zostało podkreślone jest aktywnym użytkownikiem wirtualnej przestrzeni, co niesie za sobą również skutki. Błędy użytkowników rzadko mają charakter „drobnych potknięć" – w praktyce mogą uruchamiać łańcuch zdarzeń prowadzący do incydentu, kosztów operacyjnych, konsekwencji prawnych oraz długotrwałej utraty zaufania. Co istotne, liczne analizy pokazują, że komponent ludzki jest regularnie obecny w znaczącej części naruszeń: w ujęciu globalnym Verizon (2024) wskazuje, że human element był składową 68% naruszeń w analizowanym zbiorze danych. Na gruncie polskim rosnąca skala incydentów opartych na socjotechnice jest widoczna w danych CERT Polska: w 2024 r. liczba zgłoszeń przekroczyła 600 tys., a najczęstszym incydentem był phishing; sam phishing stanowił 40 120 zarejestrowanych incydentów (Kancelaria Prezesa Rady Ministrów, 2025).

Jedną z konsekwencji są przede wszystkim finanse, które obejmują zarówno koszty „twarde" (np. przywracanie działania systemów, usługi zewnętrzne, obsługa prawna), jak i koszty wtórne (np. utrata klientów, działania naprawcze, komunikacja kryzysowa). Raport IBM Security (2024) wskazuje, że ataki phishingowe (silnie zależne od reakcji użytkownika) należą do najbardziej kosztownych wektorów naruszeń. Błąd użytkownika bywa punktem wejścia do zdarzeń, które realnie zatrzymują procesy biznesowe: zainfekowanie stacji roboczej, przejęcie konta, nieuprawnione udostępnienie danych czy uruchomienie złośliwego załącznika. Skutkiem jest często nie tylko problem IT, ale przerwanie usług, opóźnienia operacyjne i konieczność pracy w trybie awaryjnym. IBM podkreśla, że w kosztach incydentu istotną rolę odgrywa system downtime (przestój), a „czas oznacza pieniądze" – dłuższy cykl wykrycia i opanowania incydentu wiąże się z wyższymi kosztami (IBM Security, 2024).

Błędy użytkowników są szczególnie kosztowne w ekosystemie oszustw „na człowieka" (phishing/smishing/vishing). W Polsce skala tego

zjawiska jest dobrze widoczna w danych CERT Polska: w 2024 r. odnotowano m.in. 355 tys. zgłoszeń podejrzanych SMS-ów, a działania ochronne oparte na zgłoszeniach i blokowaniu przez operatorów pozwoliły ograniczać skutki kampanii smishingowych (Kancelaria Prezesa Rady Ministrów, 2025). Z perspektywy organizacji oznacza to, że pojedynczy błąd pracownika może skutkować nie tylko incydentem jednostkowym, ale też „otwarciem drzwi" do kolejnych prób wyłudzeń w tej samej sieci relacji (podszycia pod współpracowników, przejęcia komunikacji, fałszywe faktury itp.). Warto również wskazać utratę zaufania interesariuszy (klientów, partnerów, obywateli) które jest skutkiem trudnym do szybkiego odwrócenia. Nawet gdy incydent zostanie technicznie opanowany, organizacja pozostaje z kosztami komunikacji kryzysowej, koniecznością informowania o naruszeniu (w przypadkach wymaganych prawem) oraz ryzykiem długofalowego osłabienia reputacji. IBM Security (2024) wprost ujmuje „lost customers" i „reputation damage" jako elementy kosztów ponoszonych po naruszeniu.

W świetle przedstawionych rozważań staje się oczywiste, że użytkownik przestaje być jedynie odbiorcą technologii, a staje się współtwórcą poziomu bezpieczeństwa organizacji. Ostateczny kształt ochrony informacji nie zależy wyłącznie od systemów i procedur, lecz od codziennych, często pozornie drobnych decyzji podejmowanych przez ludzi. To właśnie na styku kompetencji, postaw i praktyki organizacyjnej rozstrzyga się realna odporność na zagrożenia cyfrowe. Dlatego rozwój kompetencji cyfrowych należy postrzegać nie jako koszt, lecz jako inwestycję w stabilność i ciągłość działania organizacji.

Rozwój kompetencji cyfrowych

W obliczu gwałtownej transformacji cyfrowej rozwój kompetencji cyfrowych przestaje być kwestią fakultatywną – staje się imperatywem zarówno dla jednostek, jak i organizacji. W Polsce funkcjonuje kompleksowy Program Rozwoju Kompetencji Cyfrowych, którego celem jest zapewnienie każdemu obywatelowi możliwości podnoszenia umiejętności cyfrowych na różnych etapach życia, począwszy od edukacji wczesnoszkolnej, aż po wsparcie dorosłych pracowników i seniorów. Program ten ma również za zadanie wspierać rozwój rynku pracy oraz włączenie społeczne poprzez eliminowanie luk kompetencyjnych związanych z technologiami cyfrowymi

(Monitor Polski, 2023). Strategie rozwoju kompetencji cyfrowych w kontekście cyberbezpieczeństwa zakładają nie tylko zdobywanie wiedzy teoretycznej, ale przede wszystkim nabywanie praktycznych umiejętności adaptacyjnych, które umożliwiają użytkownikom świadomość zagrożeń oraz właściwe reagowanie w sytuacjach ryzykownych. Badania nad kompetencjami cyfrowymi podkreślają, że są one kluczowe dla funkcjonowania we współczesnym środowisku pracy, w którym technologie cyfrowe stały się narzędziem codziennych zadań zawodowych (European Training Foundation, 2018).

W skali europejskiej funkcjonują ramy takie jak Digital Competence Framework for Citizens (DigComp), które wskazują obszary kluczowe dla rozwoju kompetencji cyfrowych i są to:

1. Informacja i dane.

Ten segment obejmuje umiejętność wyszukiwania, gromadzenia, analizowania i oceniania informacji cyfrowej. Użytkownik powinien być zdolny do identyfikowania wartościowych źródeł informacji, rozróżniania ich wiarygodności oraz rozumienia znaczenia danych w określonym kontekście. Ta kompetencja jest fundamentalna, gdyż właściwe zarządzanie informacją jest podstawą podejmowania świadomych decyzji oraz unikania dezinformacji i manipulacji.

2. Komunikacja i współpraca.

Kompetencje w tym obszarze dotyczą efektywnego uczestnictwa w środowisku cyfrowym, w tym komunikowania się, współdzielenia zasobów, pracy w zespołach online oraz uczestnictwa w społecznościach cyfrowych. Istotna jest również umiejętność dostosowania komunikacji do różnych narzędzi i kulturowych kontekstów oraz rozumienie zasad netykiety. W kontekście bezpieczeństwa umiejętność ta zmniejsza ryzyko błędów wynikających z nieporozumień komunikacyjnych i pomaga w koordynacji działań związanych z reagowaniem na występujące incydenty.

3. Tworzenie treści cyfrowych.

Ten obszar odnosi się do tworzenia, przetwarzania i prezentowania treści cyfrowych – zarówno prostych, jak i bardziej złożonych. Obejmuje to edycję i integrację różnych formatów danych, programowanie, a także rozumienie zasad praw autorskich i licencjonowania. Umiejętność ta pozwala użytkownikom nie tylko „konsumować" treści, lecz aktywnie je kreować i modyfikować zgodnie z ich potrzebami.

4. Bezpieczeństwo.

Kompetencje bezpieczeństwa odnoszą się do świadomego i odpowiedzialnego korzystania z technologii z uwzględnieniem ochrony własnej i innych osób. Obejmują ochronę danych osobowych, prywatności, zarządzanie tożsamością cyfrową oraz rozumienie i stosowanie zasad bezpieczeństwa informatycznego. Kompetencje w tym obszarze są szczególnie ważne w kontekście cyberzagrożeń – przeciwdziałanie wyciekom, ochrona przed atakami socjotechnicznymi czy właściwe zabezpieczanie urządzeń są elementami codziennego cyberdziałania.

5. Rozwiązywanie problemów.

Ostatni obszar dotyczy identyfikowania potrzeb i zasobów cyfrowych oraz podejmowania świadomych decyzji co do wyboru narzędzi i sposobów ich zastosowania. Umiejętność rozwiązywania problemów cyfrowych polega na stosowaniu logicznego myślenia, analizie błędów i optymalizacji procesów, a także adaptacji do nowych technologii. Kompetencje te umożliwiają użytkownikom radzenie sobie z nowymi wyzwaniami oraz efektywne wykorzystywanie technologii w różnych kontekstach życia zawodowego i prywatnego.

Ramy te stanowią punkt odniesienia dla tworzenia programów szkoleniowych i polityk edukacyjnych w państwach członkowskich, w tym również w Polsce.

W praktyce przyjęty jest „model 4K", który wyróżnia cztery główne kompetencje:

- krytyczne myślenie – zdolność do analizy informacji, oceny ich wiarygodności oraz dostrzegania potencjalnych zagrożeń w środowisku cyfrowym. Użytkownik potrafiący myśleć krytycznie nie reaguje automatycznie na otrzymane komunikaty, lecz weryfikuje ich źródło i kontekst. Ma to szczególne znaczenie w przypadku phishingu czy dezinformacji, gdzie emocjonalny przekaz ma skłonić do pochopnych działań,
- kreatywność – to umiejętność poszukiwania nowych rozwiązań problemów oraz elastycznego wykorzystywania dostępnych narzędzi. Nie chodzi wyłącznie o tworzenie treści, lecz o twórcze podejście do bezpieczeństwa i organizacji pracy,

- komunikacja – zdolność jasnego przekazywania informacji w kanałach cyfrowych oraz właściwe rozumienie otrzymywanych treści. W kontekście cyberbezpieczeństwa ważne jest precyzyjne zgłaszanie incydentów i ostrzeganie współpracowników przed zagrożeniami. Użytkownik kompetentny komunikacyjnie potrafi opisać problem techniczny w sposób jasny i zrozumiały,
- kooperacja – umiejętność współpracy z innymi przy wykorzystaniu narzędzi cyfrowych oraz wspólnego rozwiązywania problemów bezpieczeństwa. Cyberzagrożenia rzadko dotyczą pojedynczej osoby, dlatego kluczowe jest działanie zespołowe (Nowa Era, 2024).

Rozwój kompetencji cyfrowych nie jest procesem jednorazowym ani jednowymiarowym. W praktyce obejmuje różne formy edukacji, od formalnego kształcenia w szkołach i na uczelniach aż po działania samokształceniowe i inicjatywy organizacyjne. Jak zauważają autorzy raportu UNESCO (2021), edukacja cyfrowa powinna być integralną częścią nauczania na wszystkich poziomach, aby przygotować obywateli do aktywnego i bezpiecznego uczestnictwa we współczesnym społeczeństwie informacyjnym.

Edukacji formalnej, która obejmuje system szkolnictwa podstawowego, średniego i wyższego, warto podkreślić, że elementy kompetencji cyfrowych są coraz częściej wpisane w program nauczania. W Polsce zgodnie z podstawą programową elementy komunikacyjne i informatyki uwzględniają zagadnienia związane z bezpieczeństwem w sieci (Dziennik Ustaw RP, 2018). Marlena Plebańska podkreśla, że system edukacji formalnej – od etapu szkoły podstawowej po studia – stanowi pierwszą i najważniejszą ścieżkę nabywania kompetencji cyfrowych, integrując wiedzę teoretyczną z praktycznymi działaniami edukacyjnymi (Plebańska, 2023).

W literaturze zwraca się uwagę, że edukacja w obszarze mediów i technologii musi nadążać za zmianami rzeczywistości cyfrowej. Grzegorz Ptaszek (2019) podkreśla: „edukacja medialna musi rozwijać się równolegle do zmian rzeczywistości". Tę zasadę można bezpośrednio odnieść do kompetencji cyfrowych w organizacjach: jeżeli szkolenie i praktyki nie są aktualizowane, użytkownicy działają według nieadekwatnych schematów, co zwiększa podatność na błędy i manipulacje.

Z perspektywy szkolnictwa wyższego interesujące są również polskie opracowania wskazujące, że problematyka bezpieczeństwa i zagrożeń

w społeczeństwie informacyjnym bywa w programach kształcenia ujmowana niewystarczająco – co uzasadnia potrzebę bardziej systemowego włączania elementów bezpieczeństwa cyfrowego do edukacji formalnej (Stachowiak, 2012). W konsekwencji, sensowne projektowanie ścieżek edukacyjnych powinno łączyć treści kompetencyjne (informacja, komunikacja, tworzenie treści, bezpieczeństwo, rozwiązywanie problemów) z praktyką i odpowiedzialnością użytkownika, ponieważ dopiero taki model buduje trwałe zachowania w środowisku cyfrowym.

Edukacja pozaformalna stanowi obecnie jeden z najważniejszych filarów rozwoju kompetencji cyfrowych, zwłaszcza wśród osób dorosłych, które zakończyły już etap kształcenia szkolnego. W odróżnieniu od edukacji formalnej ma ona charakter elastyczny, krótkookresowy i silnie powiązany z praktycznymi potrzebami użytkowników oraz rynku pracy. Forma edukacji pozaformalnej jest bardzo zróżnicowana. Obejmuje kursy i warsztaty organizowane przez instytucje społeczne, uczelnie trzeciego wieku (UTW), organizacje pozarządowe oraz działania realizowane w ramach programów publicznych i unijnych, które adresują potrzeby rozwojowe osób dorosłych. W kontekście kompetencji cyfrowych szczególnie ważne są programy skoncentrowane na praktycznych umiejętnościach, tj. bezpieczne korzystanie z narzędzi cyfrowych, zarządzanie informacją czy reagowanie na zagrożenia w sieci – to one uzupełniają formalne treści edukacyjne i pozwalają użytkownikom na bieżąco aktualizować swoją wiedzę. Edukacja pozaformalna jest ściśle powiązana z pojęciem *uczenia się przez całe życie* (lifelong learning) – koncepcji uznanej za kluczową w politykach edukacyjnych Unii Europejskiej i szeroko opisaną w kontekście kompetencji cyfrowych.

Z kolei samokształcenie to proces indywidualnego rozwijania umiejętności i wiedzy poza formalnymi i instytucjonalnymi strukturami edukacyjnymi. W praktyce oznacza to korzystanie z zasobów cyfrowych - platformy np. NAVOICA, tutoriale wideo, webinaria, materiały open access, a także aktywne uczestnictwo w społecznościach praktyków i forach dyskusyjnych. W polskich realiach samokształcenie w obszarze cyfrowym zyskuje szczególne znaczenie wśród osób dorosłych, które muszą reagować na zmiany w miejscu pracy lub w życiu codziennym – od korzystania z e-administracji po świadome zabezpieczanie swoich danych (Ćwiek, Maj-Serwatka, 2024).

W świecie, w którym technologie zmieniają się szybciej niż procedury i regulaminy, to właśnie zdolność do uczenia się, aktualizowania wiedzy

decyduje o rzeczywistej dojrzałości cyfrowej. Edukacja formalna wyznacza kierunek, pozaformalna nadaje mu praktyczny wymiar, a samokształcenie pozwala reagować na to, czego nie przewidziały żadne programy nauczania. Dopiero ich połączenie sprawia, że kompetencje cyfrowe przestają być teorią, a stają się codziennym nawykiem działania. W tym sensie rozwój użytkownika staje się najtrwalszym mechanizmem cyberbezpieczeństwa – cichym, lecz skuteczniejszym niż najbardziej zaawansowane technologie.

Bariery w podnoszeniu kompetencji cyfrowych

Podnoszenie kompetencji cyfrowych we współczesnych organizacjach – i szerzej w społeczeństwie – napotyka na wiele przeszkód, które wynikają zarówno z ograniczeń strukturalnych, jak i indywidualnych oraz organizacyjnych. W podnoszeniu kompetencji cyfrowych zwykle nie przeszkadza jeden czynnik, tylko zestaw barier nakładających się na siebie – od „twardych" (sprzęt, łącze, środowisko pracy) po „miękkie" (postawy, motywacja, kultura organizacyjna).

Najnowsze badania i analizy wskazują, że rozwój tych kompetencji nie jest automatyczną konsekwencją dostępu do narzędzi cyfrowych, lecz procesem zależnym od szeregu uwarunkowań, których pokonywanie wymaga świadomego planowania i wsparcia (Urząd Marszałkowski Województwa Śląskiego, 2025). W analizach dotyczących polskich przedsiębiorstw jako najczęściej występujące przeszkody wskazuje się przede wszystkim: brak czasu na rozwój, niedostateczne wsparcie ze strony organizacji, niską świadomość znaczenia kompetencji cyfrowych oraz trudności w identyfikowaniu realnych potrzeb szkoleniowych (Dernowska-Żaczyk, Smarzewska, 2024). Autorzy badań podkreślają, że nawet dobrze zaprojektowane programy edukacyjne nie przynoszą oczekiwanych rezultatów, jeśli nie towarzyszy im odpowiednia motywacja pracowników oraz spójna polityka organizacyjna.

Istotną rolę odgrywają również bariery o charakterze kulturowym i psychologicznym. Opór wobec zmian technologicznych, obawa przed popełnieniem błędu czy przekonanie o niskiej przydatności nowych umiejętności prowadzą do powierzchownego uczestnictwa w szkoleniach i braku trwałej zmiany zachowań (Dernowska-Żaczyk, Smarzewska, 2024). W efekcie kompetencje cyfrowe pozostają na poziomie deklaratywnym, nie przekładając się na realne praktyki bezpieczeństwa w środowisku pracy.

Urząd Marszałkowski Województwa Śląskiego (2025) w raporcie wymienia kilka barier rozwoju kompetencji cyfrowych:

- ograniczenia o charakterze finansowym, organizacyjnym oraz społecznym. Środki przeznaczane na projekty cyfryzacyjne często pozostają niewystarczające, co znacząco ogranicza zarówno skalę podejmowanych działań, jak i ich długofalową efektywność. Niedobory te utrudniają tworzenie stabilnych programów edukacyjnych oraz zapewnienie odpowiedniego zaplecza technicznego,
- nierównomierny dostęp do oferty edukacyjnej wynikający z asymetrycznego rozmieszczenia. Ośrodki szkoleniowe i instytucje wspierające rozwój kompetencji cyfrowych koncentrują się głównie w dużych miastach, co powoduje, że mieszkańcy mniejszych miejscowości oraz obszarów peryferyjnych mają znacznie ograniczone możliwości uczestnictwa w tego typu inicjatywach,
- nierównej dystrybucji zasobów, które obejmują zarówno deficyty materialne – tj. brak odpowiedniego sprzętu, dostępu do szybkiego Internetu czy czasu na korzystanie z nowych technologii – jak i ograniczenia w zasobach ludzkich, związane z niewystarczającą wiedzą techniczną i motywacją kadry. Istotne znaczenie mają także zasoby społeczne i kulturowe, w tym brak sieci wsparcia, utrudniony dostęp do wiedzy eksperckiej oraz niskie kompetencje w zakresie świadomego korzystania z usług cyfrowych (Batorski, Płoszej, Jasiewicz, Czerniawska, Peszat, 2012),
- bariery „twarde" (ograniczenia infrastrukturalne i finansowe) i „miękkie" (deficyty wiedzy i umiejętności, obawy psychologiczne, niską motywację do uczenia się, a także zjawisko autowykluczenia cyfrowego),
- możliwości instytucjonalne samorządów, które często nie dysponują wystarczającymi środkami ani narzędziami do inicjowania i koordynowania szeroko zakrojonych projektów cyfryzacyjnych. Ogranicza to ich rolę jako kluczowych aktorów w procesie podnoszenia kompetencji cyfrowych na poziomie regionalnym,
- niskie zainteresowanie części potencjalnych uczestników, zwłaszcza osób powyżej 50 roku życia, dla których udział w szkoleniach

zdalnych bywa mało atrakcyjny lub zbyt wymagający. Skutkuje to częstymi rezygnacjami i osłabieniem efektów programów edukacyjnych,
- niedobór odpowiednio przygotowanej kadry szkoleniowej oraz brak usystematyzowanej wiedzy o realnych potrzebach pracodawców. Informacje dotyczące zapotrzebowania na konkretne umiejętności cyfrowe są rozproszone, co utrudnia projektowanie adekwatnej oferty szkoleniowej.

Analiza barier rozwoju kompetencji cyfrowych pokazuje, że trudności te mają charakter wielowymiarowy i nie ograniczają się wyłącznie do kwestii technicznych. Ostatecznie to nie sama technologia, lecz człowiek decyduje o realnym poziomie bezpieczeństwa cyfrowego organizacji. Dopóki bariery w rozwoju kompetencji będą ograniczać wiedzę, nawyki i gotowość użytkowników do bezpiecznego działania, każda organizacja pozostanie podatna na zagrożenia. Przełamanie tych barier staje się więc nie dodatkiem do strategii cyberbezpieczeństwa, lecz jej warunkiem podstawowym.

Podsumowanie

Przeprowadzone w rozdziale rozważania potwierdzają, że cyberbezpieczeństwo organizacji nie jest wyłącznie funkcją zastosowanych technologii, lecz w dużej mierze zależy od kompetencji cyfrowych użytkowników. Współczesne środowisko pracy, oparte na komunikacji elektronicznej, usługach chmurowych i zdalnym dostępie do danych, powoduje, że użytkownik staje się integralnym elementem systemu bezpieczeństwa informacji, a jego działania mogą zarówno wzmacniać, jak i osłabiać poziom ochrony. Jak wskazuje Plebańska, kompetencje cyfrowe należy rozumieć jako połączenie wiedzy, umiejętności i postaw, które umożliwiają odpowiedzialne funkcjonowanie w społeczeństwie cyfrowym i bezpośrednio wpływają na sposób korzystania z technologii w organizacji (Plebańska, 2023).

Problem główny rozdziału został sformułowany następująco: w jakim stopniu kompetencje cyfrowe warunkują odporność organizacji na cyberataki? Przeprowadzone analizy pozwalają stwierdzić, że kompetencje cyfrowe w znacznym stopniu determinują odporność organizacji, ponieważ wpływają na zdolność użytkowników do rozpoznawania zagrożeń, stosowania procedur bezpieczeństwa oraz reagowania na incydenty. Człowiek jako

użytkownik systemów informatycznych, stanowi bowiem zarówno potencjalne źródło podatności, jak i element pierwszej linii obrony. Celem głównym rozdziału było określenie roli kompetencji cyfrowych użytkowników w budowaniu odporności organizacji na cyberataki. Cel ten został zrealizowany poprzez omówienie znaczenia kompetencji cyfrowych, mechanizmów ich rozwoju oraz barier utrudniających ich podnoszenie. Wykazano, że kompetencje cyfrowe obejmują nie tylko umiejętności techniczne, lecz także wiedzę, postawy oraz nawyki związane z bezpiecznym korzystaniem z technologii. Ich rozwój wymaga podejścia wieloetapowego, obejmującego edukację formalną, pozaformalną oraz samokształcenie.

W świetle przeprowadzonych rozważań można stwierdzić, że kompetencje cyfrowe użytkowników pełnią funkcję strategicznego zasobu organizacji, wpływając bezpośrednio na jej zdolność do zapobiegania, wykrywania oraz reagowania na incydenty cyberbezpieczeństwa. Organizacje, które inwestują w systematyczny rozwój kompetencji cyfrowych swoich pracowników, zwiększają swoją odporność na ataki, natomiast zaniedbania w tym obszarze prowadzą do wzrostu ryzyka operacyjnego i reputacyjnego.

Ostatecznie cyberbezpieczeństwo organizacji nie jest wyłącznie problemem technologicznym, lecz przede wszystkim problemem kompetencyjnym i organizacyjnym. To użytkownik, wyposażony w odpowiednią wiedzę, umiejętności i postawy, decyduje, czy technologia stanie się skutecznym narzędziem ochrony, czy jedynie pozorną barierą wobec zagrożeń. W tym sensie rozwój kompetencji cyfrowych należy uznać za jeden z kluczowych filarów budowania odporności organizacji w erze cyfrowej.

Literatura

1. Batorski, D., Płoszej, A., Jasiewicz, J., Czerniawska, D., Peszat, K. (2012). *Diagnoza i rekomendacje w obszarze kompetencji cyfrowych społeczeństwa i przeciwdziałania wykluczeniu cyfrowemu w kontekście zaprogramowania wsparcia w latach 2014-2020.* Warszawa: Ministerstwo Rozwoju Regionalnego.
2. Ćwiek, M., Maj-Serwatka, K. (2024). *Digital Competence of Young Adults in Poland*. Studia z Polityki Publicznej, 3(368), 46-68. https://doi.org/10.18778/0208-6018.368.03

3. Dernowska-Żaczyk, N., Smarzewska, D. (2024). *The Significance and Advancement of Digital Competencies in Human Capital Management*. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 69(2), 38-49. https://doi.org/10.15611/pn.2025.2.04
4. Digital Skills and Jobs Platform. (2020). *Poland Digital Competence Development Programme (2020–2030).* Pobrano z: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/poland-digital-competence-development-programme-2020-2030 (dostęp: 01.02.2026).
5. DigComp. (b.d.) *Europejskie ramy kompetencji cyfrowych – DigComp.* Pobrano z: https://www.digcomp.pl (dostęp: 01.02.2026).
6. European Training Foundation. (2018). *Digital Skills and Competence, and Digital and Online Learning.* Bruksela: European Training Foundation. Pobrano z: https://www.etf.europa.eu/sites/default/files/2018-10/DSC%20and%20DOL_0.pdf (dostęp: 01.02.2026).
7. European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity Skills Development in the EU.* Athens: European Union Agency for Cybersecurity (ENISA). Pobrano z: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (dostęp: 01.02.2026).
8. IBM Security, Ponemon Institute. (2024). *Cost of a Data Breach Report 2024.* Pobrano z: https://www.ibm.com/reports/data-breach (dostęp: 01.02.2026).
9. Kancelaria Prezesa Rady Ministrów. (2025). *Analiza bezpieczeństwa polskiego Internetu w 2024 roku.* Pobrano z: https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku (dostęp: 01.02.2026).
10. Khadka K. Barkat Ullah A. (2025) *Human factors in cybersecurity: an interdisciplinary review and framework proposal,* https://doi.org/10.1007/s10207-025-01032-0 (dostęp: 01.02.2026).
11. Komisja Europejska. (2025). Termin: *Umiejętności cyfrowe*. Pobrano z: https://digital-strategy.ec.europa.eu/pl/policies/digital-skills (dostęp: 01.02.2026).
12. Ministerstwo Cyfryzacji. (2022). Termin: *Czym jest cyfrowa higiena?* Pobrano z: https://www.gov.pl/web/cyfryzacja/czym-jest-cyfrowa-higiena (dostęp: 01.02.2026).

13. Ministerstwo Cyfryzacji. (2020). Termin: *Kompetencje cyfrowe.* Pobrano z: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe (dostęp: 01.02.2026).
14. Monitor Polski. (2023). *Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. 2023 poz. 318).* Pobrano z: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20230000318/O/M20230318.pdf (dostęp: 01.02.2026).
15. Nowa Era. (2024). *4K, czyli cztery najważniejsze kompetencje XXI wieku*. Pobrano z: https://www.nowaera.pl/4k-czyli-cztery-najwazniejsze-kompetencje-xxi-wieku (dostęp: 01.02.2026).
16. Pawłowska-Cyprysiak, K., Hildt-Ciupińska, K. (2024). *Kompetencje cyfrowe wymagane na współczesnym rynku pracy – perspektywa pracodawcy.* Media i Społeczeństwo, *20*(1), 257-273. https://doi.org/10.5604/01.3001.0054.6527
17. Plebańska, M. (2023). *Kompetencje cyfrowe i ich cyfrowy rozwój*. Warszawa: Wydawnictwo Difin.
18. Polska Agencja Rozwoju Przedsiębiorczości. (2024). *Rynek pracy, edukacja, kompetencje. Aktualne trendy i wyniki badań.* Pobrano z: https://serwis-uslugirozwojowe.parp.gov.pl/component/content/article/8663-3-raport-rynek-pracy-edukacja-kompetencje-aktualne-trendy-i-wyniki-badan (dostęp: 01.02.2026).
19. Ptaszek, G. (2019). *Edukacja medialna 3.0. Krytyczne rozumienie mediów cyfrowych w dobie Big Data i algorytmizacji*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
20. Rogacka, M. (2022). *Kompetencje cyfrowe w miejscu pracy – perspektywa pracowników i pracodawców*. e-mentor, *5*(97), 53-64. https://doi.org/10.15219/em97.1591
21. Siemieniecki, B. (red.). (2012). *Edukacja medialna w świecie ponowoczesnym*. Toruń: Wydaw. Naukowe UMK.
22. Stachowiak, B. (2012). *Problematyka bezpieczeństwa i zagrożenia jednostki w społeczeństwie informacyjnym – podstawy programowe i standardy kształcenia a wymagania rzeczywistości.* W: B. Siemieniecki (red.), Edukacja medialna w świecie ponowoczesnym, Toruń: Wydawnictwo Naukowe UMK.

23. UNESCO. (2021). *Reimagining Our Futures Together: A New Social Contract for Education.* Pobrano z: https://unesdoc.unesco.org/ark:/48223/pf0000379707 (dostęp: 01.02.2026).
24. Urząd Marszałkowski Województwa Śląskiego. (2025). *Badanie identyfikacji barier utrudniających rozwój kompetencji cyfrowych wraz z analizą wpływu wykorzystania technologii informacyjno-komunikacyjnych na rozwój tych kompetencji*. Katowice: Urząd Marszałkowski Województwa Śląskiego.
25. Vademecum Bezpieczeństwa Informacyjnego. (2020). Termin: *Kompetencje cyfrowe*, Pobrano z: https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/10/kompetencje-cyfrowe/ (dostęp: 01.02.2026).
26. Verizon. (2024). 2024 *Data Breach Investigations Report.* Pobrano z: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (dostęp: 01.02.2026).
27. Włodarczyk, J. (2020). Termin: *Human Firewall*. Pobrano z: https://cyberwiedza.pl/zs/human-firewall (dostęp: 01.02.2026).

Małgorzata Wilczyńska[1]
Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu

Justyna Wilczyńska-Baraniak[2]

https://doi.org/10.29316/9788368103359_5

AUDYT BEZPIECZEŃSTWA INFORMACJI

INFORMATION SECURITY AUDIT

Streszczenie

W dobie cyfrowej transformacji i rosnących zagrożeń w cyberprzestrzeni, bezpieczeństwo informacji stało się kluczowym aspektem funkcjonowania każdej organizacji. Bezpieczeństwo informacji jest kluczowym elementem strategii organizacji, wymagającym ciągłej uwagi, inwestycji i doskonalenia w obliczu zmieniającego się krajobrazu zagrożeń cybernetycznych. Skuteczne zarządzanie bezpieczeństwem informacji wymaga kompleksowego podejścia, łączącego technologię, procesy i ludzi. Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt to systematyczny, niezależny

[1] https://orcid.org/0000-0002-1969-3498, e-mail: malgorzata.wilczynska@pansjar.edu.pl
[2] https://orcid.org/0009-0005-3148-8197, e-mail: justaw@o2.pl

i udokumentowany proces uzyskiwania dowodów z audytu oraz ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt bezpieczeństwa informacji, to kompleksowa analiza systemów IT, procedur, polityk oraz zabezpieczeń w organizacji, mająca na celu ocenę poziomu ochrony danych i zgodności z obowiązującymi standardami. Nie jest to wyłącznie techniczne badanie infrastruktury – dobry audyt uwzględnia także czynnik ludzki, dokumentację i kulturę organizacyjną w zakresie bezpieczeństwa. Z jednej strony audyt bezpieczeństwa informacji daje odpowiedź na pytanie, czy organizacja spełnia obowiązki formalne, a z drugiej analizuje wymogi techniczne dotyczące systemów informatycznych, przy pomocy których informacje są przetwarzane. Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, jest wskazane, aby cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia. Regularne audyty pozwalają zidentyfikować ryzyka związane z utratą lub ujawnieniem danych oraz wdrożyć odpowiednie środki zapobiegawcze. Celem rozdziału jest przedstawienie roli audytu bezpieczeństwa informacji, procesu audytowania oraz wskazanie podstawowych zasad audytowania. Treści prezentowane w rozdziale opracowano z wykorzystaniem teoretycznych metod badawczych, wiodącą z nich była analiza krytyczna literatury przedmiotu, analiza kwerendy źródeł internetowych, jak również metoda analizy, syntezy, uogólnienia oraz wnioskowania.

Słowa kluczowe: bezpieczeństwo informacji, audyt, jakość audytu, proces audytowania

Abstract

In the era of digital transformation and growing threats in cyberspace, information security has become a key aspect of every organization's operations. Information security is a key element of an organization's strategy, requiring constant attention, investment, and improvement in the face of a changing cyber threat landscape. Effective information security management requires a comprehensive approach that combines technology, processes, and people. Information security is an extremely important issue in the context of any activity, which is why organizations should ensure not only security procedures and policies, but also systematic audits. An audit is a systematic, independent, and documented process of obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are met.

An information security audit is a comprehensive analysis of an organization's IT systems, procedures, policies, and security measures to assess the level of data protection and compliance with applicable standards. It is not just a technical examination of infrastructure – a good audit also takes into account the human factor, documentation, and organizational culture in terms of security. On the one hand, an information security audit answers the question of whether an organization meets its formal obligations, and on the other hand, it analyzes the technical requirements for the IT systems used to process information. Regular security audits are crucial for maintaining a high level of data and IT system protection, helping organizations counteract potential threats and respond to security incidents in an appropriate manner. Due to constantly changing regulations and increasing security expectations, as well as emerging threats, it is advisable to conduct regular audits and verify the security measures in place on an ongoing basis. Regular audits allow you to identify risks related to data loss or disclosure and implement appropriate preventive measures. The purpose of this chapter is to present the role of information security auditing, the auditing process, and to indicate the basic principles of auditing. The content presented in the chapter was developed using theoretical research methods, the leading one being a critical analysis of the literature on the subject, an analysis of online sources, as well as the methods of analysis, synthesis, generalization, and inference.

Keywords: information security, audit, audit quality, auditing process

Wstęp

W dobie cyfrowej transformacji i rosnących zagrożeń w cyberprzestrzeni, bezpieczeństwo informacji stało się kluczowym aspektem funkcjonowania każdej organizacji. Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa. Taki audyt wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekiem danych i cyberatakami. Na koniec prac przygotowywany jest raport, w którym wypisane są stwierdzone niezgodności, a także wskazówki, co zrobić, aby system bezpieczeństwa informacji był szczelny i odporny na zagrożenia (Klichowski, b.d.). Rolą

audytu jest weryfikacja poprawności stosowanych zabezpieczeń w odniesieniu do założonych wymagań. Sam audyt jest procesem, prowadzonym przez niezależną jednostkę, która gromadzi i ocenia materiały funkcjonujące w organizacji i bada je pod kątem zgodności z ustalonymi kryteriami np. przepisami prawa, normami czy politykami bezpieczeństwa (Borkowski, b.d.). Zapewnienie bezpieczeństwa informacji jest kwestią bardzo ważną nie tylko dla podmiotów publicznych, ale i mniejszych organizacji. Każda organizacja narażona jest na ataki z zewnątrz, które mogą narazić ją na utratę zaufania i ogromne straty finansowe. Dlatego też powinna mieć wprowadzone procedury i polityki bezpieczeństwa, które powinny być cyklicznie sprawdzane – tylko wtedy zyska pewność, że stosowane zabezpieczenia są poprawne i adekwatne do założonych wymagań. Jednym z najbardziej skutecznych narzędzi do takiej weryfikacji jest audyt bezpieczeństwa informacji. Skuteczne funkcjonowanie SZBI w organizacji wymaga prowadzenia audytów mających na celu weryfikację poprawności stosowanych zabezpieczeń w odniesieniu do założonych wymagań. Audyt bezpieczeństwa informacji sprawdza poziom bezpieczeństwa systemu zarządzania bezpieczeństwem informacji (SZBI). Warto wspomnieć, że międzynarodowym standardem systemu zarządzania bezpieczeństwem informacji jest ISO/IEC 27001. Norma ta nie tylko określa wymagania i zasady inicjowania, wdrażania, utrzymywania i poprawy zarządzania bezpieczeństwem informacji, ale też najlepsze praktyki odnoszące się do stosowania zabezpieczeń (Klichowski, b.d.). Audyt jest procesem, w którym niezależna jednostka gromadzi i ocenia dowody o różnicach między wartością wskaźników mierzalnych a ustalonymi kryteriami. Organizacja powinna przeprowadzać wewnętrzne audyty SZBI w zaplanowanych odstępach czasu, aby określić, czy cele stosowania zabezpieczeń, same zabezpieczenia, procesy i procedury są:

- zgodne z zaleceniami standardów i odpowiednimi ustawami i przepisami,
- zgodne z zidentyfikowanymi wymaganiami bezpieczeństwa informacji
- skutecznie wdrożone i utrzymywane,
- adekwatne do zidentyfikowanych zagrożeń i poziomów ryzyka (należy uwzględnić nowe zagrożenia i nowe rodzaje ryzyka),
- zgodne z oczekiwaniami.

Z jednej strony audyt bezpieczeństwa informacji daje odpowiedź na pytanie, czy organizacja spełnia obowiązki formalne, a z drugiej analizuje wymogi techniczne dotyczące systemów informatycznych, przy pomocy których informacje są przetwarzane. Program audytu należy zaplanować, biorąc pod uwagę status i ważność procesów oraz ulokowanie obszarów wskazanych do audytu, jak również wyniki poprzednich audytów. Kryteria audytu, zakres, częstotliwość i metody powinny być zdefiniowane. Każdy audyt musi mieć wyznaczony cel (czyli co należy osiągnąć w następstwie audytu), kryteria (przepisy prawne, zarządzenia, procedury SZBI), zakres (obejmuje jednostki organizacyjne, fizyczne lokalizacje, procesy, działania) oraz termin wykonania. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa; wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekiem danych i cyberatakami. Działania audytorskie, a więc prowadzenie audytu bezpieczeństwa informacji, to systematyczny proces oceny i przeglądu procedur, polityk i systemów informatycznych organizacji w celu weryfikacji ich skuteczności i zgodności z normami i przepisami. Obejmuje on planowanie, zbieranie dowodów, analizę danych, a następnie przygotowanie raportu z rekomendacjami dotyczącymi poprawy poziomu bezpieczeństwa (raport, w którym wypisane są stwierdzone niezgodności, a także wskazówki, co zrobić, aby system bezpieczeństwa informacji był szczelny i odporny na zagrożenia). Przeprowadza się również spotkanie zamykające audytu, na którym przedstawiany jest raport wraz z rekomendacjami. Działania audytowe pomagają zidentyfikować luki w zabezpieczeniach, zapobiec cyberatakom i ochronić dane przed utratą, zapewniając tym samym ciągłość działania i minimalizując ryzyko strat finansowych. Audyt definiuje się jako systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów i ich obiektywnej oceny w celu określenia stopnia spełnienia założonych kryteriów. Wybór audytorów i sposób przeprowadzenia audytu powinny zapewnić obiektywność i bezstronność procesu audytowego. Audyt powinna wykonać jednostka zewnętrzna, aby zyskać gwarancję rzetelnej, bezstronnej i miarodajnej oceny. Audytorzy nie powinni audytować swojej własnej pracy. Audytor nie powinien także audytować obszaru, co do którego istnieje podejrzenie, że będzie miał trudności z zachowaniem obiektywizmu. Jest to ważne, bowiem celem audytora jest uzyskanie dowodów z audytu i wydanie obiektywnej oceny, która

pozwoli określić stopień spełnienia kryteriów. Celem audytorów jest szukanie zgodności, a nie poszukiwanie potknięć audytowanego. Audytorzy nie mogą kierować się negatywnymi emocjami wobec audytowanego. Audytorzy muszą pamiętać, że audyt nie jest kontrolą. Nie mogą zapominać, że audyty wewnętrzne podejmowane są dobrowolnie przez organizację i ich celem jest doskonalenie systemu. Audyt bezpieczeństwa może być realizowany zarówno przez osoby zatrudnione w weryfikowanej organizacji jak i za pomocą zewnętrznych specjalistów. Cechą audytu zewnętrznego jest niezależność oceny. Wprawdzie taki audyt można wykonać własnymi siłami (przez pracowników), ale zdecydowanie lepiej jest powierzyć to zadanie niezależnej i bezstronnej jednostce. Po pierwsze, gwarantuje to obiektywność audytu. Po drugie, instytucja audytująca ma niezbędne narzędzia oraz wiedzę o obowiązujących normach. Z kolei audyt wewnętrzny gwarantuje dobrą znajomość specyfiki organizacji i pozwala dokładnie analizować wybrane zabezpieczenia, ponieważ może być realizowany częściej niż audyt zewnętrzny. Aby dobrze wykonać zadanie audytorzy powinni rozumieć obszar audytowany i działalność audytowanego. Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Jest wiele miejsc, w których można wykonać audyt. Audyt to pojęcie spotykane względnie często, choć tak naprawdę nie ma jednoznacznej definicji. Dodatkowo często mylone jest z kontrolą lub błędnie nazywane „auditem". Kluczową trudnością w dokładnym ujęciu terminu „audyt" jest mnogość jego definicji. Co się z tym wiąże, nieraz pojawiają się nieścisłości w zakresie różnych jego klasyfikacji czy etapów przeprowadzania. Audyt – jedno z kluczowych wymagań systemów zarządzania opartych o normy ISO, którego celem jest ocena systemu, procesu, dostawcy. Audyt – zgodnie z definicją tego terminu – powinien być niezależnym, systematycznym procesem, którego celem jest ocena stopnia spełnienia określonych wymagań. Jeśli chodzi o oficjalne definicje, jedna z nich została zawarta w normie PN-EN ISO 19011:2018, która opisuje audytowanie systemów zarządzania, zasady jego przeprowadzania i zarządzania tego typu programami. Zgodnie z nią audyt to: „systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu obiektywnego oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów

audytu". Generalnie zatem uznaje się, że audyt to szczegółowe badanie (analiza działalności) wybranej jednostki, które wykonują odpowiednio do tego przygotowani audytorzy. Często jest to proces, który powtarza się regularnie i ma duże znaczenie dla kontrolowania sytuacji panującej w danej jednostce, jej postępowania względem zgodności z prawem, wskazywania jej mocnych oraz słabych stron czy tworzenia planów na przyszłość. Audyt wewnętrzny to niezależna, obiektywna ocena, która pomaga organizacji ocenić jej procesy, mechanizmy kontroli i systemy, aby zapewnić skuteczne zarządzanie wydajnością, ryzykiem i zgodnością z przepisami. Można go traktować jako sposób na utrzymanie wszystkiego pod kontrolą, aby organizacja realizowała swoje cele i unikała potencjalnych problemów operacyjnych (Highspring, 2025). Audyt ma być narzędziem wspomagającym a nie kontrolnym, przeszkadzającym i nic nie wnoszącym dla doskonalenia organizacji. Audyt polega na weryfikacji zgodności w oparciu o obiektywne dowody. Celem jest znalezienie dowodów zgodności a nie doszukiwania się niezgodności. Audyt nie ocenia ludzi, lecz funkcjonowanie systemu/procesu. Nie może się odbyć bez audytowanego (Akademia Jakości, b.d.). Audyt to systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt jest sprawdzeniem, czy wszystkie procedury w organizacji i posiadane dokumenty są zgodne z obowiązującym prawem i przyjętymi standardami bezpieczeństwa systemów. Ta kontrola jest połączona z analizą zarówno miejsca, jak i całego funkcjonującego systemu w miejscu audytowanym. Kompleksowy audyt bezpieczeństwa będzie wskazywać mocne i słabe strony organizacji. Wskaże również niezgodności – jeżeli występują. Z działań audytowych powstaje raport, którego analiza, a także wdrożenie zaleceń i działań poaudytowych da realną poprawę poziomu bezpieczeństwa. Należy też dodać, że każdy audyt powinien mieć jasno określone ramy czasowe, a jego sposób przeprowadzenia opierać się o bardzo konkretne procedury. Audyty bezpieczeństwa przeprowadza się m.in. w oparciu o normę ISO/IEC 27001, Ustawę o Krajowym Systemie Cyberbezpieczeństwa oraz Krajowe Ramy Interoperacyjności (Jurkiewicz, 2023). Jednostki publiczne mają obowiązek m.in.:

- przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (tzw. audytu KRI). Audyt KRI to kompleksowy proces weryfikacji zgodności systemów teleinformatycznych

i procesów organizacyjnych z wymaganiami Krajowych Ram Interoperacyjności,
- zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Można wnioskować, iż celem audytu jest dokładna i niezależna ocena danej organizacji, projektu, systemu, procesu, usługi czy nawet konkretnego produktu oraz wyszukanie wszelkich związanych z tym problemów. Ma to przynieść wiarygodne informacje, które w efekcie mają za zadanie pomóc w zarządzaniu określonym obszarem. Audyt zwykle ma zatem także charakter doradczy, czego finalnym celem jest wsparcie zarządzania organizacją i doprowadzenie do poprawy oraz usprawnienia działalności określonego podmiotu. Celem audytu jest potwierdzenie prawidłowego działania systemów bezpieczeństwa funkcjonujących w organizacji. Wszelkie raporty powstałe podczas audytu są przekazywane do osób upoważnionych oraz do instytucji państwowych, jeśli tak wymaga prawo. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, zaleca się cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia.

Bezpieczeństwo informacji w organizacji

W dzisiejszym cyfrowym świecie informacja stała się jednym z najcenniejszych zasobów każdej organizacji. Bezpieczeństwo informacji to kompleksowe podejście do ochrony danych, które wykracza daleko poza tradycyjne zabezpieczenia techniczne. Obejmuje ono całokształt działań organizacyjnych, prawnych i technicznych mających na celu zapewnienie ochrony informacji przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. Bezpieczeństwo informacji jest kluczowym aspektem ochrony danych osobowych i organizacyjnych przed nieautoryzowanym dostępem, ujawnieniem i naruszeniem. W obliczu rosnącej cyberprzestępczości i stale pojawiających się nowych zagrożeń, zarządzanie bezpieczeństwem informacji w każdej organizacji jest kluczowym elementem strategicznym i jednocześnie może wydawać się trudne lub wręcz niemożliwe. Zapewnienie bezpieczeństwa informacji

jest jednym z najważniejszych obszarów działania wszystkich organizacji oraz oddziaływania społecznego w rozwiniętych cywilizacyjnie i technologicznie krajach. Wraz ze wzrostem zagrożenia cyberatakami i coraz większym wykorzystaniem technologii cyfrowych, niezbędne stało się wdrożenie solidnych środków bezpieczeństwa informacji. Bezpieczeństwo informacji obejmuje różne strategie i procesy mające na celu ograniczanie ryzyka i ochronę poufnych informacji. Praktyczną cechą informacji jest to, że raz ujawniona niemal zawsze nie może już zostać powtórnie objęta ochroną, czyli pole zapewnienia ciągłości działania niemal nie istnieje. Działania podejmowane na rzecz ochrony i zarządzania bezpieczeństwem informacji powinny być kluczowe dla każdej organizacji a ich dobór powinien być proporcjonalny do zmieniającego się środowiska funkcjonowania podmiotu. W dzisiejszym świecie, gdzie informacje są kluczowym zasobem, bezpieczeństwo informacji ma ogromne znaczenie dla funkcjonowania organizacji, ochrony prywatności danych oraz utrzymania stabilności systemów informatycznych. W odniesieniu do opinii ekspertów, bezpieczeństwo wyraża się we wszystkich obszarach działalności organizacji. Jego struktura jest w istocie równoważna ze strukturą funkcjonowania podmiotu, zaś bezpieczeństwo informacyjne jest umiejscawiane, obok bezpieczeństwa publicznego, ekonomicznego i militarnego w ramach szerszych pojęć bezpieczeństwa międzynarodowego i narodowego (Koziej, 2011, s. 256). Bezpieczeństwo informacji (infosec) definiowane jest jako „stan i proces, w ramach którego zapewnia się w całym cyklu życia informacji (powstanie, przekazanie, przetworzenie, kopiowanie, wykorzystywanie, przechowywanie, gromadzenie, niszczenie), osiąganie i utrzymywanie z uwzględnieniem obowiązujących standardów bezpieczeństwa na pożądanym przez dany podmiot poziomie, takich jej fundamentalnych właściwości jak: dostępność, użyteczność, integralność i poufność" (Fehler, 2016, s. 30). Bezpieczeństwo informacji to kompleksowe podejście do ochrony danych i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. Jest to kluczowy element zarządzania ryzykiem informacyjnym w organizacjach, mający na celu zapewnienie poufności, integralności i dostępności informacji. Bezpieczeństwo informacji obejmuje zestaw zasad, procedur, narzędzi i praktyk mających na celu ochronę informacji w całym cyklu ich życia. Dotyczy to zarówno danych przechowywanych w formie elektronicznej, jak i papierowej. Celem

jest zapewnienie, że informacje są chronione przed różnymi zagrożeniami, zarówno wewnętrznymi, jak i zewnętrznymi (Widomski, 2026). Bezpieczeństwo informacji można także zdefiniować jako systematyczne podejście do zarządzania kluczowymi informacjami organizacji w celu zagwarantowania racjonalnego poziomu ich bezpieczeństwa. Obejmuje ono ludzi, procesy oraz technologię - obecnie nie można bowiem ograniczać się do bezpieczeństwa danych gromadzonych i przetwarzanych w systemach informatycznych. Bezpieczeństwo informacji jest kluczowym elementem strategii organizacji, wymagającym ciągłej uwagi, inwestycji i doskonalenia w obliczu zmieniającego się krajobrazu zagrożeń cybernetycznych. Skuteczne zarządzanie bezpieczeństwem informacji wymaga kompleksowego podejścia, łączącego technologię, procesy i ludzi. Obecnie stanowi ono złożony ekosystem, w którym równie istotne są aspekty technologiczne, jak i czynnik ludzki. Bezpieczeństwo informacji to nie tylko zabezpieczenia techniczne, ale również:

- aspekty organizacyjne: obejmują one polityki bezpieczeństwa, procedury, szkolenia pracowników i zarządzanie ryzykiem,
- aspekty prawne: zgodność z przepisami dotyczącymi ochrony danych, np. w Europie (Rada Europejska Rada Unii Europejskiej, 2024) obejmuje przede wszystkim Ochronę Danych Osobowych, regulowaną przez przepisy takie jak RODO (Urząd Ochrony Danych Osobowych, UODO (2022), które przyznają osobom fizycznym większą kontrolę nad ich danymi, narzucając na organizacje obowiązek bezpiecznego, transparentnego i zgodnego z prawem ich przetwarzania.

Obejmuje ono całokształt działań organizacyjnych, prawnych i technicznych mających na celu zapewnienie ochrony informacji przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. W praktyce oznacza to konieczność wdrożenia kompleksowych rozwiązań, które uwzględniają zarówno zabezpieczenia systemów informatycznych, jak i odpowiednie procedury organizacyjne oraz szkolenia pracowników.

W swojej istocie bezpieczeństwo informacji koncentruje się na zapewnieniu trzech kluczowych aspektów: poufności, integralności oraz dostępności informacji, które wspólnie tworzą tak zwaną triadę CIA (Confidentiality, Integrity, Availability). Jest to kluczowy element zarządzania ryzykiem

informacyjnym w organizacjach, mający na celu zapewnienie poufności, integralności i dostępności informacji. W praktyce bezpieczna informacja oznacza, że muszą być spełnione trzy zasadnicze atrybuty ochrony informacji (Syta, 2025, s. 41):

- poufność (ang. *Confidentiality*) – czyli zapewnienie, że informacje są dostępne tylko dla osób uprawnionych do ich dostępu. Systemy i użytkownicy muszą być weryfikowani, aby utrzymać poufność danych,
- integralność (ang. *Integrity*) – czyli zagwarantowanie dokładności i kompletności informacji, oraz metod ich przetwarzania; oznacza utrzymanie dokładności, spójności i nienaruszalności danych przez cały ich cykl życia. Informacje nie mogą być modyfikowane w sposób nieautoryzowany,
- dostępność (ang. *Availability*) – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami. Gwarantuje, że upoważnieni użytkownicy mają dostęp do potrzebnych informacji i zasobów w odpowiednim czasie (Malon Group, b.d).

Trzy koncepcje tj. poufność, integralność i dostępność stanowią fundament silnej ochrony informacji, tworząc podstawę infrastruktury zabezpieczeń organizacji. Dodatkowo, często uwzględnia się również takie własności jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Dodatkowe własności bezpieczeństwa informacji:

- autentyczność: weryfikuje tożsamość użytkowników i systemów, potwierdzając, że są oni tym, za kogo się podają; oznacza, że informacja pochodzi ze wskazanego źródła,
- niezaprzeczalność (ang. *Non-repudiation*): pozwala na udowodnienie, że określone działania lub zdarzenia miały miejsce, a użytkownik nie może zaprzeczyć swojej aktywności,
- rozliczalność (ang. *Accountability*): oznacza możliwość przypisania działań konkretnym podmiotom (osobom lub systemom), co pozwala na śledzenie ich aktywności,
- niezawodność (ang. *Reliability*): zapewnia, że systemy i dane działają w przewidywalny sposób, bez nieoczekiwanych awarii czy zakłóceń.

„Kluczowe zasady bezpieczeństwa informacji opierają się na modelu warstwowej ochrony, znanym jako „defense in depth". Pierwszą i fundamentalną zasadą jest zasada najmniejszych uprawnień, która zakłada, że każdy użytkownik powinien mieć dostęp tylko do tych zasobów, które są niezbędne do wykonywania jego obowiązków służbowych. Takie podejście znacząco redukuje ryzyko nieautoryzowanego dostępu do wrażliwych danych oraz minimalizuje potencjalne szkody w przypadku kompromitacji konta użytkownika. Druga istotna zasada dotyczy segmentacji i separacji obowiązków. W praktyce oznacza to, że krytyczne procesy powinny być podzielone między różne osoby lub działy, co zapobiega nadużyciom i błędom. Na przykład, osoba zatwierdzająca transakcje finansowe nie powinna być jednocześnie osobą je wykonującą. Taka separacja obowiązków stanowi skuteczny mechanizm kontrolny i redukuje ryzyko fraudów. Zasada głębokiej ochrony (defense in depth) stanowi trzeci filar bezpieczeństwa informacji. Zgodnie z nią, ochrona zasobów informacyjnych powinna być realizowana na wielu poziomach, począwszy od zabezpieczeń fizycznych, poprzez kontrole dostępu logicznego, aż po monitoring i audyt. Każda warstwa bezpieczeństwa powinna być niezależna od pozostałych, dzięki czemu przełamanie jednej z nich nie prowadzi automatycznie do kompromitacji całego systemu" (Godula, 2026).

Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa; wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekiem danych i cyberatakami. Działania audytorskie, a więc prowadzenie audytu bezpieczeństwa informacji, to systematyczny proces oceny i przeglądu procedur, polityk i systemów informatycznych organizacji w celu weryfikacji ich skuteczności i zgodności z normami i przepisami.

Rodzaje audytów bezpieczeństwa

Utrzymanie wysokich standardów funkcjonowania organizacji jest kluczowe dla osiągnięcia sukcesu. Jednym z najważniejszych narzędzi wspierających ten proces jest audyt – systematyczne badanie i analiza

działań organizacji, mające na celu identyfikację obszarów wymagających poprawy oraz wdrażanie skutecznych działań korygujących. Audyty, zarówno wewnętrzne, jak i operacyjne, odgrywają istotną rolę w zarządzaniu ryzykiem, zapewnieniu zgodności z przepisami wewnętrznymi organizacji i obowiązującymi standardami (Hotiuk, 2024). Audyt bazuje na specyficznych działaniach, które mają na celu ocenić dany system, proces, projekt lub organizację. Przebieg audytu determinuje również jego rodzaj. Rodzaje audytów różnią się zakresem i celem, jednak każde badanie ma na celu analizę procesów oraz zapewnienie działań wspierających poprawę funkcjonowania organizacji w praktyce. Jak już wspomniano we wstępie audyty dzielą się na wewnętrzne (pierwszej strony) i zewnętrzne (drugiej i trzeciej strony). Zasadnicza różnica między nimi polega przede wszystkim na podmiocie, który je przeprowadza, a także celowi stojącemu za tymi działaniami. Jeśli chodzi o przedmiot audytu, jest on badany w odniesieniu do konkretnych standardów, przepisów prawnych, wzorców i norm. Jednym z kryteriów podziału audytów jest podmiot, który je przeprowadza. W tym zakresie wyróżnia się trzy podstawowe sposoby audytowania: audyt pierwszej strony (wewnętrzny), audyt drugiej strony oraz audyt trzeciej strony (z czego ostatni z opisanych poniżej – tj. audyt trzeciej strony – jest zdecydowanie najrzadszy). Przebieg audytu determinuje również jego rodzaj. Każdy z nich jest inny i ma określony własny cel. Jak już wspomniano wcześniej, audyty dzielą się na wewnętrzne (pierwszej strony) i zewnętrzne (drugiej i trzeciej strony). Zasadnicza różnica między nimi polega przede wszystkim na podmiocie, który je przeprowadza, a także celowi stojącemu za tymi działaniami.

Tabela 1. Rodzaje audytów bezpieczeństwa

Audyt pierwszej strony (audyt wewnętrzny)	Audyt wewnętrzny jest jednym z najlepszych narzędzi służących do ciągłego doskonalenia organizacji. Jest audytem wewnętrznym i jest prowadzony przez samą organizację lub w jej imieniu. Podczas tych działań ocenia się wdrożony system pod kątem prawidłowości i poprawności działania w chwili kontroli. Zgodnie z przyjętą zasadą, audytorzy nie mogą audytować obszarów, za które są odpowiedzialni. Audyt wewnętrzny jest audytem cyklicznym obejmującym określony obszar lub całą organizację.
Audyt drugiej strony (audyt zewnętrzny)	Audyt koncentruje się na badaniu systemu zarządzania przez klienta lub zainteresowaną instytucję. Takie audyty są już wykonywane przez certyfikowanych audytorów bezpieczeństwa, którzy mogą być zarówno wewnątrz organizacji, a także z zewnątrz. Przeprowadzenie takiego audytu musi być poparte pisemnym porozumieniem, np. umową.
Audyt trzeciej strony (audyt zewnętrzny)	Audyt jest przeprowadzany dla celów certyfikacji lub akredytacji, jak również dla celów prawnych i regulacyjnych. Audyty te są przeprowadzane przez niezależne organizacje audytorskie, które weryfikują poprawność funkcjonowania systemów do istniejących przepisów.
Audyt połączony (zintegrowany)	Audyt przeprowadzany wspólnie u jednego audytowanego w kontekście dwóch lub więcej systemów zarządzania.
Audyt wspólny	Audyt przeprowadzany u jednego audytowanego przez dwie lub więcej organizacji audytorskich.

Źródło: Jurkiewicz P. (2023). *Jak audyt bezpieczeństwa wygląda w praktyce?* Pobrano z: https://www.doering-partnerzy.pl/jak-audyt-bezpieczenstwa-wyglada--w-praktyce/ (dostęp: 20.09.2025).

Audyt wewnętrzny (określany audytem pierwszej strony lub audyt wewnętrzny procesu) – w większości międzynarodowych standardów, w tym w normach z rodziny ISO, audyty wewnętrzne traktowane są jako ważna część procesu ciągłego doskonalenia organizacji, ponieważ umożliwiają one monitorowanie i przeglądanie wydajności procesów. Audyty wewnętrzne dają organizacji możliwość zidentyfikowania potencjalnego ryzyka i luk w systemie oraz zaprojektowania działań naprawczych, zanim zaczną generować poważne koszty dla organizacji. Pomagają również śledzić i dokumentować ewentualne zmiany. Dostarcza wiedzę czy wszystko działa zgodnie z założeniami. Najczęściej przeprowadzany jest przez osoby

na stałe zatrudnione w danym podmiocie – funkcjonują w ramach jej struktury, choć jednocześnie zachowują odpowiednią niezależność organizacyjną. Rzadziej są to audytorzy, którym zleca się tego typu czynność np. na podstawie umowy zlecania. Jak wskazuje definicja stworzona przez The Institute of Internal Auditors (IIA – Instytut Audytorów Wewnętrznych), to niezależna, obiektywna działalność o charakterze doradczym, prowadzona w celu wniesienia do organizacji wartości dodanej i usprawnienia jej funkcjonowania. Zgodnie z definicją Instytutu Audytorów Wewnętrznych (IIA), audyt wewnętrzny (Instytut Audytorów Wewnętrznych IIA Polska, b.d). jest działalnością niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega on na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów zarządzania ryzykiem, kontroli i ładu organizacyjnego, przyczyniając się do poprawy ich działania. Audyt wewnętrzny stanowi kluczowy element systemu kontroli wewnętrznej organizacji, dostarczając kierownictwu cennych informacji i rekomendacji. Generalnie pełni zatem rolę przede wszystkim wspierającą – ma ułatwiać realizowanie celów danej organizacji, podwyższać efektywność działania zatrudnionych w niej osób, ułatwiać wykonywanie ich obowiązków, identyfikować ewentualne ryzyka i dawać wskazówki w zakresie przygotowania odpowiednich procesów zarządzania ryzykiem i wskazywać możliwe sposoby ich minimalizowania itp. Co więcej, audyt wewnętrzny został zdefiniowany także w Dziale VI. ustawy o finansach publicznych i dotyczy audytowania oraz koordynacji owych audytów w jednostkach sektora finansów publicznych. Art. 272 wskazuje, że: „Audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze". Istnienie odpowiednich komórek audytu wewnętrznego jest w tym przypadku obowiązkowe, co ma ogromne znaczenie dla ochrony interesów społecznych. Audyt wewnętrzny dostarcza wiedzę z pierwszej ręki wewnątrz czy wszystko działa zgodnie z założeniami. Często bywa tak, że oceny wyników audytu interpretowana jest jak wyrocznia. Zgodnie z założeniami audyt wewnętrzny ma służyć jako narzędzie wspomagające proces rozwoju organizacji wg wewnętrznych zasad zarządzania panujących w organizacji (Lean Partner, b.d.). Podstawą audytu jest weryfikacja systemu zarządzania, nie ocena pracy ludzi i doszukiwanie się niezgodności. Audyt

wewnętrzny przynosi organizacji wiele korzyści. Przede wszystkim przyczynia się do poprawy efektywności i skuteczności operacji poprzez identyfikację obszarów wymagających usprawnień. Wzmacnia system kontroli wewnętrznej, co pomaga w minimalizacji ryzyka błędów i nadużyć. Audyt wewnętrzny wspiera również lepsze zarządzanie ryzykiem, pomagając organizacji w identyfikacji i ocenie potencjalnych zagrożeń. Ponadto, audyt wewnętrzny przyczynia się do zwiększenia zgodności z przepisami i regulacjami, co jest szczególnie istotne w dzisiejszym złożonym środowisku prawnym. Wspiera osiąganie celów strategicznych organizacji poprzez dostarczanie informacji niezbędnych do podejmowania decyzji. Wreszcie, audyt wewnętrzny dostarcza obiektywnych informacji zarządowi i kierownictwu, co pomaga w podejmowaniu świadomych decyzji strategicznych (EITT, b.d.). Audyt wewnętrzny jest cennym narzędziem wspierającym organizację w osiąganiu jej celów i poprawie efektywności działania. Poprzez systematyczną ocenę procesów i dostarczanie obiektywnych informacji, audyt wewnętrzny przyczynia się do tworzenia wartości dodanej i usprawnienia działalności operacyjnej organizacji.

Audyt zewnętrzny to niezależna ocena, przeprowadzana przez podmiot niebędący częścią audytowanej organizacji. Audyt zewnętrzny przeprowadzany jest przez niezależnych ekspertów, niemających bezpośredniego związku z organizacją. Audyt zewnętrzny może zostać przeprowadzony zarówno przez drugą, jak i trzecią stronę. Organizacja nie korzysta wówczas z własnych zasobów, ale musi zaangażować niezależnych ekspertów, gwarantujących bezstronną i obiektywną perspektywę. W obu przypadkach cel stanowi przede wszystkim ocena skuteczności systemu zarządzania oraz potwierdzenie zgodności z wymaganiami danej normy ISO. Audyt zewnętrzny - przeprowadzają go podmioty niezależne od danej organizacji, inaczej określany audytem drugiej strony. Osoba audytująca musi jednak posiadać niezbędne do tego kompetencje i być uprawnionym audytorem (wewnętrznym lub zewnętrznym). Najczęściej są to wyspecjalizowane firmy konsultingowe lub audytorskie, które zatrudniają audytorów i rewidentów w pełni przygotowanych do auditingu (posiadających odpowiednie uprawnienia). W tym przypadku kluczowa jest ocena funkcjonowania wybranych jednostek pod względem finansowym, w przeciwieństwie do audytu wewnętrznego, który często obejmuje także obszary niefinansowe.

Audyt trzeciej strony – to szczególna forma audytu zewnętrznego (audyt certyfikacyjny). Audytorzy są bowiem zupełnie niezależni od podmiotu, który analizują. Są to np. jednostki certyfikujące (jeżeli dany podmiot chce uzyskać akredytowany certyfikat ISO, poddawanie się tego typu audytom jest obowiązkowe).

Dążenie do ciągłego doskonalenia organizacji pracy i funkcjonowania organizacji stanowi kluczowy element rozwoju. Należy pamiętać, że wdrożenie systemu zarządzania ISO to jeden z etapów złożonego procesu. Aby podjęte działania były zgodne z wymaganiami danej normy ISO, konieczne jest regularne przeprowadzanie audytów. Każdy audyt, zarówno pierwszej, drugiej, jak i trzeciej strony może przynieść organizacji wiele korzyści. Audyt wewnętrzny pozwala na dalsze doskonalenie wdrożonego systemu zarządzania poprzez identyfikację obszarów wymagających poprawy w celu podniesienia efektywności i standardów w danej organizacji. Przeprowadzenie audytów zewnętrznych, zarówno drugiej, jak i trzeciej strony pomaga w skutecznym budowaniu profesjonalnego i wiarygodnego wizerunku (CeCert, 2024). Zasadniczo mówimy o trzech rodzajach audytów: audyt pierwszej strony (audyt wewnętrzny), audyt drugiej strony (audyt klienta u dostawcy) i audyt trzeciej strony (audyt wykonywany przez niezależną organizację, np. audyt jednostki certyfikacyjnej). Wszystkie ww. typy audytów mają elementy wspólne, ale też się różnią, ponieważ pełnią nieco inne role w systemie.

Tabela 2. Różnice między audytami pierwszej, drugiej i trzeciej strony

Proces audytu	Audyt pierwszej strony	Audyt drugiej strony	Audyt trzeciej strony
Cel audytu	Ocena stopnia spełnienia wymagań danej normy i wymagań własnych organizacji oraz skuteczności systemu.	Ocena stopnia spełnienia wymagań przez dostawcę.	Ocena stopnia spełniania wymagań danej normy w odniesieniu do zakresu i kryteriów jego certyfikacji, nadzoru lub recertyfikacji.
Zakres audytu	Konkretny obszar lub proces w zakresie systemu.	Procesy, działania, usługi realizowane przez zewnętrznego dostawcę.	Udokumentowany zakres systemu zarządzania w stosunku do wymogów danej normy.

Proces audytu	Audyt pierwszej strony	Audyt drugiej strony	Audyt trzeciej strony
Kryteria	Punkty normy stanowiącej podstawę systemu, realizowane w danym obszarze/ procesie oraz konkretna dokumentacja wspierająca działania w obszarze lub proces	Dokument zawierający wymagania organizacji (np. umowa, specyfikacji, zamówień, zleceń, itp.) na podstawie których dostawca realizuje zlecony proces czy usługę	Norma, która stanowi podstawę danego systemu oraz dokumentacja systemu zarządzania
Długość trwania audytu	Jest ustalany przez audytora i zależy od stopnia skomplikowania procesu, jego znaczenia w systemie i poziomu ryzyk	Jest ustalany przez audytora i wynika z zakresu zleconych działań, procesów lub realizowanych usług	Jest wyliczany przez jednostkę certyfikującą na podstawie określonych kryteriów i zasadniczo jest nienegocjowalny
Kompetencje audytora	Ustala organizacja wg własnych kryteriów z uwzględnieniem wiedzy i umiejętności niezbędnych do prowadzenia audytu wewnątrz organizacji	Ustala organizacja wg własnych kryteriów z uwzględnieniem wiedzy i umiejętności niezbędnych do prowadzenia audytu u konkretnego dostawcy	Wynikają z normy ISO 17021 i innych dokumentów obowiązujących akredytowaną jednostkę certyfikacyjną

Źródło: opracowanie własne na podstawie Biarda, M. (2022), *Rola audytu w systemach zarządzania*. Pobrano z: https://jakoscbezretuszu.pl/rola-audytu-w-systemach-zarzadzania/ (dostęp: 12.02.2026).

Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Audyt powinna wykonać jednostka zewnętrzna, aby zyskać gwarancję rzetelnej, bezstronnej i miarodajnej oceny. Audyty z reguły powinny być przeprowadzane przez osoby posiadające doświadczenie i kompetencje poparte stosowanymi certyfikatami. Audyt wykonują specjalnie przygotowani do tego audytorzy, którzy w swoim działaniu m.in. muszą kierować się zasadami: rzetelności, uczciwości, zgodności z etyką, należytej staranności, niezależności, poufności i wnioskowaniu w oparciu o konkretne dowody.

Jakość audytu bezpieczeństwa informacji

Jakość audytu bezpieczeństwa informacji (np. wg ISO/IEC 27001) jest bezpośrednio i nierozerwalnie związana z kompetencjami, doświadczeniem oraz postawą audytora. Audytor jest ekspertem, którego rzetelność i umiejętności definiują wartość dodaną dla organizacji. Audytor bezpieczeństwa informacji to specjalista przeprowadzający systematyczne oceny systemów, procesów i procedur organizacji w celu identyfikacji zagrożeń, luk w zabezpieczeniach i niezgodności, zapewniając ochronę danych i ciągłość działania, często w oparciu o normy takie jak ISO/IEC 27001. Jego rola polega na weryfikacji infrastruktury IT, procedur, polityk i kompetencji personelu, a następnie rekomendowaniu działań naprawczych i usprawnień, co pomaga spełniać wymogi prawne, budować zaufanie i minimalizować ryzyko. Audytor bezpieczeństwa informacji to osoba, która posiada odpowiednie kwalifikacje i doświadczenie do przeprowadzania audytów systemów zarządzania bezpieczeństwem informacji. Audytor ocenia, czy organizacja skutecznie chroni swoje dane oraz czy spełnia wymagania określone przez międzynarodowe standardy, takie jak ISO/IEC 27001. Jego zadaniem jest również identyfikacja luk w zabezpieczeniach oraz rekomendowanie działań mających na celu ich eliminację. Jeśli chodzi o audytorów wewnętrznych systemów zarządzania, szczególnie podkreśla się konieczność znajomości przez nich struktury i wymagań wynikających z normy ISO 9001, zaś audytorzy systemu zarządzania bezpieczeństwem informacji – normy ISO/IEC 27001. Do przeprowadzania audytów przygotowują przede wszystkim odpowiednie szkolenia, które prowadzone są przez certyfikowane jednostki, działające na podstawie przyjętych standardów zawodowych.

Rola audytora bezpieczeństwa informacji obejmuje szereg kluczowych obowiązków. Audytor jest odpowiedzialny za planowanie i przeprowadzanie audytów bezpieczeństwa, co obejmuje analizę systemów informacyjnych, ocenę procedur bezpieczeństwa oraz identyfikację potencjalnych zagrożeń. Audytor musi również dokumentować wyniki audytu i przedstawiać je kierownictwu organizacji, dostarczając rekomendacje dotyczące usprawnień. Jego obowiązki obejmują także monitorowanie wdrażania zaleceń oraz zapewnienie, że organizacja spełnia wszystkie wymagania regulacyjne i normatywne.

Audytor bezpieczeństwa informacji odgrywa kluczową rolę w systemie zarządzania bezpieczeństwem informacji. Jego praca pomaga

organizacjom w identyfikacji i eliminacji słabości w systemach zabezpieczeń, co jest niezbędne do ochrony danych i zgodności z regulacjami prawnymi. Audytor dostarcza kierownictwu obiektywnych informacji na temat stanu bezpieczeństwa informacji, co pozwala na podejmowanie świadomych decyzji strategicznych. Dzięki jego rekomendacjom organizacje mogą poprawić swoje procedury bezpieczeństwa i zminimalizować ryzyko związane z zagrożeniami cybernetycznymi.

Przewagą organizacji, w strukturach której funkcjonuje audytor wewnętrzny, jest możliwość nieustannego kontrolowania zachodzących procesów. W pewnym sensie audyt trwa tam przez cały rok, dzięki czemu daje też szanse na szybkie zauważenie pojawiających się trudności i równie szybkie im zaradzenia. Co ważne, specjaliści kierują się w trakcie audytowania przepisami prawa, zarówno krajowego, jak i międzynarodowego (np. Unii Europejskiej), przepisami wewnętrznymi organizacji, określonymi standardami, listami kontrolnymi czy normami. Audytor powinien mieć wiedzę o procesach występujących w organizacji, procedurach obowiązujących w organizacji, a dodatkowo wiedzę specjalistyczną np. z zakresu IT, bezpieczeństwa informacji, stosowanych zabezpieczeniach i pojawiających się zagrożeń. Powinien znać również podstawowe wymagania prawne z danego obszaru. W zależności od wymagań audyt przeprowadzany jest przez jednego audytora lub grupę audytorów. Jeżeli audyt przeprowadzany jest przez zespół audytorów, w takim przypadku należy wskazać audytora wiodącego. Jest to osoba prowadząca audyt, na którym oparta jest cała odpowiedzialność za prawidłowe przeprowadzenia tego procesu. To on m.in. określa plan audytu, wytycza zakres czynności audytu w danej organizacji, a na koniec tworzy raport z audytu. Jeżeli przeprowadzamy audyt bezpieczeństwa informacji dobrze jest, aby w zespole byli również choć jeden audytor IT (Jurkiewicz, 2023). Audyt jest tak dobry, jak doświadczenie i wiedza członków zespołu audytorskiego; dlatego, aby audyt przebiegł pomyślnie, członkowie zespołu audytorskiego powinni być starannie wybierani i odpowiednio przeszkoleni. Cechy audytora wewnętrznego zostały określone między innymi w normie ISO 19011. Zawiera ona wytyczne dotyczące cech osobowości, charakterystycznych dla tego zawodu (Przybylska, Rydzak, Trębecki, 2021, s.16). Katalog przymiotów audytorskich wg ISO 19011 obejmuje bycie (Global Cert, 2023):

- Profesjonalizm: Audytor będzie posiadał cechy osobiste, takie jak wiarygodność, uczciwość i rzetelność, i będzie dostarczał rzetelnych informacji i wyników dotyczących jednostki, którą audytuje. Ponadto osoba ta podejmuje się działań audytowych tylko, gdy ma do tego kompetencje i pozostaje bezstronnym,
- Otwartość: Audytor będzie chętny słuchać, uczyć się i akceptować nowe pomysły oraz odzwierciedlać je w sytuacjach lub wymaganiach. Czasami audytor może napotkać nowe podejścia lub opinie. Audytor, pozostając obiektywnym musi mieć zdolność oceny i akceptacji różnych punktów widzenia, o ile spełniają one wymagania,
- Dyplomatyczność: Audytor będzie uprzejmy i świadomy swojej roli; audytor pełni funkcję reprezentacyjną, a więc przedstawiciela danej organizacji,
- Obserwator: Audytor będzie miał zdolność rozpoznawania i oceniania tego, co widzi, oraz rozumienia i interpretowania zdarzeń bez głębokiego przesłuchania,
- Perspektywa: Audytor będzie miał zdolność oceny sytuacji wykraczających poza wygląd osoby, z systematycznym poglądem na rzeczy i będzie miał zdolność zrozumienia konsekwencji organizacyjnych dowodów, które znajdzie,
- Wszechstronność: Audytor będzie miał zdolność do mobilizacji z jednej sytuacji do drugiej bez utraty kierunku. W jednej chwili audytor może audytować jedno pole; w następnej może to być inne. Audytor musi być w stanie pozostać skupionym,
- Wytrwałość: Audytor musi być wytrwały w swoich celach, tak, aby gdy zada pytanie, musiał otrzymać na nie odpowiedź i nie był rozpraszany przez zakłócenia lub zakłócenia. Zaleca się, aby dowód z audytu był weryfikowalny, dlatego próba uzyskania jak największej ilości informacji i dowodów jest jedynym słusznym podejściem,
- Niezależność: Audytor musi mieć własne zdanie na różne tematy, nie będzie pod wpływem otoczenia i będzie wolny od konfliktu interesów. Zaleca się, aby audytorzy byli niezależni od działań poddanych audytowi (w ramach możliwości),

- Decyzyjność: Audytor musi być gotowy podejmować decyzje, nawet jeśli są trudne lub nie zadowolą audytowanego,
- Poufność: Zaleca się, aby audytorzy wykazywali się dyskrecją w użyciu i ochronie informacji, do których otrzymują dostęp w wyniku wykonywania swoich obowiązków. Informacje audytowe nie mogą być wykorzystywane dla osobistych korzyści przez audytora lub klienta audytu.

Zakres umiejętności wymaganych od liderów audytu wewnętrznego stale się poszerza. Muszą oni posiadać kompetencje techniczne i strategiczne, aby móc współpracować z interesariuszami. Muszą być również skutecznymi liderami i strategami z dobrą znajomością organizacji. Audytorzy wewnętrzni odgrywają kluczową rolę w zapewnianiu właściwego ładu korporacyjnego, zarządzania ryzykiem i kontroli w organizacjach. Wraz z rozwojem funkcji audytu wewnętrznego, zmienia się również zakres umiejętności wymaganych od lidera audytu wewnętrznego. 10 najważniejszych cech wyróżniających wybitnych liderów audytu wewnętrznego (Highspring, 2025).

Wiarygodny: wybitni liderzy audytu wewnętrznego muszą być w stanie budować i utrzymywać wiarygodność na wysokim szczeblu w organizacji. Będą musieli konfrontować się z dyrektorami generalnymi i innymi interesariuszami najwyższego szczebla, co wymaga doskonałych umiejętności komunikacyjnych i umiejętności kwestionowania poglądów kadry kierowniczej wyższego szczebla. W tym celu muszą wykorzystywać dane do opracowania planu strategicznego, który jest zgodny z celami organizacji i zawiera konkretne kroki prowadzące do osiągnięcia sukcesu. Dobrze sporządzone raporty z audytu pomagają umocnić wiarygodność audytora wewnętrznego, gwarantując, że jego ustalenia i zalecenia będą traktowane poważnie i wdrażane przez kadrę kierowniczą wyższego szczebla.

Godny zaufania: budowanie zaufania jest kluczowe dla liderów audytu wewnętrznego, którzy muszą być w stanie budować i utrzymywać zaufanie interesariuszy na wszystkich szczeblach, w tym kierownictwa, pracowników i interesariuszy zewnętrznych. Dobry dyrektor audytu wewnętrznego potrafi angażować i wpływać na interesariuszy w całej organizacji, jednocześnie budując wysoki poziom zaufania i szacunku. Chociaż budowanie tych relacji może być czasochłonne, korzyści są niezaprzeczalne.

Ujmujący: wiarygodność i budowanie zaufania idą w parze, przyczyniając się do powstania trzeciej cechy, która staje się kluczowa dla liderów audytu wewnętrznego: zaangażowania interesariuszy. Budowanie relacji opartych na współpracy z interesariuszami jest koniecznością, a skuteczni audytorzy stosują skuteczną komunikację, aby ograniczyć opór w procesie audytu, promować lepsze zrozumienie wartości audytu wewnętrznego dla organizacji oraz przyspieszyć udostępnianie informacji w odpowiedzi na wnioski audytowe. W tym obszarze zbudowanie silnego zespołu audytu wewnętrznego może usprawnić współpracę z interesariuszami i zapewnić sprawny i efektywny proces audytu.

Technicznie uzdolniony: chociaż pracodawcy kładą większy nacisk na umiejętności miękkie, kompetencje techniczne pozostają fundamentalne dla kierowników stanowisk audytorskich. Kluczowi interesariusze oczekują najwyższego poziomu kompetencji technicznych w zakresie kontroli wewnętrznej, a wszyscy audytorzy wewnętrzni muszą znać szereg platform analityki danych, wykorzystując je do zwiększania wartości organizacji w ramach działań audytu wewnętrznego. Inne kwestie, takie jak audyty zgodności, różnią się w zależności od branży. Na przykład świadomość regulacyjna jest szczególnie ważna w sektorze usług finansowych i bankowości, dlatego kluczowe jest posiadanie inwentarza umiejętności i modelu talentów, który odpowiada ryzyku i potrzebom organizacji.

Strategiczny: chociaż audyt stanowi trzecią linię obrony, organizacje oczekują więcej od swoich obszarów ładu korporacyjnego, co często wiąże się z coraz bardziej aktywną odpowiedzialnością w myśleniu strategicznym. Liderzy audytu wewnętrznego muszą wdrażać i wykorzystywać nowe technologie, aby realizować swoje wytyczne strategiczne, proaktywnie rozwiązując potencjalne problemy, a nie tylko na nie reagując. Ten poziom planowania jest niezbędny nie tylko w przypadku audytów wewnętrznych, ale także zewnętrznych, aby pomóc organizacjom identyfikować ryzyka i odkrywać obszary wymagające poprawy.

Nastawiony na biznes: liderzy audytu wewnętrznego muszą posiadać dogłębną wiedzę na temat działalności operacyjnej organizacji, procesów sprawozdawczości finansowej oraz branży. Wybitni liderzy audytu wewnętrznego powinni również posiadać silną orientację biznesową i umieć wykorzystać swoją wiedzę do identyfikacji ryzyka i tworzenia skutecznych mechanizmów kontroli. Powinni rozpoznawać kluczowe elementy sukcesu

swojej organizacji, zwiększając wartość dodaną poprzez budowanie działu audytu wewnętrznego w oparciu o te zasady.

Zrównoważony: oprócz tradycyjnych umiejętności audytorskich, liderzy audytu wewnętrznego o specjalistycznych kompetencjach cieszą się dużym zainteresowaniem. Banki i instytucje finansowe chętnie zatrudniają audytorów posiadających specjalistyczną wiedzę regulacyjną w zakresie płynności, kredytów i zarządzania ryzykiem. Znajomość systemów rachunkowości finansowej i sprawozdawczości, przepisów o zamówieniach publicznych w sektorze obronnym oraz wymogów systemów zarządzania kosztami ma kluczowe znaczenie dla wszechstronnego audytora, a osoby posiadające taką wiedzę są bardzo poszukiwane. Specjalistyczne umiejętności audytu wewnętrznego, na przykład w zakresie bezpieczeństwa danych, są coraz bardziej cenione podczas przeprowadzania audytów finansowych w branżach o rygorystycznych wymogach regulacyjnych.

Innowacyjny: chociaż rodzaj wymaganych umiejętności przywódczych może się różnić w zależności od organizacji, skuteczne przywództwo wymaga złożonego, ewoluującego zestawu umiejętności. Najlepsi liderzy nieustannie poszukują nowych pomysłów i sposobów na zwiększenie efektywności poprzez innowacje. W rozwijaniu umiejętności przywódczych, ciągłe doskonalenie i ocena naprawdę się opłacają.

Zręczny: krajobraz audytu wewnętrznego nabiera tempa, a liderzy muszą być gotowi i zdolni do wprowadzania zmian w swoich rocznych planach audytu w obliczu nieoczekiwanych zmian warunków rynkowych. Szybkie myślenie i rozwiązywanie problemów to kluczowe umiejętności leżące u podstaw audytu wewnętrznego, a najlepsi specjaliści od rozwiązywania problemów będą wykorzystywać kreatywność i innowacyjność w rozwiązywaniu złożonych problemów. Cechy te są szczególnie ważne w audycie operacyjnym, gdzie nacisk kładzie się na ocenę efektywności wdrożonych procesów, polityk, procedur i systemów. Wraz z ciągłą ewolucją wymagań regulacyjnych, procesów i technologii, audytorzy muszą podchodzić do świadczenia usług audytorskich i doradczych z perspektywą, zachowując otwartość i gotowość do angażowania się w odpowiedni poziom ryzyka.

Wpływowy: kultura organizacji ma coraz większe znaczenie dla ładu korporacyjnego, a audyt wewnętrzny nie jest wyjątkiem. Liderzy audytu wewnętrznego stanowią kluczowy wzór do naśladowania w utrzymywaniu zespołów zarządzających na właściwym kursie. Zapewniając obiektywne

zapewnienie lub bezstronną ocenę, liderzy audytu wewnętrznego mogą wpływać na kulturę przejrzystości i ciągłego doskonalenia. Zamiast unikać zmian, najlepsi liderzy audytu wewnętrznego starają się je inspirować i tworzyć atmosferę, w której ludzie chętnie wdrażają innowacyjne pomysły.

Profesjonalni audytorzy, na których można polegać: jeśli interesariusze uznają liderów audytu wewnętrznego za wysoce skutecznych w tych cechach, wówczas lider audytu wewnętrznego, jako zaufany doradca, wnosi znaczącą wartość dodaną do organizacji. Liderzy audytu wewnętrznego budują zaufanie poprzez konsekwentną współpracę z interesariuszami na wszystkich szczeblach organizacji i transparentną komunikację. Skuteczna komunikacja jest jedną z pięciu najważniejszych kompetencji zawodowych wymaganych w środowisku audytorów wewnętrznych. Zapewniając obiektywne zapewnienie i przedstawiając jasne, uzasadnione rekomendacje, pokazują, że mają na uwadze dobro organizacji. Z czasem te działania budują wysoki poziom szacunku i zaufania, zwłaszcza wśród kadry kierowniczej wyższego szczebla, pomagając liderom audytu wewnętrznego wpływać na decyzje organizacji i wprowadzać pozytywne zmian. Skuteczni liderzy audytu wewnętrznego potrzebują połączenia wiedzy technicznej, myślenia strategicznego i silnych umiejętności przywódczych. Często wiąże się to z budowaniem wiarygodności, budowaniem zaufania i angażowaniem interesariuszy w całej organizacji poprzez skuteczne umiejętności komunikacyjne. Powinni również korzystać z nowych technologii, aby wyprzedzać potencjalne zagrożenia i szanse, dostarczać cennych spostrzeżeń i pomagać w kształtowaniu strategicznego kierunku organizacji (Highspring, 2025). Audytor rozumie sytuację w jakiej się znajduje, uwzględnia wszelkie niuanse, emanuje kulturą osobistą i pewnością. W praktyce audytor ma do czynienia z różnymi charakterami i postawami audytowanego. Musi zatem być przygotowany w różne scenariusze, zwłaszcza podczas rozmów, które są przecież jednym z najważniejszych źródeł zbierania informacji (Global Cert, 2023). Praca audytora bezpieczeństwa informacji wiąże się z wieloma wyzwaniami. Jednym z nich jest konieczność nadążania za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych, co wymaga ciągłego doskonalenia wiedzy i umiejętności. Audytorzy muszą również radzić sobie z złożonością systemów informatycznych oraz zapewniać, że ich oceny są obiektywne i niezależne. Najlepsze praktyki w pracy audytora obejmują regularne szkolenia i aktualizację wiedzy, stosowanie międzynarodowych

standardów i norm oraz efektywną komunikację z kierownictwem organizacji. Ważne jest również, aby audytorzy angażowali różne działy organizacji w proces audytu, co pozwala na uzyskanie pełniejszego obrazu stanu bezpieczeństwa. Dokumentowanie wyników audytu i monitorowanie wdrażania zaleceń to kluczowe elementy, które pomagają w zapewnieniu skuteczności działań audytowych i poprawie bezpieczeństwa informacji w organizacji (EITT, b.d.). Chambers i McDonald zwracają uwagę, że wraz z rozwojem audytu zmieniają się oczekiwania, co do kwalifikacji i kompetencji (zwanych atrybutami) audytorów. Umiejętności techniczne pozostają absolutnie niezbędne, ale same w sobie nie są już wystarczające. Skuteczny „audytor przyszłości", obok umiejętności technicznych musi posiadać szeroki zakres nietechnicznych atrybutów. Siedem najbardziej pożądanych atrybutów skutecznego audytora, zidentyfikowanych przez Chambersa i McDoalda to: umiejętność skutecznego komunikowania się, partnerstwo, umiejętność pracy zespołowej, globalny sposób myślenia, budowane relacji, ciągłe podnoszenie kwalifikacji, uczciwość (Przybylska i in., 2021, s. 19).

Audytor bezpieczeństwa informacji to specjalista odpowiedzialny za przeprowadzanie audytów mających na celu ocenę i zapewnienie skuteczności systemów zarządzania bezpieczeństwem informacji w organizacji. Jego rola jest kluczowa w identyfikacji potencjalnych zagrożeń, ocenie zgodności z normami oraz rekomendowaniu działań naprawczych. Audytor, który dobrze rozumie kontekst organizacji, podnosi jej cyberbezpieczeństwo. Wysoka jakość audytu skutkuje lepszym zarządzaniem ryzykiem, wyższą poufnością, integralnością i dostępnością informacji.

Podstawowe zasady audytowania

Audyt bezpieczeństwa informacji to systematyczna ocena systemów, procedur i praktyk organizacji w celu zidentyfikowania potencjalnych zagrożeń, luk w zabezpieczeniach oraz niezgodności z politykami i przepisami, aby zapewnić poufność, integralność i dostępność danych. Wynikiem audytu jest raport z rekomendacjami, a jego celem jest zwiększenie odporności organizacji na cyberataki i zapewnienie bezpieczeństwa danych, co jest kluczowe dla zgodności z prawem i utrzymania zaufania. Proces ten bada kilka kluczowych obszarów:

- Polityki i procedury: analiza dokumentacji organizacyjnej dotyczącej bezpieczeństwa informacji, w tym procedur zarządzania danymi, reagowania na incydenty i zasad postępowania z poufnymi informacjami,
- Infrastruktura techniczna: ocena zabezpieczeń systemów informatycznych, takich jak sieci, serwery, oprogramowanie antywirusowe, mechanizmy szyfrowania i metody uwierzytelniania, często z wykorzystaniem testów penetracyjnych,
- Praktyki pracowników: weryfikacja czy pracownicy stosują odpowiednie procedury, są świadomi zagrożeń i przestrzegają polityk bezpieczeństwa, a także ocena poziomu ich świadomości poprzez ewentualne szkolenia,
- Zgodność: sprawdzenie czy organizacja przestrzega obowiązujących przepisów prawa (np. RODO), norm branżowych (np. ISO/IEC 27001) oraz wytycznych organów nadzoru.

Podczas audytu bezpieczeństwa informacji sprawdzane są między innymi (Klichowski, b.d.):

- zgodność z obowiązującymi normami,
- bezpieczeństwo procesów związanych z przepływem informacji, infrastruktury i oprogramowania,
- bezpieczeństwo informacji w relacjach z dostawcami,
- bezpieczeństwo systemów informacyjnych,
- zarządzanie aktywami,
- zarządzanie ciągłością działania,
- kontrola dostępu,
- bezpieczeństwo komunikacji.

Częstotliwość audytu powinna być podyktowana charakterystyką działalności organizacji. Im jest ona bardziej ryzykowna i „wyeksponowana", tym badanie należy przeprowadzać częściej. Audyty bezpieczeństwa przeprowadza się zgodnie z oczekiwaniami i potrzebami organizacji, jak również wymaganiami prawnymi. Dobrą praktyką jest przeprowadzenie audytu bezpieczeństwa co najmniej raz do roku. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560), (Ministerstwo Cyfryzacji, b.d.) zobowiązuje operatorów usług kluczowych do

przeprowadzania audytów bezpieczeństwa systemów teleinformatycznych raz na dwa lata. Do realizacji audytu bezpieczeństwa zobowiązane są również podmioty publiczne i prywatne, które korzystają z dofinansowania, np. z programu NFZ czy z programu Cyberbezpieczny Samorząd. Audyty te mają za zadanie potwierdzenie czy otrzymane środku z dotacji zostały właściwie wykorzystane do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych. Każdy podmiot zarówno publiczny i prywatny powinien cyklicznie przeprowadzić audyt bezpieczeństwa informacji, często zwany również jako audyt cyberbezpieczeństwa.

Audytowanie charakteryzowane jest zgodnie z szeregiem zasad, dzięki którym proces ten staje się skutecznym i wiarygodnym narzędziem wspierającym polityki i środki nadzoru kierownictwa, dostarczając informacji na podstawie których organizacja może doskonalić swoje efekty działania. Aby zapewnić, że wnioski wynikające z przeprowadzonego audytu są właściwe i wystarczające audytorzy muszą przestrzegać pewnych warunków i zasad. Audytowanie powinno opierać się na siedmiu uniwersalnych zasadach. Rzetelność definiowana jako podstawa profesjonalizmu, która powinna gwarantować uczciwe, etyczne i nacechowane odpowiedzialnością podejście do czynności audytorskich. Obowiązek uczciwego przedstawiania wyników, czyli wymóg postępowania i obrazowania spraw zgodnie z prawdą. Należyta staranność, czyli pracowitość i rozsądek w audytowaniu. Poufność, czyli konieczność zapewnienia bezpieczeństwa informacji na każdym etapie procesu audytu. Niezależność audytora rozumiana jako podstawa bezstronności audytu oraz obiektywności wyciągniętych przez audytora wniosków. Podejście oparte na dowodach, które polega na racjonalnym, ich pozyskiwani a następnie analizie danych i obiektywnej ocenie w celu uzyskiwania wiarygodnych wniosków. Podejście oparte na ryzyku odnoszące się do konieczności uwzględniania ryzyk i szans związanych z planowaniem i realizacją audytu (Global Cert, 2025).

Tabela 3. Podstawowe zasady audytowania – 7 uniwersalnych zasad audytowania

Zasada 1	Rzetelność: podstawa profesjonalizmu	• wykonywanie swojej pracy uczciwie, sumiennie i odpowiedzialnie • stosowanie się do wszystkich mających zastosowanie „wymagań prawa", „zgodnie z prawdą". • wykazywanie się kompetencją podczas wykonywania swojej pracy • wykonywanie swojej pracy w sposób bezstronny tj. uczciwość i bez uprzedzeń • wyczulony na wszelkie wpływy, które mogą oddziaływać na dokonywane oceny podczas przeprowadzania audytu
Zasada 2	Uczciwe przedstawianie wyników: obowiązek przedstawiania spraw dokładnie i zgodnie z prawdą	• ustalenia z audytu, wnioski z audytu oraz raporty z audytu powinny odzwierciedlać działania audytowe dokładnie i zgodnie z prawdą Obiektywność w prezentacji wyników audytu jest kluczowa, ponieważ tylko wtedy organizacje mogą podejmować świadome decyzje dotyczące swoich systemów zarządzania. Rzetelne i oparte na dowodach przedstawienie wyników pozwala na pełne zrozumienie sytuacji i podjęcie działań naprawczych tam, gdzie to konieczne. Bezstronność to podstawa. • ustalenia z audytu, wnioski z audytu oraz raporty z audytu powinny odzwierciedlać działania audytowe dokładnie i zgodnie z prawd • odnotowywanie w raporcie znaczących przeszkód napotkanych podczas audytu • obowiązek przedstawiania spraw dokładnie i zgodnie z prawdą nierozstrzygniętych lub rozbieżnych opinii pomiędzy zespołem audytującym a audytowanym • komunikacja zgodna z prawdą, dokładna, obiektywna, na czas, zrozumiała i pełna
Zasada 3	Należyta staranność zawodowa: pracowitość i rozsądek w audytowaniu	• staranność odpowiednia do ważności zadań • zdolność do racjonalnego osądzania we wszystkich sytuacjach audytowych
Zasada 4	Poufność: bezpieczeństwo informacji	• dyskrecja w użyciu i ochronie informacji, do których mają dostęp w wyniku wykonywania swoich obowiązków • informacje audytowe nie mogą być wykorzystywane dla osobistych korzyści audytora, klienta audytu czy też w sposób szkodliwy dla uzasadnionych interesów audytowanego • poprawne obchodzenie się z wrażliwymi i poufnymi informacjami

Zasada 5	Niezależność: podstawa do bezstronności audytów i obiektywności wniosków audytowych	Niezależność audytorów to kolejna zasada, która ma ogromne znaczenie w procesie audytowania. Audytorzy muszą być bezstronni i niezależni od obszarów, które audytują, aby móc formułować obiektywne wnioski. Niezależność zapewnia, że audyty są przeprowadzane bez zewnętrznych wpływów, co jest niezbędne dla zachowania integralności całego procesu. Dzięki temu organizacje mogą być pewne, że wyniki audytu są wolne od uprzedzeń czy nacisków, co gwarantuje uczciwość całego procesu. • niezależni od działań podlegających audytowi, o ile jest to wykonalne • we wszystkich przypadkach powinni działać w sposób wolny od uprzedzeń i konfliktu interesów • w przypadku audytów wewnętrznych powinni być niezależni od audytowanej funkcji, jeżeli jest to wykonalne • powinni zachować obiektywność podczas całego procesu audytu, aby ustalenia i wnioski audytu były oparte wyłącznie na dowodach audytowych
Zasada 6	Podejście oparte na faktach: racjonalna metoda uzyskiwania wiarygodnych i powtarzalnych wniosków audytowych	Jedną z kluczowych zasad jest dowód z audytu. Bardzo ważne jest uzyskiwanie wiarygodnych i powtarzalnych dowodów, które stanowią podstawę do formułowania wniosków z audytu. Dowody te muszą być zbierane systematycznie i zgodnie z ustalonymi procedurami, co zapewnia, że wyniki audytu są solidne i mogą być wykorzystane do doskonalenia systemów zarządzania. Tylko na podstawie rzetelnych dowodów organizacje mogą podejmować działania, które rzeczywiście przyczynią się do poprawy ich funkcjonowania. Bez dowodów, audyt traci sens. • dowody audytowe powinny być weryfikowalne i oparte na próbkach dostępnych informacji (określony czas i ograniczone zasoby) • należy zastosować odpowiednie pobieranie próbek, ponieważ jest to ściśle związane z pewnością, którą można zawrzeć we wnioskach z audytu
Zasada 7	Podejście oparte na ryzyku: podejście audytu uwzględniające ryzyka i szanse związane z audytem	• istotny wpływ na planowanie, przeprowadzanie i raportowanie audytów • audyty koncentrują się na sprawach istotnych dla klienta audytu oraz na osiągnięciu celów programu audytów

Źródło: Global Cert (2025). Norma ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania. Pobrano z: https://certyfikacja-iso.pl/2025/01/17/norma-iso-19011-wytyczne-dotyczace-audytowania-systemow-zarzadzania/ (dostęp: 20.09.2025).

Przestrzeganie powyższych zasad jest kluczowe dla wiarygodności i skuteczności procesu audytowania, buduje zaufanie między audytorem a audytowanym oraz pozwala na podejmowanie trafnych decyzji. Audyty w organizacji przeprowadza się zgodnie z programem audytów. Program audytów stanowi jeden lub wiele audytów zaplanowanych w określonych ramach czasowych i mających określony cel.

Proces audytowania – działania audytorskie

Audyt to proces wieloetapowy, który wymaga odpowiedniego przygotowania, starannego badania oraz szczegółowej analizy wyników. Każdy z tych etapów odgrywa kluczową rolę w identyfikacji obszarów wymagających działań korygujących oraz poprawie efektywności procesów w organizacji. Dzięki jasno określonemu przebiegowi audytu możliwe jest zapewnienie zgodności działań z przepisami wewnętrznymi organizacji i obowiązującymi standardami. Proces audytowania to usystematyzowane, niezależne badanie mające na celu ocenę zgodności działań i efektywności procesów w organizacji. Składa się z planowania, zbierania danych, analizy ryzyka, raportowania oraz działań następczych (korygujących). Kluczowe działania obejmują wywiady, przegląd dokumentacji, obserwację i audytowanie na miejscu. Prowadzenie audytu to proces niezależnej oceny systemu, procesu, produktu lub organizacji pod kątem zgodności z określonymi kryteriami, takimi jak standardy, przepisy prawa lub procedury wewnętrzne. Audytorzy zbierają dane poprzez wywiady, analizę dokumentów i obserwację, a następnie identyfikują obszary do poprawy i wydają zalecenia. Kluczowe zasady prowadzenia audytu to niezależność, obiektywizm i metodyczne zbieranie dowodów, a cały proces kończy się przygotowaniem raportu zawierającego wnioski i działania naprawcze. Przygotowanie do audytu to kluczowy etap, który obejmuje określenie przedmiotu audytu oraz zakresu badania. Podczas właściwego procesu audytu audytorzy zbierają dane poprzez wywiady z pracownikami, analizę dokumentacji oraz obserwację działań w praktyce. Badanie obejmuje kontrolę zgodności procesów z obowiązującymi procedurami i standardami oraz identyfikację wszelkich niezgodności lub obszarów wymagających poprawy. Audytorzy analizują dokumentację, takie jak przepisy wewnętrzne organizacji, procedury oraz wyniki wcześniejszych audytów. Celem przygotowania jest również identyfikacja potencjalnych

obszarów ryzyka i opracowanie planu działań, który pozwoli przeprowadzić audyt zgodnie z określonymi standardami i procedurami (Hotiuk, 2024). Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Plan audytu powinien obejmować:

- cele i zakres audytu,
- kryteria audytu i wszystkie dokumenty,
- daty i miejsca, gdzie czynności audytorskie mają być prowadzone,
- rozpoznanie organizacyjnych i funkcjonalnych jednostek oraz procesów,
- oczekiwany czas i trwanie czynności audytorskich na miejscu.
- Planując audyt należy wziąć pod uwagę następujące kwestie:
- skład zespołu audytowego i jego ogólne kompetencje,
- odpowiednie techniki pobierania próbek,
- możliwości poprawy skuteczności i wydajności działań audytowych,
- ryzyko związane z osiągnięciem celów audytowych wynikających z nieefektywnego zaplanowania audytu,
- ryzyko dla audytowanego będące wynikiem przeprowadzenia audytu i działań audytorów na jego terenie.

Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Plan audytu może obejmować:

- ustalenie kluczowego przedstawiciela audytowanego biorącego udział w audycie,
- język roboczy i sprawozdawczy audytu,
- określenie ról i obowiązków członków zespołu audytorskiego i innych towarzyszących osób,
- tematy raportów audytorskich, format i struktura, oczekiwana data wydania,
- ustalenia logistyczne (podróż, udogodnienia na miejscu, itd.).

Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Do planowania audytu powinno się przyjąć podejście oparte na ryzyku, w szczególności ryzyku nieosiągnięcia celów audytu. Planowanie audytu powinno brać pod uwagę ryzyko związane z działaniami audytowanymi w procesach audytowanego i stanowić podstawę porozumienia pomiędzy klientem audytu, audytowanym i zespołem audytowanym

w zakresie przeprowadzenia audytu. Należy mieć na uwadze, iż, skala i zawartość audytu mogą się różnić, na przykład między audytami początkowymi i kolejnymi, a także między audytami wewnętrznymi i zewnętrznymi. Planowanie audytu powinno być wystarczająco elastyczne, aby umożliwić zmiany, które mogą stać się konieczne w miarę postępu działań audytowych. Plan audytu powinien być przedstawiony audytowanemu (klientowi audytu) do zapoznania się i akceptacji.

Cele audytu: audyt polega na zbadaniu aktualnego stanu zabezpieczenia zasobów informacyjnych pod względem: poufności, integralności i dostępności, wskazaniu niezgodności oraz przygotowaniu rekomendacji związanych z wprowadzeniem mechanizmów służących do uzyskania bezpieczeństwa informacji, zgodnego z normą. W praktyce audyt bezpieczeństwa informacji w oparciu o normę ISO/IEC 27001 ma na celu określenie zgodności istniejącego systemu zarządzania bezpieczeństwem informacji (SZBI) z wymaganiami zawartymi w normie.

Kryteria audytu: audyt zawsze musi odnosić się do założonych kryteriów. Kryteria audytu są to wymagania jakie organizacja ma do spełnienia w zakresie bezpieczeństwa informacji. Kryteria audytu obejmują następujące wymagania:

- zobowiązania wynikające z zawartych umów,
- wymagania zawarte w przepisach prawa,
- dokumentacja systemowa,
- normy (ISO/IEC 27001).

Działania audytowe: audyt bezpieczeństwa informacji łączy kompleksowy przegląd procedur postępowania w przypadku ataku cybernetycznego w organizacji oraz ocenę polityki bezpieczeństwa, mającej na celu codzienną prewencję przed wyciekami danych oraz innymi skutkami cyberataków, a także przestrzeganiem bezpiecznych praktyk w ochronie systemów i danych. Właściwie przeprowadzony audyt powinien być zaplanowany i przeprowadzony w sposób bardzo przemyślany. Program audytu powinien zostać zaplanowany i uwzględniać wyniki poprzednich audytów. Częstotliwość i metody przeprowadzania audytu, przyjęte kryteria i zakres, którego on dotyczy, powinny być z góry ustalone. Wybór audytorów i sposób przeprowadzenia audytu powinny zapewnić obiektywność i bezstronność procesu. Audytorzy nie powinni prowadzić audytów dotyczących ich własnej pracy. Wymagania i odpowiedzialność za planowanie i przeprowadzanie

audytów w organizacji oraz za raportowanie ich wyników i utrzymywanie zapisów powinny zostać określone w udokumentowanej procedurze. Audytorzy powinni posiadać udokumentowane uprawnienia potwierdzające wiedzę, doświadczenie oraz umiejętności.

Proces audytu bezpieczeństwa informacji obejmuje kilka kluczowych etapów (Wójcik, 2017):

ETAP 1. Inicjowanie audytu – wyznaczenie zespołu audytującego.

W celu wyznaczenia zespołu audytowego potrzebne są określone działania, w tym:

1. Wyznaczenie audytorów oraz audytora wiodącego (kierownika zespołu) do danego audytu oraz sprawdzenie uprawnień, kompetencji i doświadczenia audytorów.
2. Określenie celów audytu, jego zakresu i kryteriów. Audyt ma sprawdzić zgodność stanu zastanego z wymaganym. Zgodność ta jest oceniana na podstawie przyjętych kryteriów oceny.
3. Określenie wykonalności audytu. Zaleca się określenie wykonalności audytu z uwzględnieniem takich czynników jak:
   - dostępność wystarczających i odpowiednich informacji,
   - możliwość potrzebnej współpracy z audytowanym,
   - adekwatny czas i zasoby (w tym dostępność osób i dostęp do obszarów audytowanych).
4. Nawiązanie pierwszego kontaktu z audytowanym. Pierwszy kontakt z audytowanym może być nieformalny lub formalny, ale zaleca się, żeby był nawiązany przez audytorów odpowiedzialnych za zarządzanie programem lub przez audytora wiodącego. Celem pierwszego kontaktu jest:
   - ustalenie sposobów komunikacji z przedstawicielem audytowanego,
   - potwierdzenie uprawnień do przeprowadzenia audytu,
   - dostarczenie informacji dotyczących proponowanego harmonogramu oraz składu zespołu audytującego,
   - wnioskowanie o dostęp do stosownych dokumentów,
   - określenie zasad bezpieczeństwa mających zastosowanie w danym miejscu,
   - dokonanie ustaleń dotyczących audytu,

- uzgodnienie uczestnictwa obserwatorów oraz przewodników dla zespołu audytującego.

ETAP 2. Przegląd dokumentacji.

Przed podjęciem działań audytowych zaleca się dokonanie przeglądu dokumentacji w celu określenia zgodności kryteriów audytu z normami, np. technicznymi lub dotyczącymi zarządzania bezpieczeństwem informacji. Dokumentacja ta może obejmować odpowiednie dokumenty i zapisy dotyczące systemu zarządzania, a także raporty z poprzednich audytów. Podczas przeglądu zaleca się wzięcie pod uwagę wielkości, charakteru i złożoności przedsiębiorstwa oraz celów i zakresu audytu. Jeżeli dokumentacja okaże się nieodpowiednia, audytor wiodący powinien poinformować o tym odbiorcę audytu, osoby odpowiedzialne za zarządzanie programem audytów oraz audytowanego. Zaleca się podjęcie decyzji o kontynuacji audytu albo jego zawieszeniu do czasu rozwiązania kwestii związanych z dokumentacją.

ETAP 3. Planowanie działań audytowych realizowanych na miejscu.

Audytor powinien przygotować plan przeprowadzenia audytu stanowiący podstawę do uzgodnień pomiędzy odbiorcą audytu, zespołem audytującym oraz audytowanym. Zaleca się, żeby plan ułatwiał ustalenie terminów i koordynację działań audytowych. Plan audytu powinien być przejrzany i zaakceptowany przez odbiorcę audytu oraz przedstawiony audytowanemu przed rozpoczęciem działań audytowych. Wszelkie zastrzeżenia audytowanego powinny być rozstrzygnięte wspólnie – przez audytora, audytowanego i odbiorcę audytu. Zaleca się, żeby przed kontynuowaniem audytu każda zmiana planu została uzgodniona pomiędzy stronami, których ona dotyczy.

ETAP 4. Przeprowadzanie działań audytowych.

Audyt powinien rozpocząć się od spotkania otwierającego, na którym powinien być obecny audytor oraz osoby odpowiedzialne za audytowane dziedziny, np. kierownicy działów. Spotkanie otwierające powinno się odbyć, aby potwierdzić plan audytu, wyjaśnić jakie czynności będą przeprowadzone i ustalić sposób porozumiewania. Spotkanie otwierające powinno się odbyć z osobami odpowiedzialnymi za audytowane funkcje i procesy. Celem spotkania otwierającego jest:

- potwierdzenie planu audytu,
- krótkie zaprezentowanie, jak będą wykonywane działania audytowe,
- potwierdzenie metod komunikowania się,

- umożliwienie audytowanemu zadawania pytań.

Podczas audytu audytor wiodący powinien zgłaszać wszelkie zastrzeżenia i okresowo informować audytowanego i odbiorcę audytu o postępach w procesie audytu. Jest to dobra praktyka. Dowody zebrane podczas audytu, które wskazują na bezpośrednie i znaczące uchybienia, audytor powinien bezzwłocznie przekazać audytowanemu i jeżeli to właściwe, odbiorcy audytu. Każda sprawa dotycząca problemu wybiegającego poza zakres audytu powinna być odnotowana i przedstawiona audytorowi wiodącemu w celu ewentualnego zakomunikowania odbiorcy audytu i audytowanemu. Jeżeli dostępne dowody wskazują na to, że cele audytu są niemożliwe do osiągnięcia, zaleca się, żeby audytor wiodący przedstawił odbiorcy audytu i audytowanemu przyczyny w celu podjęcia określonych działań. Działania te mogą obejmować potwierdzenie audytu lub zmianę jego planu, celów lub zakresu lub jego zakończenie. Każda potrzeba zmiany zakresu, która może pojawić się na skutek realizacji działań audytowych, powinna być omówiona z odbiorcą, przez niego zatwierdzona oraz jeżeli to właściwe, sprawdzona i zatwierdzona przez audytowanego.

Zbieranie i weryfikowanie informacji - informacje dotyczące celów, zakresu oraz kryteriów audytu, łącznie z informacją dotyczącą oddziaływania pomiędzy funkcjami, działaniami i procesami, powinny być gromadzone poprzez odpowiednie pobieranie próbek podczas audytu i weryfikowane. Tylko uzyskana podczas audytu informacja, która jest możliwa do zweryfikowania, może stanowić dowód. Taka informacja powinna być zapisana. Gromadzenie dowodów to zbieranie informacji, które są istotne dla celów, zakresu i kryteriów audytu, w tym informacji odnoszących się do wzajemnego oddziaływania pomiędzy funkcjami, czynnościami i procesami. Zebrane informacje mogą zostać uznane za dowody audytowe, gdy są zweryfikowane przez audytorów i zaprotokołowane (zapisane). Najczęściej spotykane metody zbierania informacji (źródła informacji/dowodów) to:

- rozmowy,
- wywiady,
- obserwacje działań i procesów,
- przegląd dokumentów,
- przegląd zapisów, rejestrów,
- protokoły,

- streszczenia danych, analizy, wskaźniki,
- raporty,
- bazy danych skomputeryzowanych i witryny sieci www.

Dowody audytowe prowadzące do ustaleń audytowych powinny być rejestrowane. Jeśli zespół audytowy podczas zbierania obiektywnych dowodów dowie się o nowych bądź zmienionych okolicznościach albo zagrożeniach lub szansach, zespół powinien odpowiednio się nimi zająć. Udokumentowane informacje przygotowane do audytu oraz wynikające z niego, powinny być przechowywane przynajmniej do zakończenia audytów lub zgodnie z programem audytowym. Udokumentowane informacje stworzone podczas procesu audytowania z udziałem poufnych lub zastrzeżonych informacji powinny być przez cały czas odpowiednio chronione przez członków zespołu audytowego. Członkowie zespołu audytowego powinni gromadzić i przeglądać informacje istotne dla ich zadań związanych z audytem oraz przygotowywać udokumentowane informacje na temat audytów, wykorzystując wszelkie odpowiednie media.

Gromadzenie dowodów:

1. Wybór źródła informacji.
2. Zbieranie informacji za pomocą odpowiednich próbek.
3. Formułowanie dowodów audytowych.
4. Ocena dowodów zgodnie z kryterium audytu.
5. Zebranie i przygotowanie wyników audytu.
6. Przekazanie zaleceń audytowanego.

Gromadząc dowody należy pamiętać:

- że w razie wątpliwości co do oceny danego dowodu zawsze możesz zwrócić się do audytora wiodącego i/lub poprosić audytowanego o przedstawienie innego dowodu na potwierdzenie wcześniejszej oceny,
- aby skupić się na kryteriach audytu. Informacje, które nie dotyczą audytowanego zakresu nie powinny być poruszane i nie powinny być rejestrowane. Nie powinny one także wpływać na ocenę dowodów odnoszących się do danego audytu,
- że audytowany może być zdenerwowany i/lub zestresowany. Dlatego staraj się podczas interakcji minimalizować napiętą atmosferę, np. nie pośpieszając rozmówcy,

- kulturze osobistej oraz zasadach savoir-vivre: nie należy przerywać audytowanemu, nie należy wprowadzać zbyt luźnej atmosfery, należy unikać tematów drażliwych i osobistych,
- aby zapisywać je krótko i zwięźle; notatki mogą być częścią raportu z audytu i służyć audytorom w kolejnych audytach,
- że najlepszym sposobem dokumentowania dowodu jest powołanie się na konkretny zapis – nazwa dokumentu, wpis w rejestrze czy bazie danych, informacja udostępniona na stronie www lub w mediach społecznościowych. Jeżeli jest to konieczne, można się posiłkować zrzutami ekranu, jednak nie należy nadużywać tej metody.

Opracowanie ustaleń z audytu (ustalenia na podstawie audytu) – Ustalenia mogą wskazywać na zgodność lub niezgodność z kryteriami, np. normami technicznymi. Jeżeli jej wykazanie było jednym z celów audytu, ustalenia mogą wskazać sposób poprawy.
Wnioski z audytu – Zespół audytujący (audytor) powinien naradzić się przed spotkaniem zamykającym audyt w celu:

- sprawdzenia, co ustalono podczas audytu i jakie informacje zebrano w związku z obranymi celami,
- uzgodnienia wniosków z uwzględnieniem niepewności związanej z audytowaniem,
- przygotowania rekomendacji, jeżeli taki jest jeden z wyznaczonych celów,
- przedyskutowania działań po audycie, jeżeli uwzględniono je w planie.

Spotkanie zamykające – przeprowadzenie spotkania zamykającego. Spotkanie zamykające powinno się odbyć, aby zaprezentować wyniki audytu w taki sposób, by mieć pewność, że są one zrozumiałe i uznane przez audytowanego, a także uzgodnić czas niezbędny do zaprezentowania wszelkich planów działań naprawczych przez audytowanego. Spotkanie zamykające prowadzone przez audytora powinno odbyć się w celu przedstawienia ustaleń oraz wniosków w taki sposób, aby były one zrozumiałe i potwierdzone przez audytowanego. Zaleca się ustalenie terminu przedstawienia planu działań korygujących i zapobiegawczych przez audytowanego. W spotkaniu zamykającym powinni uczestniczyć wszyscy audytowani, ale może w nim uczestniczyć także odbiorca audytu i inne strony. Jeżeli to konieczne,

zaleca się, żeby audytor poinformował audytowanego o sytuacjach zaistniałych w trakcie audytu, które mogą negatywnie wpłynąć na ocenę wniosków z audytu. W niektórych przypadkach, np. po audycie w małym przedsiębiorstwie, spotkanie zamykające może polegać tylko na zakomunikowaniu ustaleń i wniosków. Zazwyczaj jednak powinno mieć charakter formalny i być zgodne ze wszystkimi zasadami, łącznie ze składaniem podpisów na liście obecności. Wszelkie rozbieżne opinie zespołu audytującego i audytowanego dotyczące ustaleń i wniosków powinny być przedyskutowane i, jeśli to możliwe, uzgodnione. W przypadku braku zgodności opinii zaleca się zapisanie obu opinii w raporcie z audytu. Raport powinien zawierać rekomendacje dotyczące sposobu poprawy stanu, jeżeli taki jest jeden z celów audytu. W spotkaniu otwierającym i zamykającym powinien uczestniczyć także przedstawiciel najwyższego kierownictwa audytowanego, może także brać udział przedstawiciel klienta audytu. Spotkania otwierające i zamykające mają ustalone w normie PN-EN ISO 19011:2018 strukturę i zakres. Ze spotkania otwierającego i zamykającego należy przygotować listę obecności, gdzie podpiszą się wszyscy uczestniczący – zarówno po stronie zespołu audytującego, jak i audytowanego i klienta audytu

ETAP 5. Zakończenie audytu.

Audyt będzie zakończony, gdy zostaną wykonane wszystkie działania opisane w planie i zostanie rozesłany zatwierdzony raport. Dokumenty dotyczące audytu powinny być zachowane lub zniszczone na podstawie uzgodnień pomiędzy stronami uczestniczącymi oraz zgodnie z procedurami, mającymi zastosowanie przepisami oraz wymaganiami wynikającymi z umów. Zespół audytujący oraz osoby odpowiedzialne za zarządzanie programem audytów nie powinny ujawniać osobom trzecim zawartości dokumentów, innych informacji uzyskanych podczas audytu lub raportu z audytu bez jasno wyrażonego pozwolenia odbiorcy audytu i jeżeli to właściwe, audytowanego, chyba że działanie takie jest nakazane przez prawo. Jeżeli wymagane jest ujawnienie zawartości dokumentu dotyczącego audytu, zaleca się jak najszybsze poinformowanie o tym odbiorcy audytu i audytowanego.

Przygotowanie, zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu – po zakończeniu badania audytorzy dokonują analizy wyników, identyfikując nieprawidłowości i obszary wymagające działań korygujących. Kluczowym elementem tego etapu jest przygotowanie raportu z audytu, który zawiera szczegółowe rekomendacje dotyczące poprawy

procesów i wdrażania działań naprawczych. Raport ten jest podstawą do podejmowania decyzji przez zarząd organizacji i wyznaczenia priorytetów w zakresie działań korygujących. Każdy audyt kończy się raportem, w którym oprócz wskazania luk i braków zamieszcza się również propozycję działań naprawczo-korygujących. W praktyce raport podzielony jest na dwie części – pierwsza część zawiera sumaryczne zestawienie wyników audytu w odniesieniu do wymagań bezpieczeństwa informacji, a druga – wytyczne do doskonalenia i zakres prac, które zwiększą poziom bezpieczeństwa informacji. Niezwykle ważne jest, aby sam audyt, jak i rekomendacje, dostosowane były do branży i specyfikacji organizacji, a także do już funkcjonujących procedur (Borkowski, b.d.). Raport z audytu bezpieczeństwa informacji to dokument, który daje odpowiedź na pytanie, czy organizacja spełnia normy i standardy dotyczące bezpieczeństwa informacji.

Przygotowanie raportu dotyczącego audytu – audytor jest odpowiedzialny za przygotowanie i treść raportu dotyczącego audytu. Raport z audytu powinien dostarczyć pełny, dokładny, zwięzły i jasny protokół z audytu i powinien zawierać konkluzje z audytu. Zaleca się, żeby raport ten zawierał kompletne, dokładne, zwięzłe i jasne informacje dotyczące audytu. Powinien obejmować:

- wskazanie celów audytu,
- podanie czasu trwania audytu,
- określenie zakresu audytu, w szczególności wskazanie audytowanych jednostek organizacyjnych i funkcjonalnych lub audytowanych procesów,
- wskazanie odbiorcy audytu (identyfikacja audytowanego – klienta audytu),
- wskazanie audytora wiodącego i członków zespołu audytującego (identyfikacja zespołu audytorów i uczestników ze strony audytowanego),
- podanie daty i miejsca prowadzenia działań audytowych na miejscu.
- Raport powinien powoływać się na:
- kryteria dotyczące audytu,
- ustalenia wynikające z audytu tj. ustalenia audytowe i związane z nimi dowody,
- wnioski wypływające z audytu,
- oświadczenie o stopniu spełnienia kryteriów audytu,

- wszelkie nierozstrzygnięte rozbieżne opinie między zespołem audytowym a audytowanym.

Raport dotyczący audytu jest tworzony na podstawie indywidualnego wzoru dostosowanego do potrzeb odbiorcy audytu. Najistotniejszym elementem każdego raportu powinny być wnioski z audytu – jeśli zostało to określone w planie audytu, wnioski z audytu mogą prowadzić do zaleceń dotyczących ulepszeń lub przyszłych działań związanych z audytem. Wyniki audytu mogą wskazywać na zgodność lub niezgodność z kryteriami audytu bądź wskazywać na możliwości ulepszenia. Wyniki audytu, niezależnie od rezultatu, powinny być zaprotokołowane i wsparte dowodami audytowymi. Dowody audytowe powinny być oceniane na podstawie kryteriów audytowych w celu ustalenia wyników audytu. Należy podjąć każdą próbę rozwiązania wszelkich rozbieżnych opinii dotyczących dowodów lub ich oceny przed ustaleniem ostatecznych wyników audytu. Ustalenia wyników audytu mogą wskazywać na zgodność lub niezgodność z kryteriami audytowymi. Wyniki audytu wskazujące na niezgodność powinny być omówione z audytowanym, aby wyeliminować możliwe różnice w interpretacji dowodów i wyników audytu. Dla każdej niezgodności powinien zostać przygotowany protokół niezgodności. Protokół niezgodności powinien zawierać co najmniej zdefiniowanie niezgodności, wskazanie, którego wymagania normy / zabezpieczenia dotyczy oraz jakie dowody wskazują na istnienie niezgodności. Ważne jest, aby określić miejsce wystąpienia niezgodności. Protokół niezgodności powinien być podpisany przez audytora i przedstawiciela audytowanej jednostki organizacyjnej, aby potwierdzić zidentyfikowanie niezgodności podczas konkretnej sesji audytowej. Przygotowując raport z audytu trzeba pamiętać, że raport z audytu będzie dokumentem poddawanym ocenie podczas kolejnych audytów i powinien być przygotowany rzetelnie.

Zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu – raport dotyczący audytu powinien być przekazany w uzgodnionym terminie. Jeżeli nie jest to możliwe, należy zakomunikować przyczyny opóźnienia odbiorcy audytu oraz uzgodnić nowy termin przesłania raportu. W przypadku opóźnienia, powody powinny zostać przekazane audytowanemu i klientowi audytu. Raport z audytu powinien być opatrzony datą, zweryfikowany i zaakceptowany przez wszystkie strony audytu. Raport powinien być zatwierdzony, a następnie rozesłany do odbiorców wskazanych przez

odbiorcę audytu. Raport dotyczący audytu jest własnością odbiorcy audytu. Członkowie zespołu audytującego (audytor) oraz wszyscy odbiorcy raportu powinni przestrzegać zasad dotyczących poufności raportu. Przygotowując raport z audytu należy pamiętać, że zawarte w nim wnioski i wyniki powinny opierać się na zgromadzonych wcześniej dowodach. Jeżeli w jakimś zakresie nie udało się zebrać dowodów, które odnosiłyby się do poszczególnych kryteriów, należy to odnotować, nie oceniając spełnienia lub niespełnienia danego kryterium. W raporcie muszą znaleźć się wszelkie parametry audytu, które zostały ustalone na etapie inicjacji audytu, w szczególności daty przeprowadzenia audytu, czas audytu na miejscu, skład zespołu audytowego, cele, zakres i kryteria audytu. Pamiętaj także, żeby raport miał datę jego sporządzenia i podpis audytora wiodącego.

ETAP 6. Przeprowadzenie działań poaudytowych (działania po audycie).

Wnioski wypływające z audytu mogą wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Takie działania są zwykle określane i podejmowane przez audytowanego w uzgodnionym terminie oraz nie są uważane za część audytu. Zaleca się, żeby audytowany informował odbiorcę audytu o statusie tych działań. Niezgodność to brak spełnienia jednego z kryteriów audytu. Niezgodności mogą być stopniowane w zależności od kontekstu organizacji i jej ryzyka (skala ilościowa lub jakościowa). Niezgodności powinny zostać wyeliminowane w czasie uzgodnionym z audytowanym i powinno zostać zweryfikowane wdrożenie i skuteczność tych działań. Niezgodności i towarzyszące im dowody z audytów powinny być rejestrowane. Potencjalne niezgodności, które pojawią się w trakcie gromadzenia dowodów, powinny być przedyskutowane wśród członków zespołu audytowego już czasie audytu. Niezgodności powinny zostać sprawdzone przez audytowanego w celu uzyskania potwierdzenia, że dowody audytowe są dokładne i że niezgodności są zrozumiałe dla audytowanego. Niezgodności wraz z terminem ich korekty powinny zostać ujęte w raporcie z audytu Z niezgodnościami związane są działania korekcyjne oraz działania korygujące. Działaniami korekcyjnymi można określić wszystkie działania, które są podejmowane w celu usunięcia wykrytej niezgodności. Działaniami korygującymi można określić działania podjęte w celu wyeliminowania przyczyny wykrytej niezgodności. Działania korekcyjne i korygujące powinny mieć ustalony z audytowanym termin ich wdrożenia i oceny ich skuteczności. Audytujący powinien informować

osoby zarządzające audytem i zespołem audytowym o statusie działań korekcyjnych i korygujących. Wynik oceny działań korekcyjnych i korygujących musi trafić do klienta audytu, zazwyczaj jako dodatkowy raport. Klient audytu powinien dostać potwierdzenie, że działania eliminujące niezgodność były skuteczne. Działania poaudytowe:

- rejestracja niezgodności w odpowiednim rejestrze w organizacji,
- przygotowanie planu zarządzania niezgodnością,
- analiza ryzyka związanego z niezgodnością,
- wdrożenie działań korekcyjnych,
- wdrożenie działań korygujących,
- ocena skuteczności wdrożenia działań korygujących.

Zarządzając niezgodnościami trzeba mieć na uwadze, żeby dostarczony przez audytowanego plan zarządzania niezgodnościami zawierał takie pozycje, jak analiza przyczyn wystąpienia niezgodności, terminy wdrożenia działań i osoby odpowiedzialne za ich wdrożenie, a także ocena skuteczności wdrożonych działań.

ETAP 7. Weryfikacja zakończenia i skuteczności działań korygujących.

Weryfikacja ta może być częścią następnego audytu, którego celem będzie także sprawdzenie skuteczności i efektywności działań korygujących. Program audytu może określać udział zespołu audytującego w działaniach po audycie, które przynoszą dodatkową korzyść dzięki już zdobytemu przez ten zespół doświadczeniu. Należy zadbać o bezstronność zespołu, jeżeli będzie on wykonywał dodatkowe działania audytowe.

Proces przeprowadzania audytu to nie tylko kontrola, ale także element wspierający poprawę efektywności organizacji. Regularne przeprowadzanie audytów pozwala na identyfikację potencjalnych ryzyk oraz wdrażanie skutecznych rozwiązań. Dzięki cyklicznym audytom bezpieczeństwa mamy pewność, że wszelkie ewentualne nieprawidłowości zostaną zidentyfikowane zanim pojawi się potencjalne zagrożenie. Pozwoli to organizacji na zminimalizowanie ryzyka utraty danych i utraty ciągłości działania organizacji. Najlepsze rezultaty przynosi audyt przeprowadzony przez niezależnych bezstronnych audytorów (Jurkiewicz, 2023).

Podsumowanie

Przeprowadzenie audytu bezpieczeństwa ma istotne znaczenie dla zapewnienia odpowiedniego poziomu ochrony dla organizacji lub instytucji. Pozwala on na identyfikację luk w zabezpieczeniach, wzmocnienie procedur oraz ochronę danych i infrastruktury przed różnymi zagrożeniami. Audyt ma dostarczać obiektywnych dowodów, że procesy działają zgodnie z wymaganiami norm i przepisów, a nie skupiać się na wychwyceniu każdej nieprawidłowości za wszelką cenę. Może być pomocny w osiąganiu celów organizacyjnych, bowiem stanowi systematyczne i metodyczne podejście do oceny skuteczności zarządzania organizacją. Należy podkreślić, że audyt stanowi skuteczny i niezawodny instrument wspierający politykę bezpieczeństwa obiektu i umożliwiający skontrolowanie zarządzania bezpieczeństwem. Dostarcza informacji, które są niezbędne, by zadbać o bezpieczeństwo w organizacji. W przeprowadzaniu audytu ważne są (Wójcik, 2019): uczciwość, rzetelność, profesjonalizm w działaniu, poufność, niezależność, ustalenie faktów, uwzględnienie trudności i określenie prawdopodobieństwa, że cele audytu zostaną osiągnięte (ta zasada jest narzucona przez normę ISO 19011). Należy przestrzegać powyższych zasad, aby wyniki audytu były jednoznaczne i aby można było spodziewać się, że inni audytorzy uzyskają podobne wyniki w podobnych okolicznościach. Można go zatem potraktować jako narzędzie do doskonalenia organizacji i przyniesienia jej wartości dodanej (Gualitywise, b.d.). Proces przeprowadzania audytu to nie tylko kontrola, ale także element wspierający poprawę efektywności organizacji. Regularne przeprowadzanie audytów pozwala na identyfikację potencjalnych ryzyk oraz wdrażanie skutecznych rozwiązań, które mają na celu zapewnienie zgodności działań z przepisami wewnętrznymi organizacji i oczekiwaniami rynku. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, zaleca się cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia.

Literatura

1. Akademia Jakości. (b.d.). *Audyt wewnętrzny*, *Wewnętrzny audyt jakości w przedsiębiorstwie produkcyjnym,* akademiajakosci.com. Pobrano z: https://akademiajakosci.com/wewnetrzny-audyt-jakosci-w-przedsiebiorstwie-produkcyjnym (dostęp: 20.09.2025).
2. Biarda, M. (2022). *Rola audytu w systemach zarządzania*, *Jakość bez retuszu z Anna Farion*. Pobrano z: https://jakoscbezretuszu.pl/rola-audytu-w-systemach-zarzadzania (dostęp: 12.02.2026).
3. Borkowski, T. (b.d.). *Raport z audytu bezpieczeństwa informacji – co powinien zawierać?* Pobrano z: https://www.pbsg.pl/raport-z-audytu-bezpieczenstwa-informacji/#:~:text=Raport%20z%20audytu%20bezpiecze%C5%84stwa%20informacji%20to%20dokument%2C%20kt%C3%B3ry%20daje%20odpowied%C5%BA,i%20standardy%20dotycz%C4%85ce%20bezpiecze%C5%84stwa%20informacji (dostęp: 12.02.2026).
4. CeCert. (2024). *Co to jest audyt w firmie? Rodzaje audytów i korzyści z ich przeprowadzenia*, Pobrano z: https://cecert.pl/co-to-jest-audyt-w-firmie-rodzaje-audytow-i-korzysci-z-ich-przeprowadzenia (dostęp: 20.09.2025).
5. Delkomtech. (b.d.). *Czym jest audyt bezpieczeństwa informacji i kiedy jest potrzebny w Twojej firmie?* Delkom Group Sp. z.o.o. Pobrano z: https://www.delkomtech.pl/aktualnosci/czym-jest-audyt-bezpieczenstwa-informacji-i-kiedy-jest-potrzebny-w-twojej-firmie (dostęp: 12.02.2026).
6. EITT. (b.d.). Effective IT Trainings. *Audyt wewnętrzny*? Pobrano z: https://eitt.pl/slownik/audyt-wewnetrzny (dostęp: 20.09.2025).
7. EITT. (b.d.). Effective IT Trainings, *Co to jest Audytor bezpieczeństwa informacji?* Pobrano z: https://eitt.pl/slownik/audytor-bezpieczenstwa-informacji (dostęp: 21.09.2025).
8. Fehler, W. (2016). *O pojęciu bezpieczeństwa informacyjnego*, W: M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa: Wydawca Pracownia Wydawnicza Wydziału Humanistycznego.
9. Global Cert. (2023). *Cechy dobrego audytora wewnętrznego.* Pobrano z: https://certyfikacja-iso.pl/2023/10/26/cechy-dobrego-audytora-wewnetrznego (dostęp: 20.09.2025).

10. Global Cert. (2025). *Norma ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania.* Pobrano z: https://certyfikacja-iso.pl/2025/01/17/norma-iso-19011-wytyczne-dotyczace-audytowania-systemow-zarzadzania (dostęp: 20.09.2025).
11. Godula, M. (2026). *Czym jest Bezpieczeństwo informacji? Definicja, filary, zagrożenia i wdrażanie w organizacji.* Pobrano z: https://eitt.pl/baza-wiedzy/czym-jest-bezpieczenstwo-informacji-kompendium (dostęp: 10.03.2026).
12. Gualitywise. (b.d.). *Audyt – nie szukaj niezgodności!*
13. Highspring. (2025). *The top 10 characteristics of exceptional internal audit leaders*, Highspring Jan 29, 2025. Pobrano z: https://www.highspring.com/blog/the-10-characteristics-of-exceptional-internal-audit-leaders (dostęp: 20.09.2025).
14. Hotiuk, Z. (2024). *Audyt – narzędzie kontroli czy doskonalenia organizacji?* Pobrano z: https://pep.pl/poradnik/audyt (dostęp: 12.02.2026).
15. https://www.qualitywise.pl/audyt-nie-szukaj-niezgodnosci (dostęp: 29.09.2025).
16. Instytut Audytorów Wewnętrznych IIA Polska. (b.d). *Definicja Audyt wewnętrzny*. Pobrano z: https://www.iia.org.pl/o-nas/definicja-aw (dostęp: 21.09.2025).
17. Jurkiewicz, P. (2023). *Jak audyt bezpieczeństwa wygląda w praktyce?* Pobrano z: https://www.doering-partnerzy.pl/jak-audyt-bezpieczenstwa--wyglada-w-praktyce (dostęp: 20.09.2025).
18. Klichowski, M. (b.d.). *Na czym polega audyt bezpieczeństwa informacji i dlaczego warto go wykonywać?* Pobrano z: https://www.pbsg.pl/na-czym-polega-audyt-bezpieczenstwa-informacji (dostęp: 12.02.2026).
19. Kowalewski, M., Kowalewski J. (2004). *Zarządzanie bezpieczeństwem informacji organizacji*, Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.
20. Koziej, S. (2011). *Teoria sztuki wojennej,* Warszawa: Wydawnictwo BELLONA.
21. Lean Partner. (b.d.). *Audyt wewnętrzny, Czym jest audyt wewnętrzny? Rodzaje audytów oraz ich cele.* Pobrano z: https://leanpartner.pl/audyt--wewnetrzny (dostęp: 20.09.2025).

22. Malon Group. (b.d). ISO 27001. Wdrożenie ISO 27001 – System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami ISO 2700. Pobrano z: https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001 (dostęp: 26.07.2025).
23. Microsoft. (b.d). *Co to jest bezpieczeństwo informacji?* Pobrano z: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-information-security-infosec (dostęp: 12.02.2026).
24. Millichamp, A., Taylor, J. (2018). *Auditing*, 11th Edition, United Kingdom: Cengage Learning EMEA.
25. Ministerstwo Cyfryzacji. (b.d.). *Krajowy system cyberbezpieczeństwa.* Pobrano z: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- (dostęp: 20.09.2025).
26. Moeller, R. (2021). *Nowoczesny audyt wewnętrzny,* Warszawa: Wydawnictwo Nieoczywiste.
27. Nowak, A., Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*. Warszawa: Wydawnictwo AON.
28. Przybylska, J., Rydzak, W., Trębecki, J. (2021). *Skuteczne komunikowanie w audycie wewnętrznym*, Warszawa: Wydawnictwo CeDeWu.
29. PUW. (b.d.). *Czym jest audyt – rodzaje, metody i cele jego przeprowadzania.* Pobrano z: https://www.puw.pl/pl/strefa-wiedzy/czym-jest-audyt-rodzaje-metody-i-cele-jego-przeprowadzania (dostęp: 20.09.2025).
30. Rada Europejska Rada Unii Europejskiej. (2024) *Ochrona danych w UE*. Pobrano z:https://www.consilium.europa.eu/pl/policies/data-protection/ (dostęp: 31.08.2025).
31. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Pobrano z: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20120000526 (dostęp: 20.09.2025).
32. Serwis Rzeczypospolitej Polskiej gov.pl. (b.d.). *Standardy Krajowych Ram Interoperacyjności (KRI), Portal Interoperacyjności i Architektury*. Pobrano z:https://www.gov.pl/web/ia/koncepcja-nowych-kri-dokument (dostęp: 20.09.2025).

33. Sudhara International. (2023). *ISO 19011:2018 – Co to jest i do czego służy?* Pobrano z: https://sudharapolska.com/norma-iso-19011/ (dostęp: 12.02.2026).
34. Syta, J. (2025). *Zarządzanie cyberbezpieczeństwem. Pracownicy. Procesy. Technologie*, Warszawa: Wydawnictwo PWN.
35. Urząd Ochrony Danych Osobowych, UODO (2022). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Pobrano z: https://uodo.gov.pl/pl/131/224 (dostęp: 31.08.2025).
36. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560). Pobrano z: https://www.dziennikustaw.gov.pl/DU/rok/2018/pozycja/1560 (dostęp: 20.09.2025).
37. Widomski, P. (2026). *Co to jest i jak działa Bezpieczeństwo informacji (InfoSec)? – Analiza, Bezpieczeństwo informacji*. Pobrano z: https://nflo.pl/slownik/bezpieczenstwo-informacji/ (dostęp: 12.02.2026).
38. Wójcik, A. (2017). *Prowadzenie audytu zarządzania bezpieczeństwem organizacyjno-technicznym obiektów (część 2)*. Pobrano z: https://www.zabezpieczenia.com.pl/ochrona-informacji/prowadzenie-audytu-zarzadzania-bezpieczenstwem-organizacyjno-technicznym-obiektow (dostęp: 22.09.2025).
39. Wójcik, A. (2019). *Przeprowadzanie audytu zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 6. Prowadzenie audytu. Praktyka i wytyczne,* Pobrano z: https://www.zabezpieczenia.com.pl/ochrona-informacji/przeprowadzanie-audytu-zarzadzania-bezpieczenstwem-organizacyjno-technicznym-0 (dostęp: 13.02.2026).
40. Wójcik, A. (2017). *Podstawy przeprowadzania audytu dotyczącego zarządzania bezpieczeństwem obiektów*, *Zabezpieczenia*. Pobrano z: https://www.zabezpieczenia.com.pl/ochrona-informacji/podstawy-przeprowadzania-audytu-dotyczacego-zarzadzania-bezpieczenstwem-obiektow (dostęp: 22.09.2025).
41. Zespół LexDigital. (2024). *InfoSec – czyli bezpieczeństwo informacji.* Pobrano z: https://lexdigital.pl/bezpieczenstwo-informacji (dostęp: 12.02.2026).

Waldemar Perdion[1]
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie

https://doi.org/10.29316/9788368103359_6

OCHRONA DANYCH OSOBOWYCH W CYBERPRZESTRZENI

PERSONAL DATA PROTECTION IN CYBERSPACE

Streszczenie

W dobie dynamicznego rozwoju technologii cyfrowych, temat ochrony danych osobowych nabiera szczególnego znaczenia. Nasza codzienność coraz silniej przenika się z cyberprzestrzenią – miejscem, gdzie wymiana informacji, komunikacja, zakupy, a nawet aktywność zawodowa odbywają się za pośrednictwem Internetu. W tym wirtualnym świecie niemal każda nasza aktywność wiąże się z przetwarzaniem danych – często bardzo wrażliwych. Ochrona danych osobowych to jedno z kluczowych wyzwań XXI wieku. W epoce, w której informacja stała się jedną z najcenniejszych walut, dane osobowe mogą być zarówno zasobem, jak i zagrożeniem. Ich niewłaściwe przetwarzanie, przechowywanie czy wykorzystywanie może prowadzić nie tylko do naruszenia prywatności jednostki, ale również do realnych strat finansowych, kradzieży tożsamości, manipulacji wyborczych, a nawet destabilizacji systemów państwowych. W tym kontekście ochrona danych nie jest już wyłącznie domeną specjalistów z zakresu informatyki czy prawa, ale staje się sprawą publiczną i społeczną, dotyczącą każdego użytkownika technologii

[1] https://orcid.org/0000-0001-6956-8508, e-mail: waldemar.perdion@uth.edu.pl

cyfrowych. Celem niniejszego opracowania jest podjęcie refleksji nad skutecznością obowiązujących regulacji prawnych dotyczących ochrony danych osobowych w warunkach rzeczywistości cyfrowej. Czy obecne przepisy są wystarczające, by zapewnić realne bezpieczeństwo użytkownikom Internetu? Czy są w stanie chronić nie tylko prywatność zwykłych obywateli, ale również interesy instytucji publicznych i bezpieczeństwo państwa? W dobie rosnącej liczby cyberataków, wycieków danych oraz nadużyć ze strony podmiotów komercyjnych, pytania te stają się nie tylko zasadne, ale wręcz palące. W niniejszej pracy postaram się przybliżyć istotę zagadnienia, wskazać najważniejsze wyzwania, a także zaprezentować aktualne ramy prawne i praktyczne rozwiązania, które mają służyć ochronie danych osobowych w cyberprzestrzeni.

Słowa kluczowe: dane osobowe, przestępczość, cyberprzestrzeń, bezpieczeństwo, informacje

Abstract

In an era of dynamic development in digital technologies, the issue of personal data protection is gaining particular importance. Our daily lives are increasingly intertwined with cyberspace – a place where information exchange, communication, shopping, and even professional activities take place online. In this virtual environment, almost every activity involves the processing of data – often highly sensitive data. Personal data protection is one of the key challenges of the 21st century. In a time where information has become one of the most valuable currencies, personal data can be both a resource and a threat. Improper processing, storage, or use of such data can lead not only to violations of individual privacy but also to tangible financial losses, identity theft, electoral manipulation, and even the destabilization of state systems. In this context, data protection is no longer the exclusive domain of IT or legal specialists; it has become a public and social issue that affects every user of digital technologies. The purpose of this study is to examine the effectiveness of existing legal regulations concerning personal data protection in the digital world. Are the current regulations sufficient to ensure real security for internet users? Can they protect not only the privacy of ordinary citizens, but also the interests of public institutions and state security? In an age of increasing cyberattacks, data leaks, and abuses by commercial entities, these questions have become not only relevant but even urgent. In this paper, I will seek to explore the essence of the issue, identify the key challenges, and present the current legal framework and practical solutions for protecting personal data in cyberspace.

Keywords: personal data, crime, cyberspace, security, information

Wstęp

Informacja to jeden z najcenniejszych zasobów współczesnego świata. W dobie społeczeństwa informacyjnego stanowi ona dobro strategiczne, które należy skutecznie chronić. Wiedza – rozumiana jako umiejętność pozyskiwania, analizowania i wykorzystywania informacji – jest dziś fundamentem podejmowania decyzji na wszystkich poziomach funkcjonowania społeczeństwa: od indywidualnych obywateli, przez przedsiębiorstwa, aż po instytucje publiczne. Posiadanie informacji ułatwia planowanie, przewidywanie zagrożeń oraz efektywną realizację działań.

Właściwe gospodarowanie informacją, a także jej ochrona, są nieodłącznym elementem sprawnego funkcjonowania państwa i bezpieczeństwa jego obywateli. Ustawowe objęcie ochroną niektórych kategorii informacji oraz prawne uregulowanie dostępu do nich potwierdzają, że informacja została przez ustawodawcę uznana za dobro prawnie chronione. Współczesne podejście do informacji obejmuje zarówno jej wymiar materialny, jak i niematerialny – może ona przybierać formę idei, myśli, gestu, dźwięku, symbolu, dokumentu, dzieła sztuki, a także zapisów umownych. W tym szerokim kontekście mieszczą się również dane osobowe, będące jedną z najważniejszych i najbardziej wrażliwych kategorii informacji (Taczkowska-Olszewska, Chałubińska-Jentkiewicz, Nowikowska, 2019, s. 11).

Pojęcie danych osobowych zostało po raz pierwszy szerzej ujęte w 1980 roku w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD), gdzie zaproponowano definicję, która – w zmodyfikowanej formie – funkcjonuje do dziś. Według niej dane osobowe to wszelkie informacje dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania (Rojszczak, 2019, s. 150).

Z kolei zgodnie z obowiązującym w Unii Europejskiej Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), dane osobowe oznaczają: „Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową

lub społeczną tożsamość osoby fizycznej" (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

W praktyce oznacza to, że każda informacja, która może prowadzić do identyfikacji konkretnej osoby, nawet jeśli wymaga połączenia kilku elementów, uznawana jest za daną osobową. Szczególną kategorię stanowią dane wrażliwe, które ze względu na swój charakter wymagają dodatkowej ochrony. Zostały one zdefiniowane w art. 27 ust. 1 nieobowiązującej już ustawy o ochronie danych osobowych, a obecnie ich katalog został przeniesiony do art. 107 ust. 1 RODO. Obejmuje on m.in. informacje ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- dane o stanie zdrowia, dane genetyczne, biometryczne, nałogach lub życiu seksualnym,
- dane dotyczące wyroków skazujących, postępowań sądowych i administracyjnych (Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych).

Zarówno dane zwykłe, jak i wrażliwe są przedmiotem szczególnego zainteresowania prawodawcy, ponieważ ich ujawnienie lub niewłaściwe przetwarzanie może prowadzić do naruszenia prywatności, dyskryminacji, a nawet zagrożenia dla wolności i bezpieczeństwa jednostki.

Współcześnie obserwujemy niezwykle dynamiczny proces przenoszenia coraz większej liczby aktywności człowieka do przestrzeni wirtualnej, będącej integralną częścią cyberprzestrzeni. Funkcjonowanie w niej stało się nieodzownym elementem życia społecznego, gospodarczego i politycznego. Korzyści płynące z wykorzystania cyberprzestrzeni są niepodważalne, jednak towarzyszą im również poważne zagrożenia – w tym możliwość jej wykorzystania w sposób sprzeczny z interesem państwa i obywateli.

Zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne oraz powiązania między nimi i ich relacje z użytkownikami (Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne).

Sednem tej definicji są dwa kluczowe pojęcia: informacja oraz systemy teleinformatyczne. Informacja – jako zasób strategiczny – została dostrzeżona jako dobro wymagające szczególnej ochrony. Współcześnie traktowana jest nie tylko jako nośnik wiedzy, lecz także jako potencjalna broń, wykorzystywana na piątym teatrze działań wojennych – obok lądu, morza, powietrza i przestrzeni kosmicznej – jakim stała się cyberprzestrzeń (Lakomy, 2015, s. 63).

To także odrębna przestrzeń społeczna, w której zachodzą procesy komunikacji i wymiany gospodarczej. Wymaga ona odpowiedniego zabezpieczenia ze względu na interesy jej użytkowników – zarówno w zakresie ochrony danych osobowych, jak i ochrony nieletnich czy przeciwdziałania przestępczości (Lubasz, 2013). Do charakterystycznych cech cyberprzestrzeni zalicza się jej:

- rozległość (globalny zasięg),
- zdolność do łączenia zasobów w ogromną bazę danych,
- złożoność,
- bezprzestrzenność – brak fizycznych granic i wymiarów, jakie znamy ze świata realnego (Wasilewski, 2015).

W literaturze przedmiotu można odnaleźć różne definicje cyberprzestrzeni. M. Rojszczak przywołuje tę sformułowaną przez Departament Obrony Stanów Zjednoczonych, według której cyberprzestrzeń to: „Domena związana z użyciem elektronicznych i elektromagnetycznych urządzeń w celu gromadzenia, modyfikowania i wymiany danych za pomocą systemów sieciowych oraz związanej z nimi infrastruktury fizycznej" (Rojszczak, 2019, s. 53).

Autor jednocześnie podkreśla, że w odniesieniu do koncepcji Internetu, cyberprzestrzeń to przede wszystkim przestrzeń zastosowań i możliwości technicznych, której fizyczny wymiar trudno jest jednoznacznie zdefiniować. M. Rojszczak proponuje również najszerszą definicję cyberprzestrzeni, zgodnie z którą obejmuje ona wszelkie urządzenia zdolne do komunikacji sieciowej – niezależnie od tego, czy są w danym momencie podłączone do sieci publicznej. Internet pozostaje jej dominującą częścią, umożliwiającą globalną wymianę treści (Rojszczak, 2019, s. 54).

A. Bartnicki z kolei ujmuje cyberprzestrzeń jako przestrzeń komunikacyjną tworzoną przez systemy powiązań internetowych, pozwalającą użytkownikom na komunikację i budowanie relacji w czasie rzeczywistym.

Jego zdaniem jest to środowisko wymiany informacji za pomocą sieci i systemów komputerowych, w którym wszelkie działania mają odmienny charakter niż te podejmowane w świecie fizycznym (Bartnicki, 2020, s. 145).

Rozwój tzw. globalnej „internetomanii" oraz szeroka dostępność usług sieciowych niosą ze sobą poważne zagrożenia. Jednym z kluczowych problemów pozostaje możliwość przechwytywania danych wrażliwych przez niepowołane podmioty. Informacje te, ze względu na swoją specyfikę, mogą prowadzić m.in. do kradzieży technologii, ujawnienia rozwiązań konstrukcyjnych, kompromitacji systemów obrony, a w konsekwencji – do osłabienia lub nawet destabilizacji gospodarczej podmiotów, a w skrajnych przypadkach – całych państw (Bartnicki, 2020, s. 147).

W tym kontekście istotne staje się pojęcie cyberprzestępczości, które zostało zdefiniowane m.in. przez X Kongres ONZ w sprawie zapobiegania przestępczości i traktowania przestępców. W ujęciu szerokim cyberprzestępstwo obejmuje wszelkie działania popełnione z użyciem systemów komputerowych lub sieci, jak również te, które ich dotyczą. Obejmuje to m.in. nielegalne posiadanie, udostępnianie czy rozpowszechnianie informacji za pomocą narzędzi cyfrowych. Zjawisko cyberprzestępczości staje się coraz powszechniejsze, a jego rosnący poziom trudności wykrywania i przeciwdziałania wynika m.in. z relatywnej anonimowości sprawców oraz transgranicznego charakteru przestępstw cyfrowych (Bartnicki, 2020, s. 147).

Każda nasza aktywność w Internecie – wyszukiwanie informacji, korzystanie z mediów społecznościowych, dokonywanie zakupów online czy logowanie się do aplikacji – pozostawia po sobie cyfrowy ślad. Jest to zespół informacji, które świadomie lub nieświadomie pozostawiamy w środowisku cyfrowym. Cyfrowy ślad obejmuje zarówno dane jawne (np. zdjęcia profilowe, komentarze, posty), jak i ukryte (adresy IP, dane lokalizacyjne, czas logowania czy kliknięcia w linki). Konsekwencje istnienia cyfrowych śladów są wielowymiarowe. Z jednej strony umożliwiają one tworzenie spersonalizowanych usług i udoskonalanie doświadczenia użytkownika. Z drugiej – mogą prowadzić do nadużyć, takich jak profilowanie, sprzedaż danych stronom trzecim, manipulacja informacjami czy kradzież tożsamości. Warto podkreślić, że cyfrowy ślad ma również znaczenie prawne – jego analiza może posłużyć jako dowód w sprawach sądowych, ale też jako narzędzie inwigilacji lub represji w rękach autorytarnych reżimów. Świadomość jego istnienia oraz umiejętność zarządzania nim stają się niezbędnymi kompetencjami w świecie cyfrowym.

Kwestie związane z ochroną danych osobowych w Polsce regulowane są zarówno przez prawo unijne, jak i krajowe. Fundamentalnym aktem prawnym obowiązującym na poziomie Unii Europejskiej jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., znane szerzej jako RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Rozporządzenie to zaczęło obowiązywać we wszystkich państwach członkowskich Unii Europejskiej 25 maja 2018 roku i ujednoliciło zasady przetwarzania danych osobowych w całej UE. Wraz z nim przyjęto Dyrektywę 2016/680, dotyczącą przetwarzania danych osobowych w związku z zapobieganiem przestępczości, wykrywaniem i ściganiem przestępstw.

Zgodnie z art. 4 pkt 1 RODO, dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osoba możliwa do zidentyfikowania to taka, której tożsamość można ustalić bezpośrednio lub pośrednio, zwłaszcza na podstawie takich danych jak: imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających jej tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

RODO wprowadza katalog zasad przetwarzania danych osobowych (art. 5), a także nowe prawa i obowiązki dla administratorów danych i osób, których dane są przetwarzane. RODO znacząco rozszerzyło katalog praw przysługujących osobom fizycznym, których dane osobowe są przetwarzane. Osoby te, zwane osobami, których dane dotyczą, mają obecnie większy wpływ na to, w jaki sposób ich dane są wykorzystywane. Do najważniejszych praw tych osób należą:

- Prawo dostępu do danych – osoba ma prawo dowiedzieć się, czy jej dane są przetwarzane, a jeśli tak – uzyskać do nich dostęp oraz informacje o celu i zakresie przetwarzania,
- Prawo do sprostowania danych – umożliwia poprawienie danych nieprawidłowych lub ich uzupełnienie,
- Prawo do usunięcia danych („bycia zapomnianym") – daje możliwość żądania usunięcia danych, gdy nie są już potrzebne, zgoda została cofnięta lub przetwarzanie odbywa się niezgodnie z prawem,

- Prawo do ograniczenia przetwarzania – np. w sytuacji, gdy osoba kwestionuje prawidłowość danych,
- Prawo do przenoszenia danych – umożliwia otrzymanie danych w ustrukturyzowanym formacie i ich przekazanie innemu administratorowi,
- Prawo do sprzeciwu – można sprzeciwić się przetwarzaniu danych, np. w celach marketingu bezpośredniego,
- Prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – chroni przed automatycznym profilowaniem, które może wywoływać skutki prawne (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Zgodnie z RODO, administrator danych osobowych to podmiot (osoba fizyczna, prawna, organ publiczny, jednostka lub inny organ), który decyduje o celach i sposobach przetwarzania danych osobowych. Na administratorach ciąży szereg obowiązków mających na celu zapewnienie zgodnego z prawem i bezpiecznego przetwarzania danych.

Do podstawowych obowiązków administratora należy:

- Zasada rozliczalności – administrator musi być w stanie wykazać, że przetwarza dane zgodnie z zasadami określonymi w RODO,
- Minimalizacja danych – przetwarzane mogą być tylko te dane, które są niezbędne do realizacji danego celu,
- Obowiązek informacyjny – administrator jest zobowiązany poinformować osobę, której dane dotyczą, o celach i podstawach przetwarzania danych, czasie ich przechowywania, a także o przysługujących jej prawach,
- Zapewnienie bezpieczeństwa danych – administrator powinien stosować środki techniczne i organizacyjne zapewniające odpowiedni stopień ochrony danych,
- Zgłaszanie naruszeń danych – administrator ma obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego nie później niż w ciągu 72 godzin od jego wykrycia (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Najważniejszym dokumentem regulującym ochronę danych osobowych w cyberprzestrzeni jest również rozporządzenie unijne RODO. Określa ono zasady, narzędzia, instrumenty oraz środki ochrony danych osobowych w cyberprzestrzeni. Wprowadziło ono również kilka elementów odnoszących się wprost do ochrony danych w cyberprzestrzeni. Jednym z nich jest wspomniane wyżej prawo do bycia zapomnianym (Bakalarczyk-Burakowska, Nowicka, 2020, s. 78). Kolejną ważną regulacją jest określenie ram prawnych profilowania, czyli dowolnego zautomatyzowanego przetwarzania danych osobowych pozwalającego ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Istotnym dla przetwarzania danych osobowych w cyberprzestrzeni jest również artykuł 32 RODO, określający wymóg szacowania ryzyka w przypadku wdrażania organizacyjnych oraz technicznych środków bezpieczeństwa przetwarzania danych. Z kolei art. 35 wskazuje, że w przypadku, gdy dane są przetwarzane w szczególności z wykorzystaniem nowych technologii, konieczne jest przeprowadzanie oraz udokumentowanie oceny skutków dla ochrony danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Na poziomie krajowym ochrona danych osobowych opiera się również na następujących aktach prawnych:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.) – reguluje zasady działania Prezesa Urzędu Ochrony Danych Osobowych (UODO) i uzupełnia postanowienia RODO na gruncie krajowym,
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.) – ma na celu zapewnienie bezpieczeństwa sieci i systemów informatycznych używanych do świadczenia kluczowych usług,
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.) – dotyczy m.in. odpowiedzialności dostawców usług online w zakresie przetwarzania danych osobowych,

- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579 z późn. zm.) – odnosi się do kwestii podpisu elektronicznego, tożsamości cyfrowej i bezpieczeństwa transakcji elektronicznych,
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.) – reguluje zasady wprowadzania i stosowania technologii informacyjno-komunikacyjnych w instytucjach publicznych. Jej celem jest zapewnienie sprawnej, nowoczesnej i bezpiecznej realizacji zadań publicznych, m.in. poprzez ujednolicenie systemów teleinformatycznych, wdrożenie elektronicznej administracji, interoperacyjność systemów oraz dostęp obywateli do usług publicznych drogą elektroniczną.

Rozwój technologii informatycznych oraz powszechna cyfryzacja codziennego życia przyniosły wiele korzyści, ale również nowe zagrożenia dla prywatności. Dane osobowe użytkowników Internetu stały się cennym towarem, a ich przejęcie i wykorzystanie przez nieuprawnione podmioty może skutkować poważnymi konsekwencjami – od kradzieży tożsamości po szantaż czy oszustwa finansowe. W niniejszym rozdziale przedstawiono najczęstsze formy zagrożeń, z jakimi spotykają się użytkownicy sieci.

Phishing to jedna z najczęstszych form oszustwa internetowego, polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych osobowych, loginów, haseł czy danych karty płatniczej. Atakujący wykorzystują mechanizmy socjotechniki, czyli manipulacji psychologicznej, aby skłonić ofiarę do podjęcia określonego działania – np. kliknięcia w link, pobrania załącznika lub podania danych logowania. Przykładami mogą być fałszywe wiadomości e-mail rzekomo od banku, portalu społecznościowego lub firmy kurierskiej, w których użytkownik proszony jest o „weryfikację konta" lub „potwierdzenie przesyłki" (Hadnagy, Fincher, 2016, s. 28). Wzrost liczby ataków phishingowych potwierdzają coroczne raporty – wskazując, że każdy użytkownik e-mail prędzej czy później stanie się adresatem wiadomości phishingowej (Hadnagy, Fincher, 2016, s. 57).

Ataki hakerskie, czyli nieautoryzowane próby uzyskania dostępu do systemów informatycznych, są kolejnym poważnym zagrożeniem dla danych osobowych. Cyberprzestępcy wykorzystują luki w zabezpieczeniach

systemów firm i instytucji publicznych, aby uzyskać dane klientów, użytkowników czy pacjentów. Wycieki danych mogą mieć dramatyczne skutki – dane trafiają na czarne rynki (tzw. dark web), gdzie są sprzedawane lub wykorzystywane do dalszych oszustw. W ostatnich latach głośne były przypadki wycieków danych m.in. z serwisów społecznościowych, firm telekomunikacyjnych czy instytucji medycznych. Do popularnych technik hakerskich należą:

- ataki typu SQL injection – to podatność występująca w aplikacjach internetowych, umożliwiająca atakującemu „wstrzyknięcie" własnego zapytania SQL do bazy danych. Do ataku dochodzi w sytuacji, gdy aplikacja nie filtruje odpowiednio zapytań przesyłanych do bazy danych albo w ogóle tego nie robi. W efekcie aplikacja przekazuje do bazy danych zapytanie, które – wraz z dołączonym kodem – zostaje wykonane w całości. Skutecznie przeprowadzony atak może prowadzić do odczytu, modyfikacji, dodania lub usunięcia danych z bazy, a także obejścia mechanizmów zabezpieczających (Dymek, Nycz, Gerka, 2016, s. 27),
- wykorzystanie słabych haseł i braku uwierzytelnienia dwuskładnikowego,
- ataki typu zero-day, czyli wykorzystujące nieznane wcześniej luki bezpieczeństwa.

Malware (złośliwe oprogramowanie) to ogólna kategoria programów stworzonych w celu szkodzenia użytkownikowi – kradzieży danych, śledzenia działań online, przejęcia kontroli nad komputerem. Szczególnie niebezpieczną odmianą jest ransomware, który szyfruje pliki użytkownika i żąda okupu za ich odszyfrowanie. Do najczęstszych sposobów infekcji należą: otwieranie podejrzanych załączników e-mail, pobieranie plików z niesprawdzonych źródeł czy korzystanie z niezaktualizowanego oprogramowania. Ransomware szczególnie uderza w firmy i instytucje, powodując przestoje i straty finansowe, ale także indywidualni użytkownicy są jego ofiarami (Diogenes, Ozkaya, 2023).

Media społecznościowe są miejscem, gdzie użytkownicy dobrowolnie udostępniają wiele informacji o sobie – często bez refleksji nad tym, kto i w jakim celu może z nich skorzystać. Dane zamieszczane na Facebooku, Instagramie czy TikToku mogą być wykorzystywane nie tylko przez

reklamodawców, ale także przez osoby trzecie do profilowania, manipulacji (np. politycznej) czy kradzieży tożsamości.

Najczęstsze zagrożenia związane z mediami społecznościowymi to:

- oszustwa tożsamościowe (tworzenie fałszywych profili),
- wyłudzanie informacji w ramach konkursów lub quizów,
- rozpowszechnianie fake newsów i dezinformacji,
- brak odpowiednich ustawień prywatności, umożliwiający dostęp do danych przez nieznajomych.

W kontekście RODO nadużycia te mogą prowadzić do naruszeń prawa do prywatności, a odpowiedzialność spoczywa nie tylko na użytkownikach, ale również na administratorach portali społecznościowych, którzy mają obowiązek wdrażania środków technicznych i organizacyjnych chroniących dane osobowe.

W obliczu rosnących zagrożeń cyfrowych ochrona danych osobowych nie może ograniczać się jedynie do przepisów prawnych. Równie istotna jest świadomość użytkowników oraz stosowanie konkretnych środków technicznych i organizacyjnych. Współczesna cyberprzestrzeń wymaga od każdego – zarówno osób prywatnych, jak i podmiotów przetwarzających dane – stosowania praktycznych i skutecznych metod zabezpieczeń, które minimalizują ryzyko wycieku lub nieuprawnionego wykorzystania informacji. W niniejszym rozdziale przedstawiono najważniejsze i najbardziej dostępne sposoby ochrony danych w codziennym użytkowaniu Internetu i technologii cyfrowych.

Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że te dodatkowe informacje przechowywane są osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Wykorzystuje się ją w celu utrudnienia identyfikacji określonej osoby fizycznej. Polega na zastąpieniu danych osobowych dotyczących osoby fizycznej innymi danymi np. numerem identyfikacyjnym. Pseudonimizacji możemy dokonać za pomocą: zaciemniania lub maskowania liter, szyfrowania, tokenyzacji, zastępowania części danych ciągiem znaków, modyfikacji danych w taki sposób, by pokazywały przybliżone wartości.

Anonimizacja polega z kolei na nieodwracalnym usunięciu wszystkich informacji, które w jakikolwiek sposób umożliwiają identyfikację określonej osoby, której dane dotyczą, przez administratora danych lub osobę trzecią (Bartnicki, 2020).

Jednym z podstawowych filarów bezpieczeństwa cyfrowego pozostaje stosowanie silnych i unikalnych haseł do wszystkich kont i usług. Hasła powinny zawierać minimum 12 znaków i być kombinacją małych i wielkich liter, cyfr oraz znaków specjalnych. Należy unikać haseł łatwych do przewidzenia, takich jak daty urodzenia, imiona dzieci czy sekwencje liczb. Uzupełnieniem tej metody jest tzw. uwierzytelnianie dwuskładnikowe (2FA – Two-Factor Authentication), które znacząco podnosi poziom bezpieczeństwa, wymagając oprócz hasła dodatkowego potwierdzenia tożsamości – np. kodu SMS, aplikacji autoryzacyjnej lub klucza sprzętowego (Diogenes, Ozkaya, 2020, s. 406).

Szyfrowanie danych to jedna z najskuteczniejszych metod zabezpieczenia informacji przed dostępem osób trzecich. Dzięki niemu nawet w przypadku przechwycenia danych, ich treść pozostaje nieczytelna bez odpowiedniego klucza deszyfrującego. Szyfrowaniu powinny podlegać zarówno dane przechowywane na urządzeniach, jak i przesyłane przez sieć. W tym kontekście warto także wspomnieć o wirtualnych sieciach prywatnych (VPN – Virtual Private Network), które maskują adres IP użytkownika i szyfrują cały ruch internetowy. Korzystanie z VPN szczególnie zalecane jest podczas łączenia się z publicznymi sieciami Wi-Fi, które często stanowią łatwy cel dla cyberprzestępców (Diogenes, Ozkaya, 2020, s. 406).

Nawet najbardziej zaawansowane rozwiązania techniczne nie przyniosą oczekiwanych rezultatów, jeśli użytkownicy nie będą świadomi zagrożeń oraz zasad bezpiecznego korzystania z technologii. Dlatego tak ważna jest edukacja cyfrowa – zarówno wśród dzieci i młodzieży, jak i dorosłych użytkowników. Do podstawowych zasad należą: ostrożność przy otwieraniu załączników i linków w wiadomościach e-mail, unikanie podawania danych osobowych na nieznanych stronach internetowych, regularna aktualizacja oprogramowania i korzystanie z legalnych źródeł aplikacji. Równie istotne jest uświadamianie użytkowników na temat ich praw wynikających z RODO oraz możliwości reagowania w przypadku naruszenia ich danych osobowych.

Urządzenia mobilne – smartfony i tablety – stały się nieodłączną częścią codziennego życia, a wraz z nimi pojawiły się nowe wektory zagrożeń. Podstawą ochrony danych na tych urządzeniach jest zabezpieczenie ich ekranów hasłem, PIN-em lub biometrią, regularne instalowanie aktualizacji oraz ograniczenie dostępu aplikacji do danych wrażliwych. Podobnie korzystanie z tzw. chmur wymaga zachowania ostrożności. Użytkownicy powinni wybierać zaufanych dostawców usług chmurowych, korzystać z szyfrowania plików przed ich wysłaniem oraz regularnie monitorować, kto ma dostęp do konkretnych danych i dokumentów.

Ochrona danych osobowych nie kończy się na sformułowaniu zasad i przyjęciu odpowiednich dokumentów prawnych. Kluczową rolę odgrywa egzekwowanie tych przepisów – zarówno na poziomie organizacyjnym, jak i indywidualnym. RODO, jak również ustawa o ochronie danych osobowych z dnia 10 maja 2018 r., jasno określają obowiązki, sankcje oraz instytucje nadzorujące przestrzeganie przepisów. Zasadnicze obszary odpowiedzialności: firm i organizacji, przypadki naruszeń oraz znaczenie funkcji Inspektora Ochrony Danych.

Na mocy art. 24 i 32 RODO, administratorzy danych osobowych są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodności przetwarzania z przepisami. Obejmuje to m.in. prowadzenie rejestrów czynności przetwarzania, ocenę skutków dla ochrony danych (DPIA), szyfrowanie, pseudonimizację, czy też zapewnienie ciągłości działania w razie incydentu (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Firmy i organizacje, które nie wywiązują się z obowiązków, podlegają odpowiedzialności administracyjnej, cywilnej i karnej. Zgodnie z art. 83 RODO, wysokość administracyjnych kar pieniężnych może sięgnąć do 20 milionów euro lub 4% całkowitego rocznego obrotu z poprzedniego roku obrotowego – w zależności od tego, która kwota jest wyższa (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). W polskim porządku prawnym kwestie te reguluje m.in.:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, która uzupełnia postanowienia RODO na poziomie krajowym,
- Kodeks cywilny, który umożliwia dochodzenie roszczeń z tytułu naruszenia dóbr osobistych, takich jak prywatność (art. 23 i 24 KC).

W praktyce naruszenia ochrony danych obejmują:

- nieuprawnione udostępnienie danych osobom trzecim,
- niezabezpieczone formularze kontaktowe lub bazy danych,
- przetwarzanie danych bez odpowiednich podstaw prawnych,
- niedopełnienie obowiązku informacyjnego wobec osób, których dane dotyczą (Bielak-Jomaa, Lubasz, 2018, s. 263).

Jednym z kluczowych elementów systemu odpowiedzialności w organizacjach przetwarzających dane jest funkcja Inspektora Ochrony Danych (IOD). Zgodnie z art. 37-39 RODO, wyznaczenie IOD jest obowiązkowe dla:

- podmiotów publicznych,
- podmiotów, których główna działalność polega na przetwarzaniu danych na dużą skalę.

Zadania IOD obejmują:

- informowanie i doradzanie administratorowi danych w zakresie obowiązków wynikających z RODO,
- monitorowanie zgodności przetwarzania z przepisami,
- współpracę z organem nadzorczym (UODO),
- pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą.

W praktyce IOD pełni rolę niezależnego strażnika danych, który nie tylko nadzoruje zgodność działań firmy z przepisami, ale również uczy pracowników, opiniuje procedury i ocenia ryzyka związane z przetwarzaniem danych (Lubasz, 2020, s. 345).

Ochrona danych osobowych jest procesem dynamicznym, który musi nadążać za tempem postępu technologicznego i zmieniającymi się realiami społecznymi. Choć podstawy prawne zostały ugruntowane na poziomie Unii Europejskiej (RODO), a także w krajowych regulacjach, to coraz częściej wskazuje się na konieczność aktualizacji i elastyczności przepisów. Przyszłość ochrony danych osobowych wiąże się ściśle z takimi zjawiskami jak rozwój sztucznej inteligencji, upowszechnienie danych biometrycznych, globalizacja przepływu informacji oraz skutki pandemii COVID-19, które przyspieszyły cyfryzację wielu sektorów życia.

Jednym z największych wyzwań dla sztucznej inteligencji są przepisy o ochronie danych osobowych. Duża część zastosowań sztucznej inteligencji

dotycz osób fizycznych, a tym samym wiąże się z przetwarzaniem ich danych osobowych.

Aby zapewnić zgodność z prawem przetwarzania danych osobowych w projektach AI, należy traktować je tak jak każdy inny projekt przetwarzania danych osobowych i stosować do niego zasady opisane w RODO. Nie jest to łatwe, ponieważ sposób w jaki są tworzone i funkcjonują algorytmy AI stoi w kontrze do zadań ochrony danych osobowych. AI nie tworzy scentralizowanej bazy danych, o której mówią przepisy, a tylko w takich bazach danych łatwo jest zidentyfikować administratorów danych. Technologia blockchain, która opiera się na architekturze rozproszonych baz danych i niezmienności zapisanych w niej informacji utrudnia np. realizowanie praw osób, których dotyczą dane np. prawa do sprostowania danych czy ich usunięcia. Tym samym obecnie nie ma jednego uniwersalnego rozwiązania, które sprawiłoby, że każdy blockchain byłby zgodny z RODO (Wittbrodt, Brodecki, Dargas-Draganik, 2024, s. 211).

Sztuczna inteligencja (AI), zwłaszcza w obszarze przetwarzania danych i uczenia maszynowego, może generować poważne ryzyka dla prywatności jednostek. Algorytmy uczące się na podstawie dużych zbiorów danych mogą nie tylko nieświadomie utrwalać uprzedzenia i dyskryminację, ale też naruszać zasadę minimalizacji danych czy ograniczenia celu ich przetwarzania (zgodnie z art. 5 RODO). Problemem staje się także tzw. „czarna skrzynka" algorytmów – brak przejrzystości i kontroli nad ich działaniem. Z tego względu coraz większego znaczenia nabierają zasady tzw. privacy by design oraz privacy by default, które nakładają obowiązek projektowania systemów z uwzględnieniem ochrony prywatności już na etapie ich tworzenia (Świerczyński, 2021).

Dane biometryczne, takie jak odciski palców, skan twarzy, głosu czy siatkówki oka, uznawane są za szczególną kategorię danych osobowych (art. 9 RODO). Ich przetwarzanie dopuszczalne jest tylko w ściśle określonych przypadkach, np. w kontekście bezpieczeństwa publicznego lub ochrony zdrowia. Jednocześnie są to dane niezwykle wrażliwe – ich utrata lub przejęcie może mieć nieodwracalne skutki, ponieważ w przeciwieństwie do hasła nie można ich zmienić. Z tego względu konieczne jest stosowanie najwyższych standardów bezpieczeństwa, w tym szyfrowania, a także prowadzenie ocen skutków dla ochrony danych (DPIA – Data Protection Impact Assessment).

Pandemia COVID-19 przyspieszyła cyfrową transformację – praca zdalna, e-usługi czy zdalna edukacja stały się powszechne. Wraz z tym wzrosła powierzchnia ataku cyberprzestępców. Wyzwania pojawiają się zarówno po stronie użytkowników indywidualnych (np. słabe zabezpieczenia domowych sieci Wi-Fi), jak i instytucji, które musiały błyskawicznie wdrażać nowe technologie. Ochrona danych w takim kontekście wymaga zintegrowanego podejścia do cyberbezpieczeństwa, w którym kluczowe są m.in. szkolenia, aktualizacje systemów, kontrola dostępu oraz świadomość zagrożeń. W świetle ustawy o krajowym systemie cyberbezpieczeństwa podmioty świadczące usługi kluczowe muszą spełniać konkretne obowiązki w zakresie zabezpieczenia informacji (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa).

Dane osobowe coraz częściej przekraczają granice państw - są przetwarzane na serwerach ulokowanych poza Unią Europejską, zwłaszcza w krajach, które nie zapewniają odpowiedniego poziomu ochrony (np. nie posiadają ekwiwalentnych regulacji jak RODO). W związku z tym unijne prawo (m.in. art. 44-49 RODO) przewiduje mechanizmy takie jak: decyzje o adekwatności Komisji Europejskiej, standardowe klauzule umowne czy wiążące reguły korporacyjne (BCR). Jednak globalizacja stawia pytania o skuteczność tych narzędzi, zwłaszcza wobec potęg technologicznych i państw, które gromadzą dane w celach nadzoru. Niezbędna wydaje się szersza współpraca międzynarodowa i harmonizacja standardów ochrony danych (Bielak-Jomaa, Lubasz, 2018, s. 905).

Podsumowanie

Upowszechnienie Internetu oraz dynamiczny rozwój technologii przetwarzania informacji – w tym nowych modeli, takich jak chmura obliczeniowa czy analizy Big Data - znacząco zwiększyły potrzebę wdrożenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni. Cyberprzestrzeń, ze swoim pozbawionym granic charakterem, iluzoryczną anonimowością i łatwością rozpowszechniania informacji, wymusza ponowną refleksję nad tym, czy obowiązujące normy prawne - często uchwalone w zupełnie innych realiach technologicznych – są dziś wystarczające i adekwatne wobec rosnących zagrożeń dla prywatności. Ochrona danych osobowych w cyberprzestrzeni to dziś nie tylko kwestia techniczna czy formalna – to

jeden z fundamentów zaufania społecznego oraz sprawnie funkcjonującego społeczeństwa informacyjnego. W dobie cyfrowej transformacji dane osobowe stały się walutą XXI wieku, a ich nadużycia prowadzą do poważnych konsekwencji zarówno dla jednostek, jak i całych instytucji. Podjęcie tematu w niniejszym opracowaniu miało na celu pokazanie złożoności zagadnienia, zwrócenie uwagi na najczęstsze zagrożenia, a także przybliżenie aktualnych rozwiązań prawnych i praktycznych metod ochrony danych:

- Dane osobowe stanowią dobro szczególnie chronione, a ich ochrona wpisuje się w konstytucyjne prawo do prywatności,
- Wprowadzenie RODO ujednoliciło zasady ochrony danych w krajach UE i znacznie zwiększyło odpowiedzialność podmiotów przetwarzających dane,
- W cyberprzestrzeni użytkownicy narażeni są na różnorodne formy ataków, takie jak phishing, wycieki danych, ransomware czy nadużycia w mediach społecznościowych,
- Ochrona danych wymaga zarówno narzędzi technologicznych (szyfrowanie, silne hasła, VPN), jak i ciągłego podnoszenia świadomości społecznej,
- Kluczową rolę pełnią firmy i organizacje – ich obowiązkiem jest nie tylko zabezpieczanie danych, ale także transparentne działania i edukacja użytkowników.

W dobie dzisiejszego świata, gdzie wykorzystywana jest sztuczna inteligencja (AI) i na niespotykaną skalę Internet, należy dążyć do zaleceń:

- Niezbędne jest prowadzenie szkoleń z zakresu cyberbezpieczeństwa – zarówno w sektorze publicznym, jak i prywatnym,
- Użytkownicy powinni korzystać z menedżerów haseł, dwuskładnikowego uwierzytelniania i unikać udostępniania danych na niesprawdzonych stronach,
- Instytucje powinny regularnie przeprowadzać audyty bezpieczeństwa oraz wdrażać polityki ochrony danych zgodne z RODO i ustawą krajową,
- Warto zwiększyć nakłady na edukację cyfrową – już od poziomu szkoły podstawowej – tak by kształtować kompetentnych i świadomych cyfrowo obywateli.

Bezpieczeństwo danych osobowych w dużej mierze zależy od decyzji podejmowanych przez samych użytkowników. To właśnie ich codzienne wybory – jak np. korzystanie z publicznych sieci Wi-Fi, nieaktualizowanie oprogramowania, kliknięcie w podejrzany link – mogą zadecydować o tym, czy dane pozostaną bezpieczne. W związku z tym, budowanie świadomości i odpowiedzialności cyfrowej powinno stać się jednym z priorytetów nie tylko polityki państwowej, ale także codziennego funkcjonowania w świecie on-line.

Literatura

1. Bakalarczyk-Burakowska, K., Nowicka, J. (2020). Ochrona danych osobowych w cyberprzestrzeni. W: Z. Ciekanowski (red.), *Współczesne zagrożenia bezpieczeństwa państwa. Część 1*. Państwowa Szkoła Wyższa im. Papieża Jana Pawła II, Biała Podlaska.
2. Bartnicki, A., Wojciechowski, Z., Zaskórski, P. (2020). *Analiza ryzyka i pseudonimizacja w systemie zabezpieczania danych osobowych cyberprzestrzeni*, *IV rewolucja przemysłowa. Mity, paradygmaty i zastosowania*, WAT, Warszawa.
3. Bielak-Jomaa, E., Lubasz, D. (2018). *Komentarz do RODO*, Wolters Kluwer, Warszawa.
4. Bielak-Jomaa, E., Lubasz, D. (2018). *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Wolters Kluwer, Warszawa.
5. Diogenes, Y., Ozkaya, E. (2023). *Cyberbezpieczeństwo. Strategie ataku i obrony*, Helion, Gliwice.
6. Dymek, M., Nycz, M., Gerka, A. (2016). *Analiza statycznych metod obrony przed atakami SQL Injection*, zeszyty Naukowe Politechniki Rzeszowskiej, Rzeszów.
7. Hadnagy, Ch., Fincher, M. (2016). *Mroczne odmęty phishingu. Nie daj się złowić!*, Helion, Gliwice.
8. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Uniwersytet Śląski, Katowice.
9. Lubasz, D. (2020). *Ochrona danych osobowych. Komentarz do przepisów RODO*, Wolters Kluwer, Warszawa.

10. Lubasz, D. (2013). *Techniczne, ekonomiczne i prawne uwarunkowania handlu elektronicznego, Handel elektroniczny. Bariery prawne*, LexisNexis, Warszawa.
11. Rojszczak, M. (2019). *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa.
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
13. Świerczyński, M. (2021). *Sztuczna inteligencja a ochrona danych osobowych*, Przegląd Prawa Publicznego, Uniwersytet Wrocławski, Wrocław.
14. Taczkowska-Olszewska, J., Chałubińska-Jentkiewicz, K., Nowikowska, M. (2019). *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Wolters Kluwer, Warszawa.
15. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.).
16. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.).
17. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. z 2018 r. poz. 1560 z późn. zm.).
18. Wasilewski, J. (2015). *Zarys definicyjny cyberprzestrzeni*, Zeszyty Naukowe (13/2025). Warszawska Wyższa Szkoła Informatyki, Warszawa.
19. Wittbrodt, E., Brodecki, Z,. Dargas-Draganik, M. (2024). *Przedwiośnie ery sztucznej inteligencji technologia – zarządzanie – prawo. Tom 2* , Uniwersytet Gdański, Gdańsk.

Tomasz Grudniewski[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

Karol Zygo[2]

Uniwersytet w Siedlcach

Sławomir Żurawski[3]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

https://doi.org/10.29316/9788368103359_7

CYBERTERRORYZM W ERZE ZAGROŻEŃ HYBRYDOWYCH

CYBERTERRORISM IN THE AGE OF HYBRID THREATS

Streszczenie

Rozdział podejmuje problematykę cyberterroryzmu jako jednego z kluczowych wyzwań współczesnego środowiska bezpieczeństwa międzynarodowego. W części pierwszej przedstawiono ewolucję pojęcia cyberterroryzmu oraz dokonano analizy najważniejszych podejść definicyjnych obecnych w literaturze przedmiotu, ze

[1] https://orcid.org/0000-0003-3394-8992, e-mail: t.grudniewski@dyd.akademiabialska.pl
[2] https://orcid.org/0000-0002-8274-1958, e-mail: karolzygo@interia.pl
[3] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl

szczególnym uwzględnieniem trudności w rozróżnieniu cyberterroryzmu od cyberprzestępczości, hacktywizmu i cyberwojny. Część druga poświęcona została identyfikacji głównych aktorów cyberterroryzmu oraz omówieniu metod działań stosowanych we współczesnej cyberprzestrzeni, w tym ataków na infrastrukturę krytyczną, operacji informacyjnych oraz wykorzystania oprogramowania ransomware. W części trzeciej cyberterroryzm ukazano jako element zagrożeń hybrydowych oraz przeanalizowano jego znaczenie dla bezpieczeństwa międzynarodowego, ze szczególnym uwzględnieniem problemu atrybucji oraz podatności państw demokratycznych na tego rodzaju oddziaływania. Problem badawczy rozdziału sformułowano: czy cyberterroryzm we współczesnym środowisku bezpieczeństwa funkcjonuje jako autonomiczne zjawisko, czy też stanowi narzędzie wykorzystywane w ramach szerszego spektrum zagrożeń hybrydowych? Hipoteza badawcza zakłada, że cyberterroryzm nie występuje obecnie jako samodzielna forma zagrożenia, lecz pełni funkcję narzędzia strategicznego oddziaływania w działaniach hybrydowych, którego skuteczność opiera się przede wszystkim na generowaniu efektów psychologicznych, społecznych i politycznych, a nie na bezpośrednim niszczeniu infrastruktury teleinformatycznej. W badaniach zastosowano metodę analizy jakościowej, obejmującą krytyczną analizę literatury przedmiotu, dokumentów strategicznych organizacji międzynarodowych, aktów prawnych Unii Europejskiej oraz raportów instytucji zajmujących się bezpieczeństwem cybernetycznym. Przeprowadzona analiza potwierdza zasadność przyjętej hipotezy oraz wskazuje na potrzebę dalszych badań nad cyberterroryzmem w kontekście zagrożeń hybrydowych.

Słowa kluczowe: bezpieczeństwo, cyberterroryzm, hybrydowość, bezpieczeństwo międzynarodowe

Abstract

The chapter addresses the issue of cyberterrorism as one of the key challenges of the contemporary international security environment. The first part presents the evolution of the concept of cyberterrorism and analyses the most important definitional approaches present in the literature on the subject, with particular emphasis on the difficulties in distinguishing cyberterrorism from cybercrime, hacktivism and cyberwar. The second part was devoted to the identification of the main actors of cyberterrorism and the discussion of methods of action used in modern cyberspace, including attacks on critical infrastructure, information operations and the use of ransomware. The third part shows cyberterrorism as an element of hybrid threats and analyses its significance for international security, with particular emphasis on the problem of attribution and the vulnerability of democratic states to such influences.

The research problem of the chapter is formulated: does cyberterrorism in the modern security environment function as an autonomous phenomenon, or is it a tool used within a wider spectrum of hybrid threats? The research hypothesis assumes that cyberterrorism does not currently exist as an independent form of threat, but serves as a tool of strategic influence in hybrid operations, the effectiveness of which is based primarily on generating psychological, social and political effects, and not on the direct destruction of ICT infrastructure. The research used the method of qualitative analysis, including a critical analysis of the literature on the subject, strategic documents of international organizations, legal acts of the European Union and reports of institutions dealing with cyber security. The analysis confirms the legitimacy of the adopted hypothesis and indicates the need for further research on cyberterrorism in the context of hybrid threats.

Keywords: security, cyberterrorism, hybridity, international security

Wstęp

Dynamiczny rozwój technologii informacyjnych oraz powszechna cyfryzacja życia społecznego, gospodarczego i politycznego sprawiły, że cyberprzestrzeń stała się jednym z kluczowych obszarów funkcjonowania współczesnych państw. Systemy teleinformatyczne odpowiadają obecnie za prawidłowe działanie infrastruktury krytycznej, administracji publicznej, sektora finansowego, energetycznego oraz transportowego. Wraz ze wzrostem zależności od technologii cyfrowych pojawiły się nowe formy zagrożeń, których charakter wykracza poza tradycyjnie rozumiane konflikty zbrojne.

Jednym z najbardziej złożonych i trudnych do jednoznacznego zdefiniowania zagrożeń jest cyberterroryzm. Pojęcie to funkcjonuje w literaturze przedmiotu od kilku dekad, jednak do dziś nie wypracowano jednej, powszechnie akceptowanej definicji. Wczesne ujęcia cyberterroryzmu koncentrowały się głównie na technicznych aspektach ataków na systemy informatyczne oraz na potencjalnych skutkach materialnych takich działań. Współczesne środowisko bezpieczeństwa, zdominowane przez zagrożenia hybrydowe, wymusza jednak szersze i bardziej kompleksowe spojrzenie na to zjawisko.

Cyberterroryzm coraz częściej nie występuje jako autonomiczna forma przemocy, lecz jako element złożonych operacji obejmujących działania informacyjne, dezinformacyjne oraz presję psychologiczną. Granice pomiędzy cyberterroryzmem, cyberwojną, cyberprzestępczością czy hacktywizmem ulegają zatarciu, co znacząco utrudnia identyfikację sprawców oraz reakcję państw i organizacji międzynarodowych. Celem niniejszego rozdziału jest wykazanie, że cyberterroryzm należy postrzegać przede wszystkim jako narzędzie strategicznego oddziaływania, którego skuteczność opiera się na destabilizacji społecznej i politycznej, a nie wyłącznie na technicznym zniszczeniu systemów.

Cyberterroryzm – współczesne podejścia definicyjne

Pojęcie cyberterroryzmu pojawiło się w literaturze naukowej pod koniec XX wieku wraz z gwałtownym rozwojem technologii informacyjnych oraz upowszechnieniem Internetu. Wczesne próby jego definiowania były silnie inspirowane klasycznymi teoriami terroryzmu i koncentrowały się na przeniesieniu znanych mechanizmów przemocy politycznej do nowej domeny, jaką stała się cyberprzestrzeń. Jednym z pierwszych badaczy, którzy podjęli próbę konceptualizacji tego zjawiska, był Barry Collin, wskazujący na cyberterroryzm jako formę wykorzystania systemów komputerowych do realizacji celów terrorystycznych (Collin, 1997).

W klasycznych ujęciach cyberterroryzm definiowano przede wszystkim jako politycznie lub ideologicznie motywowane ataki na systemy informatyczne, których celem było zastraszenie społeczeństwa lub wymuszenie określonych decyzji na rządach. Takie podejście wskazuje, że aby dane działanie mogło zostać zakwalifikowane jako cyberterroryzm, musi ono prowadzić do realnego strachu, porównywalnego ze skutkami tradycyjnych aktów terrorystycznych. W tym ujęciu cyberterroryzm odróżniano zarówno od cyberprzestępczości, jak i od zwykłych incydentów bezpieczeństwa teleinformatycznego (Denning, 2000, s. 10).

Jednocześnie już na wczesnym etapie rozwoju badań nad cyberterroryzmem zaczęto wskazywać na trudności definicyjne wynikające z niematerialnego charakteru cyberprzestrzeni oraz problemu oceny skutków ataków. W przeciwieństwie do klasycznych aktów terrorystycznych, cyberataki rzadko prowadzą do bezpośrednich ofiar śmiertelnych, co rodzi pytania

o zasadność stosowania terminu „terroryzm" w odniesieniu do działań prowadzonych wyłącznie w cyberprzestrzeni (https://www.unodc.org).

Współczesne podejścia definicyjne coraz częściej odchodzą od wyłącznie technicznego rozumienia cyberterroryzmu. Badacze zwracają uwagę, że istotą tego zjawiska nie jest sam atak na system informatyczny, lecz intencja oraz efekt oddziaływania społecznego i politycznego. Wskazuje się, że wiele działań określanych mianem cyberterroryzmu nie spełnia klasycznych kryteriów terroryzmu, jednak ich znaczenie strategiczne polega na destabilizacji, podważaniu zaufania do instytucji państwowych oraz wzmacnianiu poczucia zagrożenia (Rid, 2013, s. 14). Na tym tle szczególnie istotne staje się rozróżnienie cyberterroryzmu od zjawisk pokrewnych, takich jak cyberprzestępczość, hacktywizm czy cyberwojna. Cyberprzestępczość, zgodnie z definicjami stosowanymi przez Europol i ONZ, ma charakter przede wszystkim ekonomiczny i nastawiona jest na osiąganie zysków finansowych[5]. Hacktywizm natomiast, choć często motywowany ideologicznie, ma zazwyczaj charakter symboliczny i rzadko prowadzi do trwałego zastraszenia społeczeństwa.

Najwięcej kontrowersji budzi relacja pomiędzy cyberterroryzmem a cyberwojną. Cyberwojna jest zazwyczaj wiązana z działaniami prowadzonymi przez państwa lub podmioty działające na ich rzecz w ramach konfliktów zbrojnych lub rywalizacji strategicznej (https://www.nato.int). W praktyce jednak wiele działań w cyberprzestrzeni realizowanych jest przez aktorów pośrednich (proxy actors), co prowadzi do zatarcia granic pomiędzy terroryzmem a działaniami państwowymi. Problem ten jest szeroko omawiany w dokumentach NATO oraz Unii Europejskiej dotyczących zagrożeń hybrydowych (https://www.consilium.europa.eu).

Współczesne instytucje międzynarodowe coraz częściej unikają jednoznacznego definiowania cyberterroryzmu, koncentrując się zamiast tego na funkcjonalnym opisie zagrożeń. Przykładem jest podejście Unii Europejskiej, która w dokumentach strategicznych dotyczących bezpieczeństwa cybernetycznego i zagrożeń hybrydowych wskazuje na potrzebę wzmacniania odporności systemów i społeczeństw, niezależnie od formalnej kwalifikacji danego incydentu. Podobne stanowisko prezentuje Organizacja Narodów Zjednoczonych, akcentując znaczenie współpracy międzynarodowej i budowania zdolności reagowania.

Podsumowując, ewolucja pojęcia cyberterroryzmu prowadzi od wąskiego, technicznego ujęcia ku rozumieniu tego zjawiska jako narzędzia strategicznego oddziaływania. Współczesny cyberterroryzm nie musi prowadzić do fizycznego zniszczenia infrastruktury, aby osiągnąć swoje cele. Jego skuteczność opiera się na destabilizacji, chaosie informacyjnym oraz presji psychologicznej, co czyni go szczególnie niebezpiecznym elementem współczesnych zagrożeń hybrydowych.

Aktorzy i metody cyberterroryzmu we współczesnym środowisku bezpieczeństwa

Współczesny cyberterroryzm charakteryzuje się znacznym zróżnicowaniem aktorów oraz metod działań, co odróżnia go od klasycznych form terroryzmu. Rozwój cyberprzestrzeni, niski próg wejścia technologicznego oraz globalny zasięg Internetu sprawiają, że działania o charakterze cyberterrorystycznym mogą być prowadzone zarówno przez zorganizowane struktury, jak i przez pojedyncze osoby. W literaturze przedmiotu coraz częściej podkreśla się, że cyberterroryzm nie jest już domeną wyłącznie klasycznych organizacji terrorystycznych, lecz elementem szerszego spektrum aktywności niepaństwowych w cyberprzestrzeni (Kowalewski, Kowalewski, 2014, s. 25).

Do pierwszej kategorii aktorów zalicza się organizacje terrorystyczne, które wykorzystują cyberprzestrzeń przede wszystkim jako narzędzie wsparcia swojej działalności. Jak wskazują raporty Europolu (Europol, 2025), Internet odgrywa kluczową rolę w propagandzie, rekrutacji, komunikacji wewnętrznej oraz pozyskiwaniu środków finansowych. Choć bezpośrednie cyberataki prowadzone przez tego typu organizacje są stosunkowo rzadkie, ich aktywność w sferze informacyjnej i psychologicznej może generować efekty porównywalne z klasycznymi aktami terroru.

Drugą, coraz istotniejszą grupą aktorów są podmioty niepaństwowe działające jako aktorzy pośredni (proxy actors). Są to grupy lub jednostki, które formalnie nie są powiązane z żadnym państwem, lecz w praktyce realizują działania zbieżne z interesami określonych aktorów państwowych. Zjawisko to jest szeroko analizowane w kontekście zagrożeń hybrydowych, gdzie cyberterroryzm może pełnić funkcję narzędzia destabilizacji bez jednoznacznego przypisania odpowiedzialności. Tego rodzaju działania

znacząco utrudniają reakcję prawną i polityczną na poziomie międzynarodowym (Jokinen, Normark, 2022, s. 5).

Szczególną kategorię stanowią samotni aktorzy (lone actors), którzy dzięki powszechnemu dostępowi do narzędzi informatycznych są w stanie prowadzić działania o charakterze destabilizującym bez zaplecza organizacyjnego. Jak wskazują analizy The European Union Agency for Cybersecurity (ENISA), niska bariera wejścia sprawia, że nawet osoby o ograniczonych kompetencjach technicznych mogą wykorzystywać gotowe narzędzia do przeprowadzania ataków lub kampanii dezinformacyjnych. W tym kontekście cyberterroryzm staje się zjawiskiem trudnym do przewidzenia i monitorowania (ENISA, 2023).

Jeśli chodzi o metody działań, współczesny cyberterroryzm obejmuje szerokie spektrum technik, które nie ograniczają się do klasycznych ataków na systemy informatyczne. Jednym z najczęściej wskazywanych obszarów są ataki na infrastrukturę krytyczną, w tym systemy energetyczne, transportowe, wodociągowe oraz telekomunikacyjne. Raporty instytucji międzynarodowych podkreślają, że nawet krótkotrwałe zakłócenia w funkcjonowaniu takich systemów mogą prowadzić do poważnych skutków społecznych i politycznych. Coraz większe znaczenie zyskują również operacje informacyjne i dezinformacyjne, które stanowią istotny element współczesnych działań cyberterrorystycznych. Ich celem nie jest fizyczne zniszczenie infrastruktury, lecz manipulowanie percepcją społeczną, pogłębianie podziałów oraz podważanie zaufania do instytucji publicznych. Działania informacyjne w cyberprzestrzeni są często integralną częścią szerszych operacji hybrydowych, w których cyberterroryzm pełni rolę katalizatora destabilizacji. Szczególnym narzędziem współczesnego cyberterroryzmu stało się oprogramowanie ransomware. Choć ransomware jest najczęściej klasyfikowane jako forma cyberprzestępczości, w określonych kontekstach może pełnić funkcję narzędzia terroru, zwłaszcza gdy jego celem jest sparaliżowanie funkcjonowania instytucji publicznych lub infrastruktury krytycznej. Ataki tego typu mogą prowadzić do efektu zastraszenia znacznie wykraczającego poza wymiar ekonomiczny (Stodolnik, 2025).

Warto również zwrócić uwagę na rosnącą rolę automatyzacji i sztucznej inteligencji w działaniach cyberterrorystycznych. Narzędzia oparte na algorytmach uczenia maszynowego mogą być wykorzystywane do automatyzacji ataków, generowania treści dezinformacyjnych czy analizy

podatności systemów. ENISA podkreśla, że rozwój tych technologii zwiększa skalę i tempo potencjalnych działań cyberterrorystycznych, jednocześnie utrudniając ich wykrywanie.

Podsumowując, współczesny cyberterroryzm charakteryzuje się dużą elastycznością oraz zdolnością adaptacji do zmieniającego się środowiska bezpieczeństwa. Zarówno zróżnicowanie aktorów, jak i ewolucja metod działań sprawiają, że cyberterroryzm stanowi istotne wyzwanie dla państw i organizacji międzynarodowych. Jego skuteczność opiera się nie na skali technicznego zniszczenia, lecz na zdolności do generowania długotrwałych skutków psychologicznych, społecznych i politycznych.

Cyberterroryzm jako element zagrożeń hybrydowych i wyzwanie dla bezpieczeństwa międzynarodowego

Współczesne środowisko bezpieczeństwa międzynarodowego charakteryzuje się rosnącą rolą zagrożeń hybrydowych, które łączą działania militarne i niemilitarne, jawne i skryte, państwowe i niepaństwowe. W tym kontekście cyberterroryzm należy postrzegać nie jako zjawisko izolowane, lecz jako jeden z instrumentów szerszego spektrum oddziaływań strategicznych. Jego znaczenie wynika przede wszystkim z możliwości prowadzenia działań destabilizujących bez formalnego wypowiadania wojny oraz przy zachowaniu wysokiego poziomu niejednoznaczności co do tożsamości sprawcy.

Zagrożenia hybrydowe definiowane są w dokumentach Unii Europejskiej oraz NATO jako działania wykorzystujące jednocześnie różne środki nacisku – polityczne, ekonomiczne, informacyjne, cybernetyczne i militarne – w celu osłabienia państwa przeciwnika. Cyberterroryzm doskonale wpisuje się w tę logikę, ponieważ umożliwia oddziaływanie na funkcjonowanie państwa i społeczeństwa bez konieczności użycia siły kinetycznej. Jego skuteczność opiera się na połączeniu cyberataków z operacjami informacyjnymi oraz dezinformacyjnymi, które wzmacniają efekt psychologiczny i społeczny.

Jednym z kluczowych problemów związanych z cyberterroryzmem w kontekście bezpieczeństwa międzynarodowego jest kwestia atrybucji, czyli jednoznacznego przypisania odpowiedzialności za dane działanie. W cyberprzestrzeni identyfikacja sprawcy jest szczególnie trudna ze względu na możliwość maskowania pochodzenia ataków, wykorzystywania

serwerów pośredniczących oraz działania aktorów proxy. Problem atrybucji stanowi jedno z głównych ograniczeń skutecznej reakcji państw na zagrożenia cybernetyczne. W przypadku cyberterroryzmu niejednoznaczność ta może być wykorzystywana celowo w celu eskalacji napięć lub destabilizacji relacji międzynarodowych (Derian-Toth, Walsh, Sergueeva, Kim, Coon, Hadan, Stancombe, 2021, s. 7).

Cyberterroryzm stanowi szczególne wyzwanie dla państw demokratycznych, które opierają swoje funkcjonowanie na otwartych systemach informacyjnych, wolności słowa oraz zaufaniu społecznym. Działania cyberterrorystyczne mogą prowadzić do erozji zaufania obywateli do instytucji publicznych, podważania legitymacji władzy oraz wzmacniania polaryzacji społecznej. Odporność społeczeństw demokratycznych staje się kluczowym elementem przeciwdziałania zagrożeniom hybrydowym, w tym cyberterroryzmowi.

W odpowiedzi na rosnące zagrożenia cybernetyczne organizacje międzynarodowe podejmują działania mające na celu wzmocnienie zdolności państw do zapobiegania i reagowania na cyberataki. Unia Europejska rozwija ramy prawne i instytucjonalne w zakresie cyberbezpieczeństwa, czego przykładem jest dyrektywa NIS2, nakładająca na państwa członkowskie obowiązek wzmacniania odporności infrastruktury krytycznej oraz systemów informacyjnych. Działania te mają pośrednio ograniczać skuteczność cyberterroryzmu poprzez podniesienie poziomu zabezpieczeń i zdolności reagowania (Dyrektywa NIS2).

Równie istotną rolę odgrywa Organizacja Narodów Zjednoczonych, która koncentruje się na budowaniu norm odpowiedzialnego zachowania państw w cyberprzestrzeni oraz na wspieraniu współpracy międzynarodowej. W dokumentach ONZ podkreśla się, że cyberzagrożenia, w tym cyberterroryzm, mogą stanowić zagrożenie dla pokoju i bezpieczeństwa międzynarodowego, nawet jeśli nie prowadzą bezpośrednio do konfliktu zbrojnego. W tym ujęciu cyberterroryzm traktowany jest jako element szerszego problemu bezpieczeństwa globalnego.

Istotnym aspektem cyberterroryzmu jako zagrożenia hybrydowego jest również jego niski koszt prowadzenia działań w porównaniu z klasycznymi formami konfliktu. Relatywnie niewielkie nakłady finansowe mogą prowadzić do nieproporcjonalnie dużych skutków politycznych i społecznych. Z tego względu cyberterroryzm stanowi atrakcyjne narzędzie dla

aktorów dysponujących ograniczonymi zasobami, a jednocześnie dążących do wywarcia presji na silniejsze państwa (Nye, 2017, s. 44-46).

Podsumowując, cyberterroryzm jako element zagrożeń hybrydowych stanowi poważne wyzwanie dla współczesnego bezpieczeństwa międzynarodowego. Jego specyfika polega na połączeniu działań cybernetycznych z oddziaływaniem informacyjnym i psychologicznym, co utrudnia zarówno identyfikację sprawców, jak i skuteczną reakcję. Przeciwdziałanie cyberterroryzmowi wymaga zatem nie tylko rozwoju zdolności technicznych, lecz także wzmocnienia odporności instytucjonalnej i społecznej oraz pogłębionej współpracy międzynarodowej.

Podsumowanie

Przeprowadzona w rozdziale analiza pozwala stwierdzić, że cyberterroryzm stanowi jedno z najbardziej złożonych i dynamicznie ewoluujących zagrożeń współczesnego środowiska bezpieczeństwa. Jego istota nie sprowadza się wyłącznie do technicznych ataków na systemy informatyczne, lecz obejmuje znacznie szerszy wymiar oddziaływania politycznego, psychologicznego i informacyjnego. W tym sensie cyberterroryzm należy postrzegać jako narzędzie strategicznego wpływu, którego skuteczność opiera się na destabilizacji funkcjonowania państw i społeczeństw, a niekoniecznie na fizycznym zniszczeniu infrastruktury.

Analiza ewolucji pojęcia cyberterroryzmu wskazuje, że klasyczne definicje, wypracowane na przełomie XX i XXI wieku, coraz częściej okazują się niewystarczające wobec współczesnych realiów. Wczesne ujęcia, koncentrujące się na analogii do tradycyjnych aktów terrorystycznych, nie uwzględniały w pełni specyfiki cyberprzestrzeni jako domeny niematerialnej, transgranicznej i trudnej do jednoznacznej kontroli. Współczesne podejścia definicyjne przesuwają akcent z samego aktu cyberataku na jego intencję oraz efekt oddziaływania społecznego, co pozwala lepiej uchwycić istotę cyberterroryzmu jako zjawiska politycznego i strategicznego.

Rozważania dotyczące aktorów i metod cyberterroryzmu potwierdzają, że zjawisko to nie jest ograniczone do działalności klasycznych organizacji terrorystycznych. Coraz większą rolę odgrywają aktorzy niepaństwowi działający pośrednio, a także samotni sprawcy, wykorzystujący powszechnie dostępne narzędzia cyfrowe. Zróżnicowanie podmiotów oraz

niski próg wejścia sprawiają, że cyberterroryzm staje się trudny do przewidzenia i skutecznego zwalczania. Jednocześnie ewolucja metod działań, obejmująca ataki na infrastrukturę krytyczną, operacje dezinformacyjne, ransomware oraz wykorzystanie automatyzacji i sztucznej inteligencji, wskazuje na rosnące znaczenie efektu psychologicznego i informacyjnego jako kluczowego elementu oddziaływania.

Umiejscowienie cyberterroryzmu w kontekście zagrożeń hybrydowych pozwala lepiej zrozumieć jego rolę w architekturze bezpieczeństwa międzynarodowego. Cyberterroryzm funkcjonuje jako narzędzie umożliwiające prowadzenie działań destabilizujących poniżej progu wojny, często bez jednoznacznego przypisania odpowiedzialności. Problem atrybucji, charakterystyczny dla cyberprzestrzeni, znacząco ogranicza możliwości reakcji państw i organizacji międzynarodowych, co czyni cyberterroryzm szczególnie atrakcyjnym środkiem oddziaływania asymetrycznego. Wyniki analizy wskazują również, że państwa demokratyczne są szczególnie podatne na skutki cyberterroryzmu. Otwartość systemów informacyjnych, znaczenie opinii publicznej oraz wysoki poziom cyfryzacji sprzyjają skuteczności działań wymierzonych w zaufanie społeczne i stabilność instytucjonalną. W tym kontekście cyberterroryzm stanowi wyzwanie nie tylko dla bezpieczeństwa technicznego, lecz także dla spójności społecznej i odporności politycznej państw. Podsumowując, cyberterroryzm należy postrzegać jako trwały element współczesnego środowiska bezpieczeństwa, którego znaczenie będzie rosło wraz z dalszym rozwojem technologii informacyjnych oraz pogłębianiem się procesów cyfryzacji. Skuteczne przeciwdziałanie temu zjawisku wymaga podejścia wielowymiarowego, łączącego środki techniczne, prawne, organizacyjne i edukacyjne, a także intensyfikacji współpracy międzynarodowej. Dalsze badania nad cyberterroryzmem powinny koncentrować się na doprecyzowaniu ram pojęciowych, analizie mechanizmów oddziaływania psychologicznego oraz wypracowaniu skutecznych modeli reagowania, adekwatnych do realiów zagrożeń hybrydowych XXI wieku.

Literatura

1. Collin B. (1997). *The Future of Cyberterrorism*. Hanover: Institute for Security Technology Studies, Dartmouth College.

2. Countering hybrid threats. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (dostęp: 20.03.2026).
3. Cyber defense. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
4. Cyberterrorism. Pobrano z: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html (dostęp: 20.03.2026).
5. Denning, D. E. (2000). *Cyberterrorism: Testimony before the U.S. House of Representatives*. Washington D.C: United States House of Representatives.
6. Derian-Toth, G., Walsh, R., Sergueeva, A., Kim, E., Coon, A., Hadan, H., Stancombe, J. (2021). *Opportunities for Public and Private Attribution of Cyber Operations*, TALLINN PAPERS YOUNG SCHOLAR EDITION, Nr 12, Tallin.
7. Developments in the field of information and telecommunications in the context of international security. Pobrano z: https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context (dostęp: 20.03.2026).
8. Dyrektywa NIS2. Pobrano z: https://eur-lex.europa.eu/eli/dir/2022/2555 (dostęp: 20.03.2026).
9. European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*, Luksemburg 2023.
10. Europol, *European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT)* Publications Office of the European Union, Luksemburg 2025.
11. Hybrid threats. Pobrano z: https://www.consilium.europa.eu/en/policies/hybrid-threats/?utm_source (dostęp: 20.03.2026).
12. Jokinen, J., Normark, M. (2022). *Hybrid threats from non-state actors: A taxonomy***,** Helskinki: The European Centre of Excellence for Countering Hybrid Threats.
13. Kowalewski, J., Kowalewski, M. (2014). Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa. *Telekomunikacja i Techniki Informacyjne*, (1-2), 24-32.
14. Nye Jr, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

15. Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford-New York: Oxford University Press.
16. Stodolnik, M. (2025). Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation. *Terroryzm – studia, analizy, prewencja*", Special Issue, 225-248.

Marta Chodyka[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

Sławomir Żurawski[2]

Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

Marcin Oskierko[3]

Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103359_8

CYBERTERRORYZM JAKO ZAGROŻENIE BEZPIECZEŃSTWA PAŃSTWA W ŚRODOWISKU CYFROWYM

CYBERTERRORISM AS A THREAT TO NATIONAL SECURITY IN THE DIGITAL ENVIRONMENT

Streszczenie

Celem niniejszego rozdziału jest analiza cyberterroryzmu jako zagrożenia bezpieczeństwa państwa w środowisku cyfrowym oraz identyfikacja jego uwarunkowań, mechanizmów oddziaływania i sposobów przeciwdziałania. Problem badawczy

[1] https://orcid.org/0000-0002-8819-2451, e-mail: m.chodyka@dyd.akademiabialska.pl
[2] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl
[3] https://orcid.org/0000-0003-3450-6037, e-mail: moskierko@panschelm.edu.pl

sformułowano: w jakim stopniu cyberterroryzm wpływa na poziom bezpieczeństwa państwa oraz jakie działania podejmowane są w celu ograniczenia skutków tego zjawiska. Przyjęto hipotezę badawczą zakładającą, że cyberterroryzm stanowi jedno z najistotniejszych zagrożeń asymetrycznych współczesnych państw, a skuteczność przeciwdziałania temu zjawisku zależy od integracji działań instytucjonalnych, prawnych i technologicznych. W opracowaniu zastosowano metodę analizy literatury przedmiotu, analizę dokumentów strategicznych oraz metodę analizy systemowej, co pozwoliło na kompleksowe ujęcie problematyki cyberterroryzmu w kontekście bezpieczeństwa państwa. Przedstawione rozważania mają na celu ukazanie charakteru i skali współczesnych zagrożeń w cyberprzestrzeni oraz wskazanie kierunków rozwoju systemów ochrony państwa przed cyberterroryzmem.

Słowa kluczowe: bezpieczeństwo, cyberterroryzm, środowisko cyfrowe, zagrożenia

Abstract

The aim of this chapter is to analyze cyberterrorism as a threat to state security in the digital environment and to identify its conditions, mechanisms of impact and ways of counteracting. The research problem was formulated: to what extent does cyberterrorism affect the level of national security and what actions are taken to limit the effects of this phenomenon. A research hypothesis was adopted assuming that cyberterrorism is one of the most important asymmetric threats of modern states, and the effectiveness of counteracting this phenomenon depends on the integration of institutional, legal and technological activities. The study uses the method of literature analysis, analysis of strategic documents and the method of system analysis, which allowed for a comprehensive approach to the issue of cyberterrorism in the context of state security. The presented considerations are aimed at showing the nature and scale of contemporary threats in cyberspace and indicating the directions of development of state protection systems against cyberterrorism.

Keywords: security, cyberterrorism, digital environment, threats

Pojęcie cyberterroryzmu

Na przestrzeni ostatnich lat rozwinął się postęp technologiczny, postęp w procesach wytwarzania, przetwarzania i przekazywania informacji. Społeczeństwo uzależnia się od technologii informacyjnej, co sprawia, że staje ono w obliczu wzrastającego zagrożenia jakim jest cyberterroryzm.

Cyberterroryzm jest pojęciem wieloaspektowym. Stanowi jedno z trzech głównych wyzwań i zagrożeń dla bezpieczeństwa teleinformatycznego w wymiarze narodowym i międzynarodowym oraz jest zjawiskiem o dynamicznie narastającej charakterystyce. Cyberterroryzm powstał na podstawie terroryzmu z wykorzystaniem obszaru jakim jest cyberprzestrzeń, a także jest zjawiskiem z pogranicza innych obszarów, takich jak:

- bezpieczeństwo teleinformatyczne,
- technologie informatyczne i teleinformacyjne,
- bezpieczeństwo osobowe,
- bezpieczeństwo fizyczne,
- regulacje prawne narodowe i międzynarodowe,
- dane osobowe (Białoskórski, 2011).

Termin cyberterroryzm nie posiada jednoznacznej definicji zawierającej charakterystykę przedmiotu. W literaturze podjęto wiele prób definiowania cyberterroryzmu i do tej pory nie udało się jego zdefiniować. Terminu cyberterroryzm pojawił się po raz pierwszy w 1979 roku w Szwecji, w raporcie szwedzkiego ministerstwa obrony na temat zagrożeń komputerowych, w odniesieniu do destrukcyjnego wykorzystywania komputerów, który miał na celu niszczenia systemów teleinformatycznych, danych w nich przechowywanych, oprogramowania, a w konsekwencji w celu zastraszania rządów i społeczeństwa, wywierania presji psychologicznej, doprowadzenie do zagrożenia życia lub znacznych start materialnych. W tym samym czasie termin ten używany był przez amerykańskich specjalistów w dziedzinie wywiadu wojskowego.

Pierwszą próbę sformułowania pojęcia cyberterroryzmu podjął się Barry Collin w latach 80. XX wieku. Według niego to *„świadome wykorzystywanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji”*. Cyberterroryzm przyjmuje formę ataków przeprowadzanych w cyberprzestrzeni przy pomocy komputerów na zasoby przeciwnika. Do najczęściej spotykanych definicji cyberterroryzmu należą:

- Dorothy Denning: „cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanych w nich, by zastraszyć lub wymusić na rządzie lub

społeczeństwie polityczne lub społeczne cele. By zakwalifikować atak jako cyberterroryzm powinien skutkować przemocą przeciwko ludziom lub mieniu lub przynajmniej wyrządzić wystarczająco szkody by stwarzać strach",

- James Lewis: „(...) wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe, itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań",
- US National Infrastructure Protection Centre: „(...) akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i / lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu",
- US Federal Bureau of Investigation: „(...) jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne",
- M. Pollitt z George Washington University: „(...) jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe" (Szybrycht, 2005).

W powyższych definicjach można zauważyć pojawiające się w nich dwa zasadnicze wyróżniki, a mianowicie:

- uwzględniają istnienie możliwości wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku cybernetycznego,
- komputery i systemy informacyjne są celem takiego ataku (Yannakogeorgos, 2014).

Rozważając znaczenie pojęcia cyberterroryzm należy zauważyć, że cyberterroryzm to coś więcej aniżeli przedrostek rodzajowy zestawiony ze standardową aktywnością o charakterze terrorystycznym (Yannakogeorgos, 2014).

W dokumentach instytucji Unii Europejskiej pojęcie cyberterroryzmu nie zawsze funkcjonuje jako jedna, zamknięta definicja, jednak jest ono interpretowane poprzez regulacje dotyczące terroryzmu oraz cyberprzestępczości. Zgodnie z podejściem Unii Europejskiej cyberterroryzm można rozumieć jako działania terrorystyczne prowadzone z wykorzystaniem systemów teleinformatycznych lub skierowane przeciwko infrastrukturze cyfrowej w celu wywołania poważnych zakłóceń w funkcjonowaniu państwa, społeczeństwa lub gospodarki. Jednym z kluczowych aktów prawnych UE odnoszących się do tej problematyki jest Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 w sprawie zwalczania terroryzmu. Dokument ten wskazuje, że przestępstwa terrorystyczne obejmują działania polegające m.in. na: *„poważnym zakłóceniu lub zniszczeniu infrastruktury, w tym systemów informatycznych, które mogą narazić życie ludzkie lub spowodować poważne straty gospodarcze”* (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu, 2017).

Polskie prawo karne za działania o charakterze terrorystycznym przewiduje dla sprawcy karę pozbawienia wolności co najmniej 5 lat, jeśli dopuścił się on czynu mającego na celu:

- poważne zastraszenie wielu osób,
- zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
- wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej,
- innego państwa czy organizacji międzynarodowej (Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, 1997).

Analizując szereg różnorodnych definicji cyberterroryzmu można zaobserwować, że wszystkie definicje sprowadzają się do jednego wspólnego elementu, a mianowicie cyberterroryzm występuje wtedy, kiedy

mamy do czynienia z politycznie motywowanym atakiem z użyciem sieci teleinformatycznych.

Obszary oddziaływania cyberterroryzmu na bezpieczeństwo państwa

Obiektami i obszarami atakowanymi przez cyberterrorystów może być infrastruktura krytyczna państw, wspólnot i różnego rodzaju organizacje, czyli innymi słowy systemy, funkcjonalne obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Typologia zaproponowana przez Thomasa R. Mockaitisa wskazuje, że działania cyberterrorystyczne mogą być realizowane przez różnorodne podmioty, w tym państwa prowadzące operacje w cyberprzestrzeni, organizacje terrorystyczne, zorganizowane grupy przestępcze oraz tzw. samotnych sprawców, którzy wykorzystują technologie informacyjne do destabilizacji systemów bezpieczeństwa państwa (Mockaitis, 2008).

Cyberterroryzm może być postrzegany jako zagrożenie będące konsekwencją rozwoju technologii, zwłaszcza Internetu oraz globalizacji. Z uwagi na specyfikę tego zjawiska, cyberterroryzm powinien stanowić przedmiot szczególnej analizy ze strony współczesnych decydentów odpowiedzialnych za bezpieczeństwo państw i społeczności międzynarodowej. Poniżej przedstawiono kluczowe aspekty, które powodują, że cyberterroryzm stanowi poważne zagrożenie dla bezpieczeństwa międzynarodowego:

- niskie koszty materialne – organizacja cyberataku nie wymaga znacznych nakładów finansowych, lecz przede wszystkim specjalistycznej wiedzy; koszty tego typu operacji są znacząco niższe niż tradycyjnych działań terrorystycznych,
- dostosowanie środków do celów operacyjnych – społeczeństwa adaptują swoje działania w celu osiągnięcia jak najbardziej efektywnych rezultatów. Cyberterroryzm minimalizuje ryzyko utraty życia, gdyż nie wiąże się z tak ekstremalnymi działaniami, jak ataki samobójcze,

- relatywna anonimowość – identyfikacja sprawców cyberataków jest wyjątkowo trudna, podobnie jak wykrycie motywacji stojących za konkretnymi aktami cyberterroryzmu,
- specyfika środowiska operacyjnego – Internet umożliwia przygotowanie ataków z wielu lokalizacji, ułatwiając działanie sprawców,
- efekt psychologiczny – w dzisiejszych czasach Internet jest wykorzystywany przez osoby fizyczne i instytucje do obsługi infrastruktury krytycznej. Skutkiem cyberataków jest zastraszenie obywateli poprzez naruszenie poczucia bezpieczeństwa,
- współzależność podmiotów – ogólnodostępny charakter cyberprzestrzeni sprzyja podejmowaniu działań, które mogą mieć negatywne, destrukcyjne skutki,
- globalny zasięg ataku – Internet jako medium globalne umożliwia przeprowadzenie ataków z dowolnego miejsca na świecie, co pozwala na skuteczne oddziaływanie na różnorodne cele.

Przyjmując atak cybernetyczny jako proces, można go przedstawić jako sekwencję następujących po sobie etapów obejmujących rozpoznanie celu, uzyskanie nieautoryzowanego dostępu do systemu oraz realizację działań destrukcyjnych lub destabilizujących. Poniżej na Rysunku 1 przedstawiono procesowy model realizacji ataku cybernetycznego.



Rysunek 1. Procesowy model realizacji ataku cybernetycznego

Źródło: opracowanie własne.

Rysunek 1 przedstawia procesowy model realizacji ataku cybernetycznego obejmujący trzy zasadnicze fazy. Pierwsza faza polega na identyfikacji i analizie celu ataku poprzez zbieranie informacji o systemie teleinformatycznym. Druga faza obejmuje działania prowadzące do uzyskania nieautoryzowanego dostępu do systemu poprzez wykorzystanie jego podatności.

Trzecia faza obejmuje realizację działań operacyjnych, takich jak modyfikacja, kradzież lub niszczenie danych oraz zakłócanie funkcjonowania systemów informatycznych.

W literaturze wyróżnia się dwa rodzaje akcji cyberterrorystycznych:

- ataki fizyczne na systemy informacyjne,
- ataki mające miejsce w cyberprzestrzeni (Białoskórski, 2011).

Atak fizyczny na systemy informacyjne to prowadzenie walki starymi metodami. W poprzednich latach terroryści uważali, że niszcząc systemy i instalacje komputerowe, atakują samo serce państwa. Natomiast specjaliści twierdzą, że nie trzeba się znać na informatyce by zniszczyć sieć informatyczną i tym samym sparaliżować życie w krajach wysoko rozwiniętych.

Atak w cyberprzestrzeni polega na uderzeniu w oprogramowanie przeciwnika (ang. Software). W tym przypadku jest wiele sposobów do przeprowadzenia takiego typu akcji w cyberprzestrzeni. Poniżej przedstawiono niektóre metody:

- stealing passwords – polega na uzyskaniu haseł dostępu do sieci,
- social engineering – wykorzystanie niekompetencji osób, które mają dostęp do systemu,
- bugs and backdoors – korzystanie z systemu bez zezwoleń lub używanie oprogramowania z nielegalnych źródeł,
- authentication failures – zniszczenie mechanizmu używanego do autoryzacji,
- protocol failures – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub więcej niezależnymi urządzeniami lub procesami,
- information leakage – atakujący uzyskuje informacje dostępne tylko dla administratora, niezbędne dla prawidłowego funkcjonowania sieci,
- denial of service – uniemożliwienie użytkownikom korzystania z ich systemu (Szybrycht, 2005).

Cyberataki to działania mające na celu zakłócenie funkcjonowania systemów informatycznych lub uzyskanie nieautoryzowanego dostępu do danych poprzez różnorodne metody, takie jak kradzież haseł, wykorzystywanie luk w zabezpieczeniach czy instalowanie złośliwego oprogramowania. Współcześnie cyberprzestrzeń stała się jednym z głównych obszarów konfliktów, a cyberterroryzm jest uznawany za poważne zagrożenie

dla bezpieczeństwa państw i społeczeństw. W efekcie, zarówno instytucje publiczne, jak i prywatne firmy muszą nieustannie rozwijać środki ochrony przed tego typu zagrożeniami, aby zapewnić ciągłość działania i ochronę wrażliwych informacji.

System przeciwdziałania cyberterroryzmowi oraz kierunki jego rozwoju w środowisku bezpieczeństwa państwa

Rozwój cyberterroryzmu, rozumianego jako działania w cyberprzestrzeni ukierunkowane na zastraszenie społeczeństwa, wymuszenie decyzji politycznych lub destabilizację funkcjonowania państwa, wymaga budowy zintegrowanego systemu ochrony obejmującego rozwiązania prawne, organizacyjne, techniczne oraz kompetencyjne. W praktyce przeciwdziałanie cyberterroryzmowi opiera się na łączeniu narzędzi bezpieczeństwa informacji (zarządzanie ryzykiem, ciągłość działania, procedury reagowania na incydenty), cyberobrony i ochrony infrastruktury krytycznej, a także na mechanizmach współpracy międzysektorowej (administracja – operatorzy usług kluczowych – sektor prywatny) i międzynarodowej, ponieważ znaczna część incydentów ma charakter transgraniczny.

Postępujący rozwój technologii informacyjnych pozwala na stwierdzenie, iż ryzyko cyberataku terrorystycznego rzeczywiście wzrasta (Smarzewski, 2017).

Na poziomie międzynarodowym istotną rolę odgrywa NATO, które po doświadczeniach m.in. ataków na Estonię i rosnącej liczbie operacji w cyberprzestrzeni rozwija cyberobronę jako element zbiorowej obrony. Kluczowym krokiem było przyjęcie polityki cyberobrony na szczycie w Walii (2014), gdzie uznano cyberobronę za część fundamentalnych zadań NATO, a także wskazano, że poważny cyberatak może stanowić przesłankę do uruchomienia mechanizmu art. 5 Traktatu Północnoatlantyckiego (Cyber defence). Równolegle Sojusz rozwija zdolności operacyjne i planistyczne w cyberprzestrzeni oraz wzmacnia ochronę własnych systemów i świadomość sytuacyjną, co jest realizowane m.in. przez struktury NCIA i zdolności reagowania na incydenty (NCIRC) w ramach ochrony zasobów NATO (NCIA). Istotnym trendem pozostaje także pogłębianie współdziałania NATO – UE w zakresie wymiany informacji o incydentach (np. porozumienie techniczne

NCIRC – CERT-EU), co wzmacnia zdolności wykrywania i reagowania w obu organizacjach (EEAS).

Na poziomie Unii Europejskiej ciężar działań przesunął się w stronę spójnych wymagań prawnych i budowania odporności systemowej. Dyrektywa NIS2 ustanawia jednolite ramy cyberbezpieczeństwa dla kluczowych sektorów i wzmacnia obowiązki w zakresie zarządzania ryzykiem oraz zgłaszania incydentów, a także zakłada rozwój współpracy między państwami członkowskimi (European Commission). Równocześnie wzmocniono rolę ENISA, która działa na podstawie tzw. Cybersecurity Act (rozporządzenie 2019/881), otrzymując stały mandat oraz wspierając operacyjną koordynację i rozwój kultury cyberbezpieczeństwa w UE, w tym poprzez sieci współpracy CSIRT. W perspektywie rozwojowej oznacza to przejście od podejścia „reaktywnego" (po incydencie) do podejścia „odpornościowego" (resilience-by-design): audyty i minimalne standardy, wymogi zarządcze (odpowiedzialność kierownictwa), ćwiczenia, współdziałanie transgraniczne oraz tworzenie zdolności reagowania na kryzysy na poziomie UE.

W odniesieniu do ONZ/ITU należy podkreślić, że Global Cybersecurity Agenda (GCA) ma przede wszystkim charakter ramowy i historycznie ważny, natomiast współcześnie dyskusja międzynarodowa koncentruje się na harmonizacji podejść, budowaniu zdolności państw (capacity building) i wypracowywaniu zasad odpowiedzialnego zachowania w cyberprzestrzeni. Samo wskazywanie filarów ITU może pozostać w tekście jako tło, ale warto je osadzić w logice „rozwoju zdolności" i ograniczyć opisowość. Podobnie wątek IMPACT wymaga doprecyzowania: jest to inicjatywa współpracująca z ITU, opisywana jako platforma wsparcia i współpracy w obszarze cyberzagrożeń, jednak jej znaczenie w praktyce polityk cyberbezpieczeństwa państw UE jest zwykle drugorzędne względem mechanizmów NIS2/ENISA i struktur krajowych.

W Polsce zasadniczą ramą organizacyjną jest ustawa o krajowym systemie cyberbezpieczeństwa, która porządkuje role i obowiązki podmiotów oraz zakłada współpracę kluczowych zespołów reagowania na incydenty. Z perspektywy praktycznej i aktualnej terminologii należy wskazywać trzy CSIRT poziomu krajowego: CSIRT NASK, CSIRT GOV i CSIRT MON, które koordynują obsługę incydentów w swoich domenach oraz współdziałają, aby zapewnić spójny system reagowania na incydenty poważne i krytyczne. W tym ujęciu wcześniejsze określenie „CERT.GOV.PL" warto

zastąpić aktualnym „CSIRT GOV" (portal csirt.gov.pl), a opis zadań oprzeć na współczesnym katalogu: monitorowanie zagrożeń, szacowanie ryzyka, ostrzeganie, reagowanie i koordynacja obsługi incydentów istotnych dla ciągłości działania państwa i infrastruktury krytycznej. Dodatkowo komponent wojskowy cyberbezpieczeństwa i cyberobrony wzmacniany jest przez struktury odpowiedzialne za funkcjonowanie CSIRT MON, co wpisuje się w trend integracji bezpieczeństwa cywilnego i wojskowego w obszarze zagrożeń hybrydowych.

Kierunki zmian w systemie przeciwdziałania cyberterroryzmowi zarówno w Polsce, jak i w UE i NATO można ująć w kilku dominujących tendencjach:

- wzrost roli zarządzania ryzykiem i odporności (ciągłość działania, segmentacja, „security by design"),
- przyspieszenie wymiany informacji i wspólnego reagowania (CSIRT-y, koordynacja transgraniczna, ćwiczenia),
- wzmacnianie ochrony infrastruktury krytycznej i usług cyfrowych poprzez minimalne standardy oraz obowiązki raportowania,
- profesjonalizacja kadr i rozwój kompetencji w administracji, służbach i wymiarze sprawiedliwości,
- rosnące znaczenie współpracy publiczno-prywatnej, ponieważ znaczna część zasobów i usług krytycznych znajduje się w domenie operatorów i dostawców technologii.

Współczesne bezpieczeństwo cybernetyczne wymaga zintegrowanego podejścia na poziomie międzynarodowym, europejskim i krajowym. Organizacje międzynarodowe, takie jak NATO i Unia Europejska, rozwijają polityki i struktury, które mają na celu zwiększenie odporności na cyberzagrożenia, promowanie współpracy i wymiany informacji, a także koordynację działań w przypadku incydentów. Jednolitość przepisów prawnych, ustanawianie minimalnych standardów ochrony i wzmacnianie systemów raportowania są dziś kluczowymi narzędziami budowania odporności infrastruktury krytycznej. Równocześnie wzrasta rola specjalistycznych zespołów reagowania na incydenty, profesjonalizacji kadr oraz łączenia sił pomiędzy administracją publiczną i sektorem prywatnym. Coraz większe znaczenie mają także działania edukacyjne i rozwijanie kompetencji, by sprostać dynamicznie zmieniającym się wyzwaniom w cyberprzestrzeni. Współczesna

strategia opiera się na prewencji, szybkim reagowaniu i budowaniu kultury bezpieczeństwa, która obejmuje zarówno państwa, jak i obywateli.

Podsumowanie

Cyberterroryzm stanowi jedno z kluczowych zagrożeń bezpieczeństwa współczesnych państw, którego znaczenie systematycznie wzrasta wraz z rozwojem technologii informacyjno-komunikacyjnych oraz postępującą cyfryzacją życia społecznego, gospodarczego i administracyjnego. Analiza problematyki cyberterroryzmu pozwala stwierdzić, że jest to zjawisko wielowymiarowe, łączące elementy klasycznego terroryzmu z wykorzystaniem narzędzi cyberprzestrzeni, co powoduje, że jego skutki mogą obejmować zarówno sferę bezpieczeństwa narodowego, jak i stabilność ekonomiczną oraz funkcjonowanie społeczeństwa informacyjnego.

Przeprowadzone rozważania wskazują, że cyberterroryzm może oddziaływać na państwo poprzez ataki na infrastrukturę krytyczną, systemy administracji publicznej, sektor finansowy oraz systemy komunikacyjne. W ujęciu procesowym działania cyberterrorystyczne mają charakter wieloetapowy i obejmują rozpoznanie celu, uzyskanie nieautoryzowanego dostępu do systemów teleinformatycznych oraz realizację działań destrukcyjnych lub destabilizujących. Złożoność i transgraniczny charakter tych zagrożeń powodują trudności w identyfikacji sprawców oraz skutecznym przeciwdziałaniu incydentom cybernetycznym.

Istotnym elementem przeciwdziałania cyberterroryzmowi jest rozwój systemów bezpieczeństwa obejmujących współpracę międzynarodową, regulacje prawne oraz rozwiązania technologiczne. Na poziomie globalnym i regionalnym znaczącą rolę odgrywają organizacje międzynarodowe, takie jak NATO, Unia Europejska oraz struktury ONZ, które podejmują działania na rzecz zwiększenia odporności państw na cyberzagrożenia oraz rozwijania mechanizmów reagowania na incydenty cybernetyczne. Równie istotne znaczenie ma rozwój krajowych systemów cyberbezpieczeństwa, w tym instytucji odpowiedzialnych za monitorowanie zagrożeń oraz reagowanie na incydenty w cyberprzestrzeni.

Współczesne kierunki rozwoju systemów przeciwdziałania cyberterroryzmowi wskazują na konieczność przechodzenia od działań reaktywnych do strategii opartych na zarządzaniu ryzykiem, budowaniu odporności

infrastruktury krytycznej oraz wykorzystywaniu nowoczesnych technologii, w tym systemów analizy danych i sztucznej inteligencji. Istotnym wyzwaniem pozostaje także rozwój kompetencji specjalistów w zakresie cyberbezpieczeństwa oraz wzmacnianie współpracy między sektorem publicznym i prywatnym.

Cyberterroryzm stanowi dynamicznie rozwijające się zagrożenie dla bezpieczeństwa państwa w środowisku cyfrowym, wymagające systemowego i wielowymiarowego podejścia do jego zwalczania. Skuteczność przeciwdziałania temu zjawisku zależy przede wszystkim od integracji działań instytucjonalnych, prawnych i technologicznych, a także od zdolności państw do adaptacji do zmieniającego się środowiska zagrożeń w cyberprzestrzeni.

Literatura

1. Białoskórski, R. (2011). *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku, Zarys problematyki*. Warszawa: Wyższa Szkoła Cła i Logistyki.
2. Cyber defence. (2026). *NATO Topic*. Pobrano z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence (dostęp: 20.03.2026).
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu.
4. EEAS. (2026). *EU and NATO increase information sharing on cyber incidents*. Pobrano z: https://www.eeas.europa.eu/node/5253_en (dostęp: 20.03.2026).
5. European Commission. (2026). *NIS2 Directive: securing network and information systems, Shaping Europe's digital future*. Pobrano z: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (dostęp: 20.03.2026).
6. Mockaitis, T. R. (2008). *The New Terrorism: Myths and Reality*. Stanford: Stanford University Press.
7. NCIA. (2026). *NATO Cyber Security Centre.* Pobrano z: https://www.ncia.nato.int/about-us/service-portfolio/nato-cyber-security-centre (dostęp: 20.03.2026).
8. Smarzewski, M. (2017). Cyberterroryzm a cyberprzestępstwa o charakterze terrorystycznym. *Ius Novum, 11*(1), 64-75.

9. Szybrycht, T. (2005). Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. *Zeszyty Naukowe Akademii Marynarki Wojennej, 1*(160), 173-181.
10. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553).
11. Yannakogeorgos, P. A. (2014). *Rethinking the Threat of Cyberterrorism*. W: T. M. Chen, L. Jarvis, S. Macdonald (red.), *Cyberterrorism: Understanding, Assessment, and Response* (s. 43-62). New York: Springer.

Patryk Ochyra[1]

Menadżerska Akademia Nauk Stosowanych w Warszawie

Mariusz Kubisz[2]

Wojskowa Akademia Techniczna w Warszawie

Bartosz Tarnowski[3]

Politechnika Gdańska

https://doi.org/10.29316/9788368103359_9

CYBERTERRORYZM JAKO WYZWANIE DLA BEZPIECZEŃSTWA PAŃSTWA – EWOLUCJA FORM, STRUKTUR ORGANIZACYJNYCH I IMPLIKACJE DLA POLSKI

CYBERTERRORISM AS A CHALLENGE TO NATIONAL SECURITY – THE EVOLUTION OF FORMS AND ORGANIZATIONAL STRUCTURES, AND IMPLICATIONS FOR POLAND

[1] https://orcid.org/0000-0001-8991-4068, e-mail: patryk.ochyra@op.pl

[2] https://orcid.org/0009-0003-7901-4690, e-mail: mariusz.kubisz@gmail.com

[3] https://orcid.org/0009-0000-0597-6684, e-mail: Bartosz.tarnowski@protonmail.ch

Streszczenie

Celem rozdziału jest analiza cyberterroryzmu jako współczesnego zagrożenia dla bezpieczeństwa państwa, ze szczególnym uwzględnieniem ewolucji form działalności terrorystycznej, zmian w strukturach organizacyjnych ugrupowań oraz implikacji tych procesów dla bezpieczeństwa Polski. Problem badawczy sformułowano: w jaki sposób rozwój cyberprzestrzeni wpływa na ewolucję terroryzmu oraz jakie zagrożenia cyberterroryzm stanowi dla bezpieczeństwa Polski? Przyjęto hipotezę, że cyberterroryzm stanowi realne i rosnące zagrożenie dla bezpieczeństwa państwa, ponieważ umożliwia destabilizację funkcjonowania kluczowych systemów, wywieranie presji politycznej oraz oddziaływanie psychologiczne na społeczeństwo przy relatywnie niskich kosztach i wysokiej anonimowości sprawców. W rozdziale zastosowano metody badawcze właściwe dla nauk o bezpieczeństwie, w szczególności analizę literatury przedmiotu, analizę danych empirycznych dotyczących incydentów cyberbezpieczeństwa oraz metodę analizy porównawczej i systemowej, pozwalające na identyfikację mechanizmów funkcjonowania współczesnych organizacji terrorystycznych oraz ocenę podatności państwa na zagrożenia w cyberprzestrzeni. Główny wniosek wskazuje, że cyberterroryzm stanowi jeden z istotnych elementów współczesnych zagrożeń hybrydowych, a skuteczne przeciwdziałanie temu zjawisku wymaga kompleksowego podejścia obejmującego rozwój zabezpieczeń technicznych, wzmacnianie odporności instytucjonalnej i informacyjnej oraz podnoszenie świadomości społecznej w zakresie bezpieczeństwa cyfrowego.

Słowa kluczowe: cyberterroryzm, bezpieczeństwo państwa, terroryzm, cyberbezpieczeństwo, zagrożenia hybrydowe

Abstract

The aim of the chapter is to analyze cyberterrorism as a contemporary threat to the security of the state, with particular emphasis on the evolution of forms of terrorist activity, changes in the organizational structures of groups and the implications of these processes for the security of Polish. The research problem was formulated: how does the development of cyberspace affect the evolution of terrorism and what threats does cyberterrorism pose to the security of Polish? It has been hypothesized that cyberterrorism poses a real and growing threat to the security of the state, as it allows for destabilization of the functioning of key systems, exerting political pressure and psychological impact on society at relatively low costs and high anonymity of perpetrators. The chapter uses research methods specific to security sciences, in particular the analysis of the literature on the subject, the analysis of empirical data

on cybersecurity incidents and the method of comparative and systemic analysis, allowing for the identification of the mechanisms of functioning of modern terrorist organizations and the assessment of the state's vulnerability to threats in cyberspace. The main conclusion points out that cyberterrorism is one of the important elements of today's hybrid threats, and effectively countering this phenomenon requires a comprehensive approach including the development of technical safeguards, strengthening institutional and information resilience and raising public awareness of digital security.

Keywords: cyberterrorism, state security, terrorism, cybersecurity, hybrid threats

Wstęp

Współczesne środowisko bezpieczeństwa państwa podlega dynamicznym i wielowymiarowym przemianom, wynikającym m.in. z postępu technologicznego, globalizacji oraz rozwoju cyberprzestrzeni. Jednym z kluczowych wyzwań XXI wieku pozostaje terroryzm, który ewoluuje zarówno pod względem form działania, jak i struktur organizacyjnych. Obok klasycznych metod przemocy coraz większe znaczenie zyskują działania prowadzone w cyberprzestrzeni, określane mianem cyberterroryzmu. Zjawisko to, choć rzadko prowadzi do bezpośrednich ofiar w ludziach, może powodować poważne zakłócenia funkcjonowania państwa, destabilizację społeczną oraz osłabienie zaufania obywateli do instytucji publicznych.

Celem niniejszego rozdziału jest analiza cyberterroryzmu jako współczesnego zagrożenia dla bezpieczeństwa państwa, ze szczególnym uwzględnieniem jego organizacyjnych uwarunkowań oraz implikacji dla Polski. Autor koncentruje się na ukazaniu ewolucji terroryzmu od form tradycyjnych do działań hybrydowych, łączących przemoc fizyczną z oddziaływaniem cyfrowym i informacyjnym. Praca podejmuje również próbę oceny skali i charakteru zagrożenia cyberterrorystycznego w polskiej cyberprzestrzeni, wskazując na kluczowe obszary podatności oraz wyzwania stojące przed systemem bezpieczeństwa państwa.

Istota i formy współczesnego terroryzmu

Współczesny terroryzm stanowi jedno z najpoważniejszych i najbardziej złożonych zagrożeń dla bezpieczeństwa państw oraz społeczności międzynarodowej. Jego istotą pozostaje stosowanie przemocy lub groźby jej użycia wobec ludności cywilnej, instytucji państwowych bądź infrastruktury krytycznej w celu osiągnięcia określonych celów politycznych, ideologicznych, religijnych lub ekonomicznych. Charakterystycznym elementem działań terrorystycznych jest instrumentalne traktowanie ofiar, które nie są celem samym w sobie, lecz środkiem do wywołania określonego efektu psychologicznego i społecznego (Hoffman, 2017).

Klasyczne formy terroryzmu obejmują zamachy bombowe, zabójstwa, porwania, wzięcia zakładników, podpalenia oraz ataki z użyciem broni chemicznej lub biologicznej. Działania te mają na celu wywołanie strachu, destabilizacji oraz poczucia bezradności wśród obywateli, co w konsekwencji prowadzi do osłabienia zaufania do instytucji państwowych (Piątkowski, 1996). Strach staje się w tym ujęciu podstawowym narzędziem walki, oddziałującym nie tylko na bezpośrednie ofiary, lecz również na szerokie grono odbiorców za pośrednictwem mediów tradycyjnych i cyfrowych.

Współczesne ugrupowania terrorystyczne dowodzą, że do osiągnięcia znaczących efektów destabilizacyjnych nie są konieczne zaawansowane technologicznie środki ani rozbudowane struktury organizacyjne. Niewielkie grupy, a nawet pojedynczy sprawcy działający w ramach tzw. terroryzmu indywidualnego, są w stanie wywołać poważne skutki polityczne i społeczne. Zjawisko to nabrało szczególnego znaczenia w dwudziestym pierwszym wieku wraz z rozwojem Internetu i mediów społecznościowych, które ułatwiają proces radykalizacji, rekrutacji oraz rozpowszechniania propagandy ekstremistycznej.

Podział rozległego zjawiska jakim jest terroryzm nie jest jednolity, a każdy podejmujący się tego zadania autor przyjmuje własną koncepcję (Europol, 2023). W literaturze przedmiotu najczęściej wyróżnia się trzy główne nurty terroryzmu: polityczny, religijny i kryminalny (Superczyńska, 2019).

Terroryzm polityczny stanowi formę walki prowadzonej przez podmioty słabsze wobec silniejszych struktur państwowych. Jego celem jest wywarcie presji na władze poprzez akty przemocy lub groźby ich użycia. Terroryści polityczni dążą do zwrócenia uwagi opinii publicznej na postulowane

przez siebie problemy, destabilizacji porządku konstytucyjnego państwa lub pogłębienia istniejących antagonizmów społecznych i narodowościowych. Akt przemocy ma często charakter symboliczny i służy zapoczątkowaniu procesu eskalacji konfliktu.

Szczególną odmianą terroryzmu jest terroryzm religijny, który w ostatnich dekadach zyskał na znaczeniu. Opiera się on na fundamentalistycznej interpretacji doktryn religijnych, w ramach której przemoc uznawana jest za moralnie usprawiedliwioną, a niekiedy wręcz nakazaną. Przekonanie o działaniu w imię sił nadprzyrodzonych prowadzi do zniesienia tradycyjnych ograniczeń etycznych i sprzyja eskalacji brutalności, w tym gotowości do poświęcenia własnego życia (Hoffman, 2017).

Terroryzm kryminalny stanowi zjawisko pograniczne, w którym metody charakterystyczne dla działań terrorystycznych wykorzystywane są w celu osiągnięcia korzyści materialnych. Zorganizowane grupy przestępcze sięgają po zamachy, porwania czy zastraszanie, co prowadzi do przenikania się motywacji kryminalnych i politycznych. Zjawisko to obserwowane jest szczególnie w regionach dotkniętych słabością instytucji państwowych oraz wysokim poziomem korupcji (Wałek, 2018).

Inny podział omawianego zjawiska wskazuje na terroryzm międzynarodowy i lokalny. Terroryzmem międzynarodowym określamy działania skierowane przeciwko różnym krajom i rządom na całym świecie. Ta forma dotyczy takich sytuacji, gdy terroryści stacjonują, planują i realizują zamach na obcym terytorium. Stanowi ona potencjalnie większe zagrożenie w stosunkach międzynarodowych, oddziałując na obywateli różnych państw (Wałek, 2018). Terroryzm lokalny koncentruje swoje działania na walce z miejscowym rządem i ograniczając się do działalności na terenie danego kraju nie przekracza jego granic. Taka działalność ma głównie na celu zastraszenie lub usunięcie osób, które są postrzegane jako wróg publiczny lub działają wbrew woli ludności. Często wrogami terrorystów są inni terroryści lub niewygodne grupy etniczne stwarzające zagrożenie na własnym terytorium. Ten rodzaj terroryzmu zmierza do zastraszenia społeczeństwa, poprzez realizowanie ataków na cele przypadkowe i newralgiczne. Celem takich działań nie jest w przeciwieństwie do terroryzmu międzynarodowego uzyskanie rozgłosu, a jeśli nawet to nie w celu nagłośnienia swojej sprawy. Skupia się on na wyrażeniu niezadowolenia w postępowaniu władz danego kraju (Wałek, 2018).

Współczesne analizy wskazują również na rosnące znaczenie nowych form zagrożeń, takich jak cyberterroryzm. Cyberterroryzm obejmuje działania wymierzone w systemy teleinformatyczne, infrastrukturę krytyczną oraz sferę informacyjną państwa. Choć ataki te rzadko powodują bezpośrednie ofiary w ludziach, mogą prowadzić do poważnych zakłóceń funkcjonowania administracji publicznej, gospodarki oraz systemów bezpieczeństwa (Europol, 2023).

Podsumowując, terroryzm pozostaje zjawiskiem dynamicznym, które nieustannie dostosowuje się do zmieniających się warunków politycznych, technologicznych i społecznych. Zrozumienie jego nurtów i form stanowi kluczowy element skutecznego przeciwdziałania temu zagrożeniu na poziomie krajowym i międzynarodowym.

Organizacja grup terrorystycznych w warunkach cyfrowych

Cyberterroryzm jest współcześnie definiowany jako forma działalności terrorystycznej wykorzystująca narzędzia teleinformatyczne do wywoływania strachu, destabilizacji oraz presji politycznej lub społecznej poprzez zakłócanie dostępności, integralności lub poufności informacji i systemów informatycznych. Obejmuje on zarówno działania techniczne, takie jak ataki typu DDoS, sabotaż systemów informacyjnych czy niszczenie danych, jak również operacje informacyjne, w tym dezinformację, propagandę ekstremistyczną oraz oddziaływanie psychologiczne prowadzone w cyberprzestrzeni. W przeciwieństwie do klasycznych form terroryzmu, celem cyberterroryzmu jest najczęściej nie fizyczna destrukcja infrastruktury, lecz wywołanie efektu społecznego i psychologicznego poprzez paraliż usług, manipulację informacją oraz podważenie zaufania do instytucji państwowych (Liszkowska, 2023).

W literaturze przedmiotu podkreśla się, że cyberterroryzm bywa niekiedy określany jako potencjalna forma „broni masowego rażenia", jednak współczesne analizy odchodzą od tego ujęcia na rzecz koncepcji „broni masowych zakłóceń" (*mass disruption*). Oznacza to, że skuteczność cyberterroryzmu nie polega na generowaniu bezpośrednich ofiar, lecz na zdolności do dezorganizacji funkcjonowania państwa i społeczeństwa, w szczególności poprzez uderzenie w systemy informacyjne, komunikacyjne oraz infrastrukturę krytyczną. Zjawisko to nabiera szczególnego znaczenia w warunkach

rosnącego uzależnienia państw i organizacji międzynarodowych, w tym struktur bezpieczeństwa zbiorowego, takich jak NATO, od niezawodnych i bezpiecznych systemów teleinformatycznych (ENISA, 2024).

Współczesne organizacje terrorystyczne funkcjonują w sposób coraz bardziej złożony, łącząc klasyczne, hierarchiczne modele organizacyjne z elastycznymi strukturami sieciowymi, charakterystycznymi dla środowiska cyfrowego. Tradycyjny model oparty na centralnym dowództwie, komórkach wywiadowczych, logistycznych i wykonawczych nadal występuje, jednak w ostatnich latach ulega on istotnej transformacji pod wpływem rozwoju cyberprzestrzeni oraz technologii informacyjnokomunikacyjnych (Hoffman, 2017).

Na najwyższym szczeblu struktury organizacyjnej znajduje się dowództwo, które odpowiada za wyznaczanie strategicznych celów, kierunków ideologicznych oraz alokację zasobów finansowych. Coraz częściej osoby pełniące funkcje decyzyjne pozostają całkowicie anonimowe, działając w przestrzeni cyfrowej z wykorzystaniem szyfrowanych kanałów komunikacji, sieci TOR oraz kryptowalut, co znacząco utrudnia ich identyfikację przez służby bezpieczeństwa (CyberDefence24, 2022).

Kluczową rolę w nowoczesnych organizacjach terrorystycznych odgrywają komórki wywiadowcze i analityczne, które obecnie funkcjonują w dużej mierze w cyberprzestrzeni. Ich zadania obejmują nie tylko klasyczne rozpoznanie potencjalnych celów, lecz także analizę danych dostępnych w otwartych źródłach, monitorowanie mediów społecznościowych oraz prowadzenie działań dezinformacyjnych. Proces werbunku coraz częściej odbywa się online, a radykalizacja potencjalnych członków następuje za pośrednictwem forów internetowych, komunikatorów i platform streamingowych (Schmid, 2021).

Grupa wsparcia logistycznego, obok tradycyjnych zadań związanych z zapewnieniem schronienia, dokumentów i środków finansowych, rozszerzyła swoje działania o obsługę zaplecza cyfrowego. Obejmuje to zarządzanie infrastrukturą informatyczną, zabezpieczanie komunikacji, obsługę portfeli kryptowalutowych oraz ukrywanie przepływów finansowych przy użyciu technologii blockchain. Cyberprzestrzeń stała się kluczowym obszarem umożliwiającym funkcjonowanie organizacji bez konieczności fizycznej obecności jej członków na danym terytorium.

Realizacja działań operacyjnych, w tym zamachów terrorystycznych, nadal pozostaje domeną grup taktycznych. Jednak także w tym obszarze widoczny jest wpływ cyberterroryzmu. Ataki fizyczne coraz częściej poprzedzane są działaniami cybernetycznymi, takimi jak zakłócanie systemów alarmowych, infrastruktury krytycznej czy systemów łączności. Cyberataki pełnią również funkcję wspomagającą, dezorganizując działania ratownicze i utrudniając reakcję służb bezpieczeństwa. Taktyka działania organizacji terrorystycznych obejmuje obecnie zarówno klasyczne metody konspiracji, jak i zaawansowane techniki cyfrowe. Minimalizacja kontaktów osobistych, wykorzystanie szyfrowanych komunikatorów, skrzynek kontaktowych w sieci, a także stosowanie dezinformacji i fałszywych tożsamości cyfrowych stanowią podstawowe elementy współczesnego modus operandi. Działania te pozwalają na prowadzenie operacji niskokosztowych, a jednocześnie o wysokim potencjale oddziaływania psychologicznego (Liszkowska, 2023).

Analiza celów ataków terrorystycznych wskazuje na cztery podstawowe grupy podmiotów narażonych na oddziaływanie terroru: instytucje rządowe, aparat bezpieczeństwa państwa, sektor gospodarczy oraz ludność cywilną. W kontekście cyberterroryzmu szczególnie istotne stają się ataki na infrastrukturę krytyczną, systemy energetyczne, telekomunikacyjne oraz finansowe, których paraliż może prowadzić do długotrwałych skutków społecznych i gospodarczych bez konieczności użycia przemocy fizycznej (Carbonelli i in., 2024).

Motywacje działalności terrorystycznej pozostają złożone i wielowymiarowe. Obejmują one czynniki ideologiczne, społecznoekonomiczne oraz psychologiczne, które wzajemnie się przenikają. W środowisku cyfrowym proces radykalizacji ulega przyspieszeniu, a izolacja społeczna, frustracja oraz narracje spiskowe sprzyjają podatności jednostek na propagandę ekstremistyczną. Cyberprzestrzeń stała się zatem nie tylko narzędziem działania, lecz także środowiskiem sprzyjającym powstawaniu nowych form terroryzmu.

Podsumowując, współczesne organizacje terrorystyczne funkcjonują jako hybrydowe struktury łączące tradycyjne formy przemocy z zaawansowanymi działaniami w cyberprzestrzeni. Rosnące znaczenie cyberterroryzmu wymusza konieczność redefinicji dotychczasowych strategii

przeciwdziałania oraz wzmocnienia zdolności państw w zakresie ochrony cyberbezpieczeństwa i przeciwdziałania radykalizacji online.

Cyberterroryzm jako zagrożenie dla Polski

Ocena zagrożenia cyberterroryzmem dla Polski powinna być osadzona w empirycznym obrazie „codziennych" incydentów cyberbezpieczeństwa. Aktualne dane z krajowego ekosystemu reagowania pokazują dynamiczny wzrost skali zdarzeń, które choć w większości mają charakter oszustw lub cyberprzestępczości tworzą środowisko sprzyjające aktorom politycznym i ekstremistycznym. W analizie bezpieczeństwa polskiego internetu za 2024 rok, przygotowanej na podstawie danych CERT Polska, wskazano m.in., że liczba zgłoszeń przekroczyła 600 tys. (wzrost o 62% rok do roku), a liczba zarejestrowanych incydentów wzrosła o 29%. Dominującą kategorią były oszustwa komputerowe 94,7% wszystkich incydentów, w tym phishing (40 120 incydentów) (Gov.pl, 2025).

Z punktu widzenia cyberterroryzmu szczególne znaczenie mają dwie kategorie: ataki na dostępność i ciągłość działania (np. DDoS, sabotaż usług) oraz zdarzenia destrukcyjne, takie jak ransomware. W 2024 r. odnotowano 147 incydentów ransomware (spadek o ok. 8% w porównaniu z 2023), przy czym ofiarami były zarówno firmy, jak i osoby prywatne oraz instytucje publiczne. Ransomware jest o tyle istotne, że może zostać wykorzystane nie tylko do wymuszeń finansowych, lecz także do celów politycznych (np. „kara" za decyzje władz), a publikowanie danych po ataku może wzmacniać efekt zastraszenia (Gov.pl, 2025).

Wzrost skali smishingu i phishingu jest ważny również dlatego, że te techniki stanowią „wejście" do bardziej zaawansowanych kampanii. Przykładowo masowe kampanie socjotechniczne mogą posłużyć do uzyskania dostępu do kont uprzywilejowanych, co w efekcie umożliwia sabotaż usług publicznych lub zakłócenie pracy instytucji. Nawet gdy motywacją większości sprawców jest zysk, infrastruktura ataku i podatności użytkowników tworzą warunki, które mogą zostać wykorzystane przez aktorów dążących do wywołania efektu „terroru" w cyberprzestrzeni (Linkedin, 2024).

Wrażliwość Polski na cyberterroryzm wynika z trzech nakładających się czynników: rosnącego uzależnienia usług publicznych i gospodarczych od systemów informatycznych, wysokiej „widoczności" Polski w środowisku

geopolitycznym i sojuszniczym, oraz zróżnicowanego poziomu dojrzałości cyberbezpieczeństwa w sektorze publicznym i prywatnym (ABW, 2024). Cyberterroryzm w wariancie „sabotagefirst" koncentruje się na zakłóceniu usług o dużej widoczności społecznej: energetyki, wodociągów, łączności, transportu i usług finansowych. Nawet krótkotrwałe przerwy w dostępności mogą generować intensywny efekt psychologiczny, szczególnie gdy towarzyszy im narracja o „bezsilności państwa". Analizy dotyczące hybrydowego wymiaru współczesnego terroryzmu wskazują, że infrastruktura krytyczna pozostaje atrakcyjnym celem dla aktorów pragnących osiągnąć efekt polityczny i społeczny .

Administracja publiczna i usługi cyfrowe. Wraz z rozwojem eusług oraz cyfrowych kanałów kontaktu obywateli z państwem rośnie znaczenie ochrony systemów tożsamości, rejestrów oraz kanałów komunikacji. Ataki na te obszary mogą prowadzić do chaosu administracyjnego lub szeroko odczuwalnych utrudnień, a równocześnie są atrakcyjne z punktu widzenia propagandy. Z perspektywy sprawcy efekt „wymuszający" może zostać osiągnięty poprzez eskalację zakłóceń i wzrost presji społecznej na władze. Sektor zdrowia i usługi wrażliwe społecznie. Ransomware oraz ataki na dostępność systemów ochrony zdrowia mogą mieć silny efekt społeczny, ponieważ dotyczą obszaru wysokiej wrażliwości, jakim jest życie i zdrowie. Łańcuch dostaw i dostawcy usług IT. Coraz większa część usług państwa i gospodarki opiera się na zewnętrznych dostawcach oprogramowania, chmury oraz usług utrzymaniowych. Atak na dostawcę może skutkować efektem domina u wielu odbiorców. Europol zwraca uwagę na rosnącą złożoność ekosystemu cyberzagrożeń w UE, w tym na rozwój zorganizowanych modeli usług przestępczych oraz nadużyć technologicznych. W kontekście cyberterroryzmu oznacza to możliwość pośredniego oddziaływania poprzez mniej chronione ogniwa łańcucha dostaw (Europol, 2025).

W polskich realiach zagrożenie cyberterroryzmem należy postrzegać nie tylko przez pryzmat ataków technicznych na systemy informatyczne, lecz również jako ryzyko działań informacyjnych i procesów radykalizacyjnych zachodzących w cyberprzestrzeni. Środowisko cyfrowe sprzyja szybkiemu tworzeniu wspólnot ideologicznych, intensywnemu rozpowszechnianiu treści oraz funkcjonowaniu alternatywnych obiegów informacyjnych, w których narracje ekstremistyczne mogą się wzajemnie wzmacniać i normalizować. Skala oraz tempo cyrkulacji informacji powodują, że oddziaływanie

takich treści nie jest ograniczone do wąskich grup odbiorców, lecz może obejmować szerokie segmenty społeczeństwa (Liszkowska, 2023).

Szczególne znaczenie w tym kontekście mają mechanizmy charakterystyczne dla współczesnych platform cyfrowych. Przekaz może być łatwo skalowany i docierać do tysięcy odbiorców w krótkim czasie, a jednocześnie podlegać daleko idącej personalizacji dzięki algorytmom rekomendacji. Dodatkowym czynnikiem sprzyjającym jest możliwość anonimizacji działań oraz szybka migracja pomiędzy różnymi kanałami komunikacji w przypadku prób moderacji lub ograniczania treści. W rezultacie oddziaływanie informacyjne o charakterze cyberterrorystycznym nie musi opierać się na zaawansowanych kompetencjach technicznych; kluczowe staje się umiejętne wykorzystanie kanałów dystrybucji informacji oraz podatności poznawczych odbiorców. W tym sensie cyberterroryzm wpisuje się w szerszy katalog zagrożeń hybrydowych, w których presja na państwo i społeczeństwo budowana jest równolegle poprzez środki techniczne i oddziaływanie psychologiczne (Liszkowska, 2023).

Istotnym czynnikiem sprzyjającym tego rodzaju zagrożeniom jest także rosnąca skala masowych oszustw i kampanii socjotechnicznych w polskiej cyberprzestrzeni. Zjawiska te przyczyniają się do utrwalania „chaosu komunikacyjnego", upowszechnienia podszywania się pod instytucje publiczne oraz stopniowego osłabienia zaufania do cyfrowych kanałów kontaktu z państwem. W takim środowisku znacznie łatwiej o działania manipulacyjne i zastraszające, które w zależności od motywacji sprawcy i celu oddziaływania mogą przyjmować cechy cyberterroryzmu, zwłaszcza gdy służą wymuszaniu decyzji politycznych lub destabilizacji porządku społecznego (Gerwatowski, 2021).

Zagrożenie cyberterroryzmem dla Polski należy zatem ujmować jako splot kilku wzajemnie powiązanych wymiarów. Obejmuje ono ryzyko techniczne, związane z zakłóceniami dostępności i integralności systemów informatycznych, ryzyko społeczne, wyrażające się w narastaniu strachu, dezorientacji i utracie zaufania do instytucji publicznych, a także ryzyko polityczne, polegające na wywieraniu presji na decydentów poprzez eskalację zakłóceń i napięć społecznych. Skala i charakter incydentów obserwowanych w polskiej cyberprzestrzeni wskazują, że dominacja phishingu i technik socjotechnicznych tworzy sprzyjające warunki dla bardziej

ukierunkowanych i destrukcyjnych kampanii, których cele mogą wykraczać poza zwykły zysk finansowy (Rzeczpospolita, 2025).

W praktyce oznacza to, że przeciwdziałanie cyberterroryzmowi nie może ograniczać się wyłącznie do wdrażania zabezpieczeń technicznych. Równie istotna jest odporność instytucjonalna, rozumiana jako zdolność administracji i podmiotów publicznych do utrzymania ciągłości działania w warunkach zakłóceń, odporność informacyjna, polegająca na ograniczaniu skuteczności propagandy i dezinformacji, oraz odporność społeczna, obejmująca cyberhigienę i zdolność obywateli do rozpoznawania manipulacji. Z punktu widzenia badań nad terroryzmem kluczowe pozostaje przy tym precyzyjne rozróżnianie motywacji sprawców i celów ataków, tak aby polityka bezpieczeństwa była w stanie adekwatnie reagować zarówno na masową cyberprzestępczość, jak i na rzadsze, lecz potencjalnie znacznie bardziej dotkliwe scenariusze o charakterze terrorystycznym (Jankowski, 2018).

Podsumowanie

Przeprowadzona analiza potwierdza, że terroryzm pozostaje zjawiskiem dynamicznym, które nieustannie adaptuje się do zmieniających się warunków technologicznych i społecznych. Rozwój cyberprzestrzeni stworzył nowe możliwości działania dla ugrupowań terrorystycznych, umożliwiając im prowadzenie operacji o charakterze hybrydowym, łączących elementy przemocy fizycznej z cyberatakami i oddziaływaniem informacyjnym. Cyberterroryzm, rozumiany jako narzędzie „masowych zakłóceń", może prowadzić do poważnych konsekwencji społecznych, gospodarczych i politycznych, mimo braku bezpośrednich strat w ludziach.

W odniesieniu do Polski zagrożenie cyberterroryzmem należy postrzegać wielowymiarowo, uwzględniając zarówno aspekty techniczne, jak i społeczne oraz informacyjne. Rosnąca liczba incydentów cyberbezpieczeństwa, uzależnienie funkcjonowania państwa od systemów informatycznych oraz znaczenie Polski w kontekście geopolitycznym zwiększają jej podatność na tego rodzaju działania. Skuteczne przeciwdziałanie cyberterroryzmowi wymaga zatem podejścia kompleksowego, obejmującego nie tylko rozwój zabezpieczeń technicznych, lecz także wzmacnianie odporności instytucjonalnej, informacyjnej i społecznej. Tylko takie podejście pozwala na

ograniczenie skutków potencjalnych działań cyberterrorystycznych oraz zwiększenie bezpieczeństwa państwa w warunkach cyfrowej rzeczywistości.

Literatura

1. Agencja Bezpieczeństwa Wewnętrznego. (2024). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP*, Warszawa.
2. *Analiza bezpieczeństwa polskiego internetu w 2024 rok.* Pobrano z: https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku (dostęp: 20.03.2026).
3. Carbonelli, M., Quaranta, R., Malizia, A., Gaudio, P., Di Giovanni, D. (2024). An Analysis of Terrorist Attacks on Soft and Hard Targets in the Period 2000-2019, *International Journal of Safety and Security Engineering, 14*(3).
4. *Digital Scams Lead to Terror Financing.* Pobrano z: https://www.linkedin.com/pulse/digital-scams-lead-terror-financing-haunting-threat-qureshi-4ml0f (dostęp: 20.03.2026).
5. *EU struggles to protect itself from cyberattacks*. Pobrano z: https://euranetplus-inside.eu/eu-struggles-to-protect-itself-from-cyberattacks (dostęp: 20.03.2026).
6. Europol. (2023). *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg.
7. Gerwatowski, J. (2021). Cyberterroryzm jako efekt rozwoju nowych technologii informatycznych w pierwszej i drugiej dekadzie XXI wieku. *Przegląd Policyjny*, *141*(1).
8. Hoffman, B. (2017). *Inside terrorism*, Columbia University Press, Columbia.
9. Jankowski, P. (2018). Cyberterroryzm jako współczesne zagrożenie dla administracji publicznej. *Młody Jurysta*, (4), 13-27.
10. Kosta, R. A., *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*, Wydawnictwo Adam Marszałek, Toruń 2012.
11. *Kryptowaluty w finansowaniu terroryzmu.* Pobrano z: https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-kryptowaluty-w-finansowaniu-terroryzmu--realne-zagrozenie (dostęp: 20.03.2026).

12. Liszkowska, D. (2023). Cyberterrorism as a contemporary threat to the security of the state and socjet*y, De Securitate et Defensione. O Bezpieczeństwie i Obronności, 2*(9), 131-148.
13. Piątkowski, P. (1996). *Terroryzm. Nowe wyzwanie dla bezpieczeństwa*, Wydawnictwo Adam Marszałek, Warszawa.
14. Schmid, A. P., Forest, J. J. F., Lowe, T. (2021). Terrorism Studies: A Glimpse at the Current State of Research (2021). *Perspectives on Terrorism, 15*(3), 142-152.
15. *Socjotechnika lepsza niż hacking.* Pobrano z: https://www.rp.pl/przestepczosc/art42149701-socjotechnika-lepsza-niz-hacking-tak-oszusci-osaczaja-swoje-ofiary#:~:text=Cyberprzest%C4%99pcy%20odchodz%C4%85%20od%20zaawansowanych%20atak%C3%B3w%20hakerskich%20na%20rzecz%20socjotechniki%20%2D%20rp.pl (dostęp: 20.03.2026).
16. *Steal, Deal, Repeat: Cybercriminals cash in on your data*. Pobrano z: https://www.europol.europa.eu/media-press/newsroom/news/steal-deal-repeat-cybercriminals-cash-in-your-data (dostęp: 20.03.2026).
17. Superczyńska, K. (2019). *Terroryzm polityczny na pograniczu prawa i nauk politycznych, Gdańskie Studia Międzynarodowe 17*(1-2).
18. *Terroryści i darknet.* Pobrano z: https://cyberdefence24.pl/terrorysci-niechetnie--korzystaja-z-darknetu (dostęp: 20.03.2026).
19. The European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. Pobrano z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 20.03.2026).
20. Wałek, T. (2018). Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych., *Securitologia, 2*(28), 107-119.

Kamil Jaszczuk[1]

Państwowa Akademia Nauk Stosowanych w Chełmie

https://doi.org/10.29316/9788368103359_10

MECHANIZMY DEZINFORMACJI W MEDIACH SPOŁECZNOŚCIOWYCH I ICH WPŁYW NA BEZPIECZEŃSTWO NARODOWE

MECHANISMS OF DISINFORMATION IN SOCIAL MEDIA AND THEIR IMPACT ON NATIONAL SECURITY

Streszczenie

Celem rozdziału jest analiza mechanizmów dezinformacji funkcjonujących w mediach społecznościowych oraz ocena ich wpływu na bezpieczeństwo narodowe, ze szczególnym uwzględnieniem uwarunkowań Polski i regionu Europy Środkowo-Wschodniej. Sformułowano problem badawczy: w jaki sposób dezinformacja, wykorzystująca narzędzia cyfrowe, algorytmy platform społecznościowych oraz zautomatyzowane i skoordynowane działania aktorów państwowych i niepaństwowych, oddziałuje na odporność informacyjną państwa, procesy demokratyczne

[1] https://orcid.org/0009-0005-5403-514X, kjaszczuk@panschelm.edu.pl

oraz stabilność społeczną. Przyjęto hipotezę badawczą zakładającą, że dezinformacja w mediach społecznościowych stanowi istotny komponent współczesnych działań hybrydowych i realnie zagraża bezpieczeństwu narodowemu poprzez erozję zaufania społecznego, polaryzację opinii publicznej oraz osłabianie zdolności państwa do skutecznego zarządzania kryzysowego. W rozdziale zastosowano metody badawcze, w szczególności analizę literatury przedmiotu, analizę raportów instytucji krajowych i międzynarodowych, studium przypadków wybranych kampanii dezinformacyjnych oraz metodę porównawczą. Główny wniosek z przeprowadzonych badań wskazuje, że skuteczne przeciwdziałanie dezinformacji wymaga zintegrowanego podejścia obejmującego działania edukacyjne, technologiczne, organizacyjne i prawne, a także współpracę państwa, sektora prywatnego i społeczeństwa obywatelskiego w celu wzmacniania odporności informacyjnej państwa.

Słowa kluczowe: dezinformacja, media społecznościowe, bezpieczeństwo narodowe, wojna informacyjna, odporność informacyjna

Abstract

The aim of the chapter is to analyze the mechanisms of disinformation functioning in social media and assess their impact on national security, with particular emphasis on the conditions of Polish and the region of Central and Eastern Europe. The research problem was formulated: how disinformation, using digital tools, algorithms of social platforms and automated and coordinated actions of state and non-state actors, affects the information resilience of the state, democratic processes and social stability. A research hypothesis was adopted assuming that disinformation in social media is an important component of contemporary hybrid activities and poses a real threat to national security by eroding social trust, polarizing public opinion and weakening the state's ability to effectively manage crises. The chapter uses research methods, in particular the analysis of the literature on the subject, the analysis of reports of national and international institutions, a case study of selected disinformation campaigns and a comparative method. The main conclusion of the conducted research indicates that effective counteracting disinformation requires an integrated approach including educational, technological, organizational and legal activities, as well as cooperation between the state, the private sector and civil society in order to strengthen the information resilience of the state.

Keywords: disinformation, social media, national security, information warfare, information resilience

Wstęp

Rozwój technologii informacyjnych i komunikacyjnych na początku XXI wieku doprowadził do zasadniczych przemian funkcjonowania społeczeństw, instytucji, a także państw. Zmienił sposób, w jaki podmioty te zdobywają i przetwarzają informacje. Media społecznościowe, które pierwotnie miały pełnić funkcję demokratyzującą, umożliwiając każdemu obywatelowi udział w debacie publicznej oraz wymianę informacji stały się jednocześnie narzędziem kształtowania opinii publicznej o ogromnym potencjale destabilizacyjnym oraz instrumentem w nowoczesnych strategiach wojny informacyjnej (Bencsik i in., 2023). W dobie globalizacji i powszechnego dostępu do internetu zjawisko dezinformacji urasta do rangi jednego z kluczowych wyzwań dla bezpieczeństwa narodowego i międzynarodowego (Fundacja DigitalPoland, 2024).

W Polsce i regionie Europy Środkowo-Wschodniej zagrożenie dezinformacją nabiera szczególnego znaczenia ze względu na geopolityczne położenie regionu oraz aktywność Federacji Rosyjskiej, która traktuje obok działań wojskowych i ekonomicznych przestrzeń informacyjną jako strategiczny obszar prowadzenia działań hybrydowych. Rosyjska dezinformacja, oparta na starannie zaplanowanych kampaniach propagandowych, ma na celu osłabienie zaufania do instytucji demokratycznych, pogłębianie podziałów społecznych oraz podważanie pozycji Polski w strukturach Unii Europejskiej i NATO.

Zjawisko dezinformacji, choć nie jest nowe, w epoce cyfrowej przybrało zupełnie nowy wymiar. Treści rozprzestrzeniają się znacznie szybciej i skuteczniej niż kiedykolwiek wcześniej. Dzieje się to dzięki algorytmem rekomendacyjnym platform społecznościowych oraz masowym kontom automatycznym. Zasięg i szybkość rozpowszechniania informacji powodują, że manipulacja informacyjna może osiągnąć skalę trudną do opanowania.

Celem niniejszego rozdziału jest analiza mechanizmów dezinformacji w mediach społecznościowych oraz ocena ich wpływu na bezpieczeństwo narodowe ze szczególnym uwzględnieniem doświadczeń Polski i regionu Europy Środkowo-Wschodniej.

Definicja dezinformacji

Pojęcie dezinformacji nie posiada jednoznacznej, powszechnie akceptowanej definicji. W literaturze naukowej często stosuje się je zamiennie z takimi określeniami jak „propaganda" czy „fałszywa informacja", choć w praktyce mogą one oznaczać nieco odmienne zjawiska. Dezinformacja odnosi się zazwyczaj do celowego rozpowszechniania nieprawdziwych lub wprowadzających w błąd treści, mających na celu wywołanie określonych reakcji społecznych lub politycznych.

Warto zauważyć, że samo pojęcie dezinformacji ma swoje korzenie w Rosji. Zarówno w języku, jak i w praktykach politycznych tego państwa. Już w czasach Związku Radzieckiego stosowano zorganizowane działania polegające na szerzeniu fałszywych informacji, mających na celu destabilizację przeciwnika lub manipulowanie opinią publiczną, zarówno wewnątrz kraju, jak i za granicą. Z biegiem lat termin ten zyskał międzynarodowy zasięg i jest dziś powszechnie używany do opisu różnorodnych strategii manipulacji informacją w przestrzeni publicznej, zwłaszcza w kontekście nowoczesnych technologii i mediów cyfrowych (Kaczmarek, 2024).

Dezinformacja jest rozumiana jako celowe, systematyczne wprowadzanie w błąd poprzez tworzenie, rozpowszechnianie lub wykorzystywanie fałszywych bądź zmanipulowanych informacji, mających za zadanie wywołanie określonych reakcji społecznych lub politycznych (Materska, 2007). W literaturze podkreśla się, że dezinformacja różni się od nieświadomego rozpowszechniania nieprawdziwych wiadomości tym, że jest intencjonalna i najczęściej służy interesom określonych podmiotów, państwowych lub pozapaństwowych. To świadome i nieetyczne dążenie do realizacji własnych zamierzeń przy użyciu wszelkich dostępnych środków, w tym także metod niezgodnych z prawem. Takie działania mogą dotyczyć różnych obszarów funkcjonowania państwa będącego celem dezinformacji – zwłaszcza kwestii związanych z bezpieczeństwem. Zarówno obronnością, jak i bezpieczeństwem wewnętrznym, gospodarką (na przykład bezpieczeństwem energetycznym czy dostępem do kluczowych surowców), pozycją międzynarodową (w tym wiarygodnością i możliwościami negocjacyjnymi), a także relacjami między państwem a obywatelami (np. podstawowymi wartościami demokratycznymi, jak przejrzystość życia publicznego czy uczciwość wyborów). Kluczową rolę w tym procesie odgrywa środowisko informacyjne, które

staje się narzędziem wywierania presji na instytucje zarządzające państwem (NASK Państwowy Instytut Badawczy, 2024).

Dezinformacja nastawiona jest na tworzenie zamieszania oraz promowanie wyniku końcowego. Może być ona skierowana do określonej wyimaginowanej grupy odbiorów może zawierać całościowe lub częściowo fałszywe stwierdzenia, a także sensacyjne nagłówki mające na celu przyciągnięcie uwagi (Hetmański, 2003).

Dezinformacja funkcjonuje według podobnych zasad jak reklama. Kluczowe znaczenie mają tutaj emocje, jakie pojawiają się u odbiorcy w momencie zetknięcia się z nową informacją. Uczucia takie jak gniew, smutek, radość czy zaskoczenie sprawiają, że wiele osób nie analizuje źródła ani wiarygodności przekazu, zwłaszcza w środowisku mediów społecznościowych. Charakterystycznym elementem czarnej propagandy w sieci jest nadawanie fałszywej wiarygodności przedstawianym informacjom. Zamiast odwoływać się do autorytetów branżowych lub instytucji państwowych, często stosuje się chwytliwe słowa kluczowe, które mają przekonać odbiorców do prawdziwości przekazu (Urban, 2009).

Internet a co za tym idzie media społecznościowe również ma ogromny wpływ na rozprzestrzenianie dezinformacji i wprowadzanie społeczeństwa w błąd, głównie dzięki swojej globalnej dostępności przez całą dobę oraz szerokiemu zasięgowi oddziaływania. Wystarczy dostęp do sieci, by dotrzeć do niemal każdego miejsca na świecie. Dodatkowo, brak skutecznej weryfikacji publikowanych treści sprawia, że łatwo jest rozpowszechniać nieprawdziwe informacje. Dopóki autorzy fałszywych wiadomości nie złamią wyraźnych zasad obowiązujących na portalach społecznościowych czy serwisach informacyjnych, takich jak zakaz szerzenia nienawiści, przypisywania publicznym osobom nieprawdziwych wypowiedzi, nawoływania do przestępstw czy obrażania uczuć religijnych ich treści rzadko podlegają blokadzie. Nawet jeśli pojawią się sprostowania lub wyjaśnienia, nie zmienia to faktu, że pierwotna dezinformacja nadal krąży po internecie, prowadząc do nieporozumień i sporów wśród użytkowników (Stelmaszczyk, 2023).

Typologia dezinformacji w mediach społecznościowych

Współczesne media społecznościowe stały się jednym z głównych kanałów dystrybucji dezinformacji, co wynika zarówno z ich powszechnej

dostępności, jak i specyfiki mechanizmów komunikacji online (Kmiecik, 2019).

Thomas Aichner oraz Frank. H. Jacob wyróżnili katalog mediów społecznościowych do którego zaliczają się:

1. Blogi – osobiste wpisy komentowane przez innych.
2. Sieci biznesowe – kontakty zawodowe i wymiana doświadczeń.
3. Wspólne projekty – współpraca nad treściami, np. Wikipedia.
4. Fora internetowe – dyskusje tematyczne, brak rozmów w czasie rzeczywistym.
5. Sieci społecznościowe firm – integracja pracowników wewnątrz firmy.
6. Mikroblogi – krótkie, ograniczone wpisy (np. Twitter).
7. Udostępnianie zdjęć – publikowanie i komentowanie fotografii.
8. Recenzje – opinie o produktach i usługach.
9. Social bookmarking – dzielenie się zakładkami (np. Pinterest).
10. Społeczności gier – interakcje graczy online.
11. Portale społecznościowe – tworzenie profili i grup (np. Facebook).
12. Udostępnianie wideo – publikacja i komentowanie filmów.
13. Wirtualne światy – interakcja przez awatary w cyfrowych środowiskach (Aichner, Jacob, 2025).

Warto zwrócić uwagę iż, katalog ten podlega ciągłej ewolucji, w miejsce mniej używanych mediów społecznościowych mogą pojawiać się nowe, cieszące się większą popularnością.

W literaturze przedmiotu oraz licznych raportach badawczych wyróżnia się kilka podstawowych form dezinformacji, które szczególnie często pojawiają się w przestrzeni mediów społecznościowych. Pierwszą i najbardziej rozpoznawalną kategorią są tzw. fake newsy, czyli fałszywe informacje podszywające się pod treści pochodzące z wiarygodnych źródeł (Gov.pl, 2023). Fake newsy mają na celu przede wszystkim wywołanie silnych emocji, takich jak gniew, lęk czy zaskoczenie, a także polaryzację opinii publicznej. Bardzo często są one konstruowane w taki sposób, by wydawały się autentyczne. Wykorzystuje się w tym celu szatę graficzną przypominającą portale informacyjne, powoływanie się na fikcyjnych ekspertów, czy manipulację zdjęciami i nagłówkami. Zjawisko fake newsów jest szczególnie niebezpieczne w okresach zwiększonego napięcia społecznego, na przykład podczas kampanii wyborczych, kryzysów politycznych czy konfliktów

międzynarodowych. Fałszywe wiadomości rozprzestrzeniają się w mediach społecznościowych znacznie szybciej niż rzetelne informacje, co wynika z mechanizmów wiralności oraz algorytmów promujących treści budzące emocje (Raport Cyberprofilaktyka, 2023).

Drugą istotną formą dezinformacji jest propaganda, rozumiana jako długofalowe, systematyczne działania komunikacyjne, których celem jest kształtowanie i zmiana postaw politycznych lub społecznych określonych grup odbiorców. Propaganda nie zawsze wiąże się z przekazywaniem nieprawdziwych informacji. Często polega na selektywnym doborze faktów, manipulacji kontekstem czy powtarzaniu określonych narracji. W mediach społecznościowych propaganda może przyjmować różne formy. Od regularnych publikacji i kampanii informacyjnych, poprzez wykorzystywanie tzw. botów internetowych, aż po współpracę z influencerami czy mikrocelebrytami, którzy świadomie lub nie wzmacniają przekaz propagandowy. Propaganda jest szczególnie skuteczna w środowisku cyfrowym, gdzie łatwo jest dotrzeć do szerokiego grona odbiorców i precyzyjnie targetować przekaz do wybranych grup społecznych (Kaczmarek, 2024).

Kolejną formą dezinformacji jest trolling i hejt, których to w mediach społecznościowych jest coraz więcej. Trolling w przestrzeni internetowej stanowi złożone zjawisko komunikacyjne, polegające na celowym zamieszczaniu prowokacyjnych, obraźliwych bądź wprowadzających w błąd treści, których głównym celem jest wywołanie silnych reakcji emocjonalnych u innych uczestników dyskusji lub zakłócenie jej przebiegu. Osoby dopuszczające się trollingu, określane mianem „trolli", często korzystają z anonimowości oferowanej przez środowisko cyfrowe, co sprzyja eskalacji konfliktów oraz generowaniu chaosu informacyjnego. Trolling może przybierać formy od subtelnych aluzji i ironii, po jawną agresję słowną czy dezinformację. W literaturze przedmiotu podkreśla się, że działania trolli nie zawsze motywowane są rzeczywistą wrogością wobec innych użytkowników, lecz często stanowią formę zabawy, eksperymentowania z tożsamością lub próbę uzyskania poczucia kontroli nad przebiegiem interakcji online. Instrumentalizacja mediów społecznościowych takich jak Twitter, Instagram czy Facebook, doprowadziła do sytuacji, gdzie dla potrzeb walki informacyjnej np. Rosja, korzysta z płatnych usług blogerów oraz tzw. fabryki trolli (Kuczma, 2016). Hejt natomiast, określany również jako mowa nienawiści, odnosi się do wszelkich przejawów agresji słownej, obrażania, poniżania lub wykluczania

osób bądź grup społecznych ze względu na ich cechy indywidualne, światopogląd, pochodzenie czy przynależność do określonej kategorii społecznej. Hejt charakteryzuje się intencjonalnością oraz ukierunkowaniem na konkretnych odbiorców, co często prowadzi do ich stygmatyzacji, wykluczenia społecznego, a w skrajnych przypadkach także do poważnych konsekwencji psychologicznych. Współczesne badania wskazują, że hejt w środowisku internetowym jest zjawiskiem powszechnym i trudnym do zwalczania, m.in. ze względu na szybkie tempo rozprzestrzeniania się treści oraz trudności w identyfikacji sprawców. Zarówno hejt jak i trolling są poważnym zagrożeniem dla bezpieczeństwa państwa, ponieważ mogą prowadzić do destabilizacji sytuacji wewnętrznej, osłabienia zaufania do instytucji publicznych oraz pogłębiania podziałów społecznych (Dziwak, 2019).

Ostatnią wyróżnianą kategorią jest astroturfing, czyli praktyka polegająca na tworzeniu pozornie spontanicznych ruchów społecznych lub inicjatyw oddolnych, które w rzeczywistości są sterowane przez konkretne grupy interesu. Nazwa astroturfing pochodzi od sztucznej trawy (ang. astroturf), co symbolizuje sztuczność tych działań. W praktyce polega to na zakładaniu fałszywych kont w mediach społecznościowych, fałszywych tożsamości, tworzeniu grup dyskusyjnych czy inicjowaniu działań, które mają sprawiać wrażenie autentycznych. Astroturfing jest wykorzystywany zarówno przez podmioty komercyjne, jak i polityczne, a jego celem jest wywarcie wpływu na opinię publiczną poprzez kreowanie iluzji masowego poparcia lub sprzeciwu wobec danej sprawy. Astroturfing jest szczególnie trudny do wykrycia, ponieważ często wykorzystuje zaawansowane techniki ukrywania tożsamości oraz automatyzacji działań (np. boty, farmy trolli) (Gałek, 2022).

Typologia dezinformacji w mediach społecznościowych obejmuje szereg zróżnicowanych zjawisk, które wraz z postępem technologicznym ewaluują i pojawiają się nowe wykorzystujące zawansowane narzędzia sztucznej inteligencji. Łączy je jednak wspólny cel – manipulowanie opinią publiczną i osiąganie określonych korzyści przez twórców tych działań. Różnorodność form i metod stosowanych w przestrzeni cyfrowej sprawia, że przeciwdziałanie dezinformacji jest niezwykle trudne i wymaga zarówno działań edukacyjnych, jak i rozwiązań technologicznych oraz prawnych.

Mechanizmy dezinformacji w mediach społecznościowych

Dezinformacja w mediach społecznościowych jest wspierana przez szereg mechanizmów technologicznych i społecznych, które zwiększają jej skuteczność i skalę oddziaływania. Do najważniejszych należą:

1. Boty to programy komputerowe, których zadaniem jest automatyczne wykonywanie określonych czynności w przestrzeni internetowej. W kontekście dezinformacji są to najczęściej fałszywe, zautomatyzowane konta, które imitują aktywność prawdziwych użytkowników. Ich głównym celem jest wzmacnianie wybranych treści poprzez masowe polubienia, udostępnienia oraz komentowanie postów i artykułów. Dzięki postępowi technologicznemu coraz trudniej odróżnić boty od autentycznych profili, co stanowi poważne wyzwanie dla użytkowników i administratorów portali. Boty działają zazwyczaj w dużych, zorganizowanych grupach – tzw. farmach botów – obejmujących nawet tysiące kont, umożliwiając tym samym szybkie i tanie manipulowanie przekazem na szeroką skalę.
2. Zorganizowane Sieci Trolli są wykorzystywane do masowego rozpowszechniania fałszywych informacji, kreowania sztucznego poparcia dla określonych narracji oraz wzmacniania wybranych przekazów. Troll to rzeczywisty użytkownik mediów społecznościowych, który poprzez swoją aktywność celowo wywołuje konflikty, podziały oraz wzmacnia chaos i zamieszanie, utrudniając prowadzenie merytorycznej dyskusji.
3. Algorytmy rekomendacyjne i bańki informacyjne stosowane przez platformy społecznościowe personalizują przekaz, dostosowując wyświetlane treści do preferencji użytkownika. Prowadzi to do powstawania tzw. baniek informacyjnych, w których odbiorca jest narażony na powtarzające się, często zmanipulowane lub fałszywe komunikaty, wzmacniające jego wcześniejsze przekonania.
4. Manipulacja materiałami wizualnymi – dezinformacja coraz częściej wykorzystuje zmanipulowane zdjęcia, filmy, memy i grafiki, które oddziałują na emocje odbiorców i zwiększają wiarygodność fałszywych informacji (NASK Państwowy Instytut Badawczy, 2024).

5. Astroturfing i sterowane kampanie społeczne. Tworzenie pozornie spontanicznych ruchów i akcji społecznych, które w rzeczywistości są sterowane przez wyspecjalizowane podmioty, pozwala na wywieranie presji na instytucje państwowe oraz kształtowanie opinii publicznej (Gałek, 2022).
6. Targetowanie przekazu. Zaawansowane narzędzia analityczne i reklamowe umożliwiają precyzyjne kierowanie treści do wybranych grup odbiorców, z uwzględnieniem ich przekonań politycznych, zainteresowań czy emocji. To zwiększa skuteczność kampanii dezinformacyjnych, szczególnie w okresach napięć społecznych i politycznych (Fundacja DigitalPoland, 2024).

Wpływ dezinformacji na bezpieczeństwo narodowe

Dezinformacja rozumiana jako intencjonalne wprowadzanie w błąd za pomocą treści cyfrowych stała się jednym z kluczowych wektorów zagrożeń informacyjnych i może prowadzić do szeregu negatywnych skutków dla bezpieczeństwa państwa. Wśród nich wymienia się: destabilizację procesów politycznych, w tym wybory i funkcjonowanie instytucji państwowych; podważanie zaufania społecznego do instytucji publicznych; wzrost polaryzacji społecznej i napięć; osłabienie morale obywateli oraz służb państwowych w sytuacjach kryzysowych; wpływ na decyzje ekonomiczne i polityczne poprzez manipulację opinią publiczną (Kaczmarek, 2024).

Według raportu Digital Poland, ponad 60% Polaków uznaje dezinformację za realne zagrożenie dla stabilności państwa, a 70% dostrzega jej wpływ na bezpieczeństwo narodowe (Fundacja DigitalPoland, 2024). W debacie eksperckiej i w analizach instytucji publicznych coraz częściej ujmuje się ją w szerszej kategorii FIMI (Foreign Information Manipulation and Interference), tj. obcych manipulacji i ingerencji informacyjnych, które oddziałują na procesy polityczne, bezpieczeństwo wewnętrzne oraz odporność społeczną (Bryjka, 2024). W Polsce zagrożenia te są systemowo rozpoznawane m.in. w publikacjach Biura Bezpieczeństwa Narodowego i Rządowego Centrum Bezpieczeństwa, które wiążą dezinformację z hybrydowym charakterem współczesnych konfliktów i koniecznością integracji reakcji

państwa. Zagrożenia te mogą przyjąć różne mechanizmy oddziaływania na bezpieczeństwo państwa:

1) Erozja zaufania i odporności społecznej.

Stała ekspozycja na zmanipulowane treści w mediach społecznościowych obniża zaufanie do instytucji i ekspertów, utrudnia akceptację działań władz w sytuacjach kryzysowych oraz sprzyja polaryzacji. Dane z polskiego badania *„Dezinformacja oczami Polaków 2024"* pokazują, że 79 % respondentów w 2024 roku zetknęła się z fałszywymi informacjami, a zdaniem 81 % z nich, zjawisko ich rozpowszechniania nasiliło się w ciągu minionej dekady. Znaczna część z nich uznała fałszywe informacje za prawdziwe, co ilustruje skalę podatności środowiska informacyjnego (Fundacja DigitalPoland, 2024).

2) Naruszanie integralności procesów demokratycznych.

Media społecznościowe ułatwiają mikrotargetowanie emocjonalnych przekazów i koordynację kampanii wpływu z wykorzystaniem botów, a także kradzionych oraz sfałszowanych kont, co zwiększa ryzyko zakłócania kampanii wyborczych i przebiegu samego głosowania. Polskie analizy wskazują na taktyki stosowane przed wyborami oraz ich nasilenie w ostatnich 72 godzinach poprzedzających wybory. Taka działalność ma charakter manipulacyjny, jest prowadzona w sposób celowy i skoordynowany i może negatywnie wpłynąć na procesy polityczne (Legucka, 2024). Operacje wpływu podważają legitymizację instytucji, osłabiają procesy wyborcze i deliberację publiczną. Rozwarstwienie informacyjne i polaryzacja utrudniają zarządzanie kryzysowe i komunikację ryzyka. (Bryjka, 2024).

3) Integracja z działaniami hybrydowymi.

W perspektywie obronnej dezinformacja stanowi jeden z kluczowych elementów współczesnej walki informacyjnej, ujmowanej jako zorganizowany i celowy proces oddziaływania na percepcję, postawy oraz decyzje odbiorców poprzez manipulowanie zasobami informacyjnymi. W literaturze przedmiotu podkreśla się, że działania dezinformacyjne są ściśle powiązane z realizacją celów militarnych, umożliwiają one m.in. maskowanie rzeczywistych intencji operacyjnych, wprowadzanie przeciwnika w błąd, a także osłabianie morale zarówno sił zbrojnych, jak i społeczeństwa państwa będącego celem ataku (Kaczmarek, 2024).

Analizy prowadzone na łamach „Kwartalnika Bezpieczeństwo Narodowe" oraz w raportach Rządowego Centrum Bezpieczeństwa wskazują, że doświadczenia wyniesione z konfliktu zbrojnego w Ukrainie uwidoczniły nowy wymiar walki informacyjnej, w której cyberprzestrzeń i media społecznościowe stają się areną intensywnych działań propagandowych oraz kampanii dezinformacyjnych. Zjawisko to określa się „szumem informacyjnym", polegającym na celowym zalewaniu przestrzeni publicznej nadmiarem sprzecznych, niezweryfikowanych lub zmanipulowanych przekazów, co utrudnia odbiorcom odróżnienie informacji prawdziwych od fałszywych (Włodyka, 2024).

Wojna w Ukrainie stanowi przykład synergicznego wykorzystania narzędzi cybernetycznych oraz kampanii narracyjnych w mediach społecznościowych, gdzie ataki hakerskie, sabotaż teleinformatyczny oraz szeroko zakrojone operacje dezinformacyjne były ze sobą ściśle skoordynowane. Celem tych działań było nie tylko uzyskanie przewagi operacyjnej na polu walki, ale również destabilizacja zaplecza społeczno-politycznego przeciwnika, wywołanie paniki, a także zdezorganizowanie systemów komunikacji i zarządzania kryzysowego. Połączenie cyberataków, operacji psychologicznych i kampanii narracyjnych w mediach społecznościowych tworzy efekt synergii (Pelc, 2024).

4) Bezpieczeństwo wewnętrzne i porządek publiczny.

Fale dezinformacji dotyczące zdrowia publicznego, migracji czy bezpieczeństwa mogą generować panikę, eskalować napięcia oraz obciążać administrację publiczną i służby. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) – w ramach programu *„Przeciwdziałamy dezinformacji"* – dokumentuje metody i taktyki wykorzystywane w Polsce oraz prowadzi działania ostrzegawcze i edukacyjne adresowane do instytucji i obywateli. Z przeprowadzonego badania wynika, że 87% badanych jest przekonanych, że zjawisko dezinformacji wywarło już duży wpływ na życie publiczne w ich kraju (NASK Państwowy Instytut Badawczy, 2024).

5) Nowa dynamika ryzyka: generatywna AI.

Najnowsze analizy z zakresu bezpieczeństwa informacyjnego podkreślają rosnące znaczenie treści syntetycznych – takich jak generowane komputerowo obrazy, nagrania audio oraz materiały wideo w kontekście podatności platform społecznościowych na manipulacje informacyjne. Zjawisko

to jest szczególnie widoczne w świetle dynamicznego rozwoju narzędzi sztucznej inteligencji, które umożliwiają nie tylko automatyzację, ale i znaczące przyspieszenie procesu tworzenia materiałów o wysokim stopniu wiarygodności percepcyjnej. Warto zwrócić szczególną uwagę, że współczesne algorytmy generatywne, które pozwalają na produkcję treści trudnych do odróżnienia od autentycznych, co znacząco utrudnia skuteczną weryfikację źródeł informacji przez użytkowników oraz moderatorów platform społecznościowych. Ponadto, mechanizmy rekomendacyjne tych platform sprzyjają szybkiej i szerokiej dystrybucji syntetycznych materiałów, zwiększając tym samym zasięg potencjalnych kampanii dezinformacyjnych. Niepokojącym aspektem, jest również zagrożenie związane z „uczeniem" modeli sztucznej inteligencji na danych już skażonych dezinformacją. Proces ten może prowadzić do powstawania błędnych lub zniekształconych wzorców decyzyjnych w systemach AI, co w konsekwencji wzmacnia efekt dezinformacyjny poprzez dalszą automatyczną produkcję i dystrybucję fałszywych treści. Oznacza to, że nie tylko użytkownicy, ale także same technologie cyfrowe stają się podatne na manipulacje, co stwarza nowe wyzwania dla systemów bezpieczeństwa informacyjnego państwa (Wójtowicz, 2025).

Przykłady kampanii dezinformacyjnych w Polsce

W ostatnich latach w Polsce wykryto szereg kampanii dezinformacyjnych. Dezinformacja w mediach społecznościowych najczęściej nasila się w okresach podwyższonego napięcia społecznego i politycznego. Szczególnie podatne na manipulację są tematy związane z bezpieczeństwem narodowym, kryzysami migracyjnymi, pandemią oraz konfliktami międzynarodowymi, z których najbardziej znaczące dotyczyły wojny w Ukrainie oraz pandemii COVID-19.

1. Dezinformacja wokół wojny w Ukrainie.

W ciągu dwóch dni poprzedzających rosyjską inwazję na Ukrainę (24 lutego 2022 roku) Instytut Badań Internetu i Mediów Społecznościowych (IBIMS) odnotował znaczący wzrost liczby publikacji w polskiej przestrzeni informacyjnej, których celem było wywołanie poczucia zagrożenia ze strony obywateli Ukrainy. Wśród najczęściej pojawiających się sformułowań

w odniesieniu do Ukrainy dominowały takie zwroty jak „banderowcy", „UPA", „rzeź Polaków" czy „ludobójstwo" (ibims.pl, 2024).

W raporcie Digital Poland opisano zorganizowane kampanie polegające na rozpowszechnianiu fałszywych informacji dotyczących działań wojennych, rzekomych zbrodni ukraińskich żołnierzy oraz zagrożeń związanych z napływem uchodźców. Przykładem były zmanipulowane zdjęcia i filmy publikowane na Facebooku i Twitterze, które miały wywołać strach i niechęć wobec uchodźców oraz podważyć zaufanie do polskich władz. Jednym z istotnych elementów działań dezinformacyjnych, wymierzonych w solidarność społeczeństw Unii Europejskiej z Ukrainą, jest również szerzenie fałszywych narracji dotyczących rzekomo dramatycznej sytuacji gospodarczej państw członkowskich. Przekazy te sugerują, że wsparcie udzielane Ukrainie generuje ogromne koszty, które mają prowadzić do poważnych problemów ekonomicznych całej wspólnoty. W ramach takich kampanii pojawiają się nieprawdziwe informacje o domniemanych planach władz UE, mających na celu na przykład przejmowanie kont bankowych obywateli czy wprowadzanie drastycznych ograniczeń finansowych, rzekomo w odpowiedzi na wydatki związane z pomocą dla uchodźców i wsparciem dla Ukrainy (Wolska, 2024). Tego typu przekazy mają wywoływać niepokój, wzbudzać poczucie zagrożenia oraz zniechęcać do dalszego okazywania wsparcia naszym wschodnim sąsiadom, jednocześnie podważając zaufanie do instytucji unijnych i polityki solidarnościowej.

2. Dezinformacja w okresie pandemii COVID-19.

Według analiz Cyberprofilaktyka.pl, okres pandemii COVID-19 charakteryzował się intensyfikacją działań dezinformacyjnych mających na celu szerzenie fałszywych informacji na temat szczepień, potencjalnych skutków ubocznych oraz różnego rodzaju teorii spiskowych związanych z pochodzeniem i przebiegiem pandemii. W procesie tym wykorzystywano zarówno zautomatyzowane konta, jak i osoby publiczne oraz influencerów, którzy często nieświadomie przyczyniali się do upowszechniania nieprawdziwych treści w mediach społecznościowych (Raport Cyberprofilaktyka, 2023).

Szczególnie aktywne były rosyjskie konta, które już wcześniej zajmowały się propagowaniem postaw antyszczepionkowych oraz negowaniem istnienia wirusa SARS-CoV-2. Profile te wykorzystywały różnorodne techniki manipulacji, by wzmacniać przekaz dezinformacyjny, docierać do szerokiego grona odbiorców i budować atmosferę nieufności wobec oficjalnych

zaleceń zdrowotnych oraz instytucji publicznych. W efekcie tego typu działania przyczyniały się do wzrostu sceptycyzmu wobec szczepień, utrudniały walkę z pandemią i osłabiały społeczną solidarność w obliczu kryzysu zdrowotnego.

3. Dezinformacja w kampaniach wyborczych.

Przypadki rozpowszechniania fałszywych informacji o kandydatach, manipulowania wynikami sondaży oraz szerzenia fake newsów mających na celu polaryzację społeczną i wpłynięcie na decyzje wyborców również pojawiały się w mediach społecznościowych. Przykładem była kampania przed wyborami parlamentarnymi w 2023 roku, podczas której zidentyfikowano zorganizowane sieci trolli publikujące zmanipulowane materiały (Legucka, 2024). Celem takiego ukierunkowanego oddziaływania jest selektywna mobilizacja. – chodzi o to, by zachęcić do udziału w głosowaniu osoby popierające daną partię lub potencjalnie skłonne ją poprzeć, a jednocześnie zniechęcić do udziału wyborców konkurencji. Ma to szczególne znaczenie, ponieważ współczesne kampanie wyborcze coraz rzadziej koncentrują się na przekonywaniu elektoratu do zmiany preferencji partyjnych, a zamiast tego skupiają się przede wszystkim na aktywizowaniu własnych zwolenników oraz demobilizowaniu sympatyków przeciwników (Cześnik, Miśta, Żerkowska-Balas, 2020).

Mikrotargetowanie reklam politycznych stało się głośnym tematem po kampanii prezydenckiej Donalda Trumpa w 2016 roku, kiedy to na Facebooku jednocześnie emitowano dziesiątki tysięcy różnych reklam. Brak przejrzystości sprzyjał nie tylko mobilizacji własnych wyborców, ale też prowadzeniu kampanii negatywnej zniechęcającej potencjalnych zwolenników przeciwnika do udziału w wyborach. Obecnie platformy takie jak Meta i Google umożliwiają bardzo precyzyjne docieranie do użytkowników według wielu kryteriów: demografii, lokalizacji, zainteresowań czy zachowań w sieci. Reklamodawcy mogą też tworzyć własne grupy odbiorców, np. na podstawie wizyt na stronie internetowej lub podobieństwa do wybranych użytkowników. W Polsce podobne praktyki pojawiły się np. podczas kampanii samorządowej w 2018 roku, kiedy na Facebooku powstały strony wyśmiewające kandydatów. Publikowały one reklamy skierowane do konkretnych grup, by zniechęcić je do udziału w głosowaniu. Takie działania, prowadzone poza oficjalnymi kampaniami wyborczymi, budzą wątpliwości związane z przejrzystością i finansowaniem kampanii. Negatywne kampanie

prowadzone przez podmioty niezwiązane oficjalnie z komitetami wyborczymi są problematyczne ze względu na brak kontroli, przejrzystości i możliwość obchodzenia przepisów dotyczących finansowania. W Polsce takie działania nie zdążyły się upowszechnić, ponieważ od 2019 roku Facebook wprowadził obowiązek rejestracji i oznaczania reklam politycznych oraz udostępnił tzw. bibliotekę reklam, co zwiększyło transparentność (Batorski, Izdebski, 2023). Dodatkowo, od wyborów do Parlamentu Europejskiego w 2024 roku, nowe unijne regulacje jeszcze bardziej poprawią przejrzystość reklamy politycznej w sieci (Rozporządzenie Parlamentu Europejskiego i Rady sprawie przejrzystości i targetowania reklamy politycznej, 2021). Ograniczona skala takich działań wynika z kilku czynników: rosnącej przejrzystości, niższych budżetów kampanijnych niż np. w USA oraz rygorystycznych przepisów dotyczących ochrony danych osobowych w Europie. Największym wyzwaniem pozostaje jednak weryfikacja finansowania reklam, ponieważ obecny system sprawozdawczości nie pozwala w pełni kontrolować, czy wszystkie wydatki są prawidłowo rozliczane w kampaniach wyborczych.

Warto zauważyć, że polityczna aktywność w internecie jest niemal nieprzerwana. Kampania wyborcza trwa przez cały czas. Politycy i partie systematycznie prowadzą działania informacyjne i dbają o stałe zwiększanie zasięgów. Liczba obserwujących i poziom zaangażowania użytkowników pozostają wysokie. Przykładowo, od stycznia 2021 do czerwca 2022 roku na Facebooku codziennie reagowało na treści PiS co najmniej 10 tysięcy osób, a Platformy Obywatelskiej – co najmniej 20 tysięcy. Średnio było to odpowiednio niemal 16 tysięcy i 35 tysięcy zaangażowanych użytkowników dziennie (Batorski, Izdebski, 2023).

Systematyczne raporty m.in. Fundacji Batorego czy Rządowego Zespołu ds. Dezinformacji (Gov.pl, 2023) pokazują, jak platformy społecznościowe stają się polem zarówno legalnej komunikacji politycznej, jak i dezinformacji o charakterze kampanijnym.

Narzędzia monitorowania i przeciwdziałania dezinformacji

Polskie instytucje państwowe oraz organizacje pozarządowe wdrażają szereg rozwiązań mających na celu ograniczenie skutków dezinformacji w mediach społecznościowych. NASK, Digital Poland oraz Demagog.org.pl prowadzą systematyczny monitoring mediów społecznościowych,

identyfikując fałszywe informacje, analizując źródła i skalę zjawiska. Użytkownicy, którzy natkną się na podejrzaną informację mają możliwość jej zgłaszania. W raporcie Digital Poland podkreślono znaczenie automatycznych narzędzi analitycznych, które pozwalają na szybkie wykrywanie kampanii dezinformacyjnych i informowanie opinii publicznej o zagrożeniach (Fundacja DigitalPoland, 2024).

Skuteczna walka z dezinformacją wymaga wielowymiarowych działań, wśród których kluczową rolę odgrywa edukacja. Podnoszenie świadomości społecznej na temat zagrożeń związanych z dezinformacją powinno koncentrować się na rozwijaniu krytycznego myślenia, umiejętności oceny wiarygodności źródeł oraz sprawdzania faktów. Istotne jest również wdrażanie programów nauczania, które uczą kompetencji medialnych i pomagają rozpoznawać techniki manipulacji oraz stronniczość przekazów. Ważną rolę w przeciwdziałaniu dezinformacji pełnią same platformy społecznościowe, które zobowiązane są do usuwania fałszywych treści, ograniczania zasięgu kont rozpowszechniających dezinformację oraz współpracy z niezależnymi organizacjami zajmującymi się weryfikacją faktów. Tradycyjne media także powinny wykazywać się odpowiedzialnością, rzetelnie weryfikując informacje przed publikacją. Odpowiedzialność za kształtowanie bezpiecznego środowiska informacyjnego spoczywa także na samych użytkownikach, którzy powinni krytycznie oceniać treści i dbać o wiarygodność przekazywanych informacji. Wreszcie, niezbędne są działania legislacyjne, które ograniczają zasięg dezinformacji, jednocześnie respektując fundamentalne zasady wolności słowa.

Polska aktywnie uczestniczy w międzynarodowych inicjatywach na rzecz przeciwdziałania dezinformacji, współpracując z UE, NATO oraz organizacjami pozarządowymi. W raporcie Biura Bezpieczeństwa Narodowego podkreślono znaczenie wymiany informacji i doświadczeń w zakresie identyfikacji oraz neutralizacji zagrożeń dezinformacyjnych Prawo polskie oraz regulacje unijne przewidują szereg mechanizmów umożliwiających walkę z dezinformacją. Kluczowa jest konieczność dostosowania przepisów do dynamicznie zmieniającego się środowiska cyfrowego oraz na wyzwania związane z egzekwowaniem prawa wobec międzynarodowych korporacji technologicznych.

Podsumowanie

Współczesna dezinformacja w polskich mediach społecznościowych to zjawisko, którego skala i złożoność rosną z każdym rokiem. Nie jest to już tylko problem kilku fałszywych postów czy pojedynczych kont trolli, a systemowy mechanizm wpływania na całe społeczeństwo, mogący podważać zaufanie obywateli do instytucji państwa, procesów wyborczych czy nawet codziennych relacji międzyludzkich. W dobie narzędzi generatywnych, takich jak sztuczna inteligencja zdolna do tworzenia realistycznych tekstów, obrazów czy filmów, granica między prawdą, a fałszem staje się coraz trudniejsza do uchwycenia. To sprawia, że odbiorcy mediów muszą być nie tylko czujni, ale także aktywnie poszukiwać rzetelnych informacji, weryfikować źródła i kwestionować to, co widzą w internecie.

Walka z dezinformacją nie może opierać się wyłącznie na reakcji na poszczególne przypadki. Potrzebne jest systemowe podejście, które zaczyna się od edukacji. Wzmacnianie kompetencji cyfrowych i medialnych powinno być priorytetem zarówno w szkołach, jak i w programach dla osób dorosłych, a szczególnie osób starszych. Społeczeństwo musi nauczyć się rozpoznawać techniki manipulacji, rozumieć mechanizmy działania algorytmów oraz świadomie korzystać z mediów społecznościowych. Tylko wtedy możliwe będzie budowanie odporności na fałszywe przekazy i manipulacje.

Równie ważne jest rozwijanie zaawansowanych narzędzi monitorowania treści w internecie oraz szybkiego reagowania na pojawiające się dezinformacje. Tu kluczowa staje się współpraca między państwem, organizacjami pozarządowymi, sektorem prywatnym i samymi użytkownikami. Instytucje publiczne muszą być otwarte na dialog ze społeczeństwem obywatelskim, wspierać działania fact-checkerów i aktywistów, a także inwestować w technologie wykrywania fałszywych treści.

Wyzwania technologiczne wymagają również nowoczesnych regulacji prawnych, które będą nadążać za zmianami w sposobach rozpowszechniania informacji. Prawo powinno chronić obywateli przed szkodliwymi treściami, nie ograniczając przy tym wolności słowa i dostępu do różnorodnych opinii. To trudna równowaga, ale niezbędna dla zachowania zdrowej debaty publicznej.

Nie można też zapominać o potrzebie prowadzenia systematycznych badań nad mechanizmami dezinformacji. Tylko dzięki pogłębionemu rozumieniu tego zjawiska, zarówno na poziomie technologicznym, jak

i społecznym będzie możliwe przewidywanie nowych zagrożeń i opracowywanie skutecznych strategii przeciwdziałania. Przyszłość walki z dezinformacją zależy od aktywnego zaangażowania wszystkich uczestników życia publicznego, gotowości do uczenia się i adaptacji oraz otwartości na współpracę ponad podziałami.

Literatura

1. Aichner, T., Jacob, F. H. (2015). Measuring the Degree of Corporate Social Media Use. *International Journal of Market Research, 57*(2), 257-276. https://doi.org/10.2501/IJMR-2015-018
2. Batorski, D., Izdebski, K. (2023). *Media społecznościowe i wybory*, Fundacja im. Stefana Batorego.
3. Bencsik, A., Karpiuk, M., Kelemen, M., Włodyka, E. (2023). *Cybersecurity in the Visegrad Group Countries, Institute for Local Self-Government*, Maribor.
4. Bryjka, F. (2024). *Ofensywa dezinformacyjna Rosji przeciwko Ukrainie*, *Biuletyn PISM, 46*(2856).
5. Bryjka, F. (2024). *Podejście UE do zwalczania obcych manipulacji informacyjnych i ingerencji*, Polski Instytut Spraw Międzynarodowych, nr 3.
6. Cześnik, M., Miśta, R., Żerkowska-Balas, M. (2020). Uczestnictwo i mobilizacja w wyborach parlamentarnych 2019 roku, *Studia Socjologiczne, 4*(239), 91-121.
7. Dziwak, E. (2019). Od egalitarności do inkluzywności. Hejt jako następstwo komercjalizacji internetu. *Zeszyty prasoznawcze*, t. *62*, nr 1, Kraków.
8. Fundacja DigitalPoland. (2024). Raport Dezinformacja oczami Polaków. Warszawa.
9. Gałek, B. (2022). Cyfrowy astroturfing jako instrument kreowania procesów politycznych. Zarys problematyki. *Studia Społeczno-Polityczne,* 19/2022, Siedlce.
10. Gov.pl. (b.d). *Rozpoznawanie nieprawdziwych informacji*. Pobrano z: https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych--informacji (dostęp: 20.03.2026).

11. Gov.pl. (2023). *Walka z dezinformacją w mediach społecznościowych: O czym należy wiedzieć?* Pobrano z: https://www.gov.pl/web/5g/walka-zdezinformacja-w-mediach-spolecznosciowych-o-czym-nalezy-wiedziec (dostęp: 20.03.2026).
12. Hetmański, M. (2003). *Społeczny charakter informacji, Społeczeństwo informatyczne, Szansa czy zagrożenie?*, Lublin.
13. Kaczmarek, K. (2024). Konsekwencje dezinformacji: Przegląd wybranych narzędzi i technik manipulacji. *Bezpieczeństwo narodowe*, 2024/45, Koszalin.
14. Kmiecik, P. (2019). *Bezpieczeństwo informacyjne Rzeczypospolitej w dobie fake news – przykłady wykorzystania mediów cyfrowych w szerzeniu dezinformacji*, Warszawa.
15. *Komunikat ws. dezinformacji ws. sytuacji na Ukrainie w internecie, Instytut Badań Internetu i Mediów Społecznościowych*. Pobrano z: https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ (dostęp: 02.11.2025).
16. Kuczma, K. (2016). *Dezinformacja jako instrument zwalczania polskich planów dywersyfikacji źródeł energii*, Securitologia, nr 2.
17. Legucka, A. (2024). Kampanie dezinformacyjne Rosji przed wyborami do Parlamentu Europejskiego. *PISM*, Nr 82 (2892).
18. Materska, K. (2007). *Informacja w organizacjach społeczeństwa wiedz*, Warszawa.
19. NASK Państwowy Instytut Badawczy. (2024). *Zjawisko dezinformacji w dobie rewolucji cyfrowej,* Warszawa.
20. NASK. (2024). *Jak przeciwdziałać dezinformacji? Poradnik dla administracji publicznej*.
21. NASK. (b.d.). *Przeciwdziałym dezinformacji*. https://www.nask.pl/weryfikuje?utm_source (dostęp: 20.03.2026).
22. Pelc, P. (2024). *Cyberprzestrzeń jako element walki informacyjnej – doświadczenie z konfliktu w Ukrainie*, Akademickie Centrum Polityki Cyberbezpieczeństwa, Akademia Sztuki Wojennej.
23. *Rozporządzenie Parlamentu Europejskiego i Rady sprawie przejrzystości i targetowania reklamy politycznej*, 2021.
24. Stelmaszczyk, Ł., Chrząszcz, A. (2023). Zagrożenia w Internecie, *Studia Społeczne*.
25. Urban, A. (2009). *Bezpieczeństwo społeczności lokalnych*, Warszawa.

26. Włodyka, E. M. (2024). *Polaryzacja, kohabitacja czy integracja? Wyzwania dla cyberbezpieczeństwa procesów wyborczych w Polsce*. Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe. Akademia Sztuki Wojennej.
27. Wójtowicz, A. (2025). Wpływ sztucznej inteligencji na dezinformację, *PISM*, NR 63 (3066).
28. Wolska, A. (2024). *Fejk tygodnia: UE jest na krawędzi bankructwa, więc będą zajmowane oszczędności obywateli*, EURACTIV.pl.
29. *Zjawisko dezinformacji w dobie rewolucji cyfrowej*. Raport Cyberprofilaktyka.pl. 2023.

Zuzanna Jordan[1]

https://doi.org/10.29316/9788368103359_11

PRAWO A DEZINFORMACJA – ANALIZA REGULACJI DOTYCZĄCYCH BEZPIECZEŃSTWA INFORMACYJNEGO W POLSCE I UE

LAW AND MISINFORMATION – AN ANALYSIS OF INFORMATION SECURITY REGULATIONS IN POLAND AND THE EU

Streszczenie

Dezinformacja stanowi jedno z kluczowych wyzwań dla współczesnych systemów bezpieczeństwa i porządku publicznego. W dobie dynamicznego rozwoju mediów społecznościowych oraz globalnego obiegu informacji, jej skutki wykraczają daleko poza sferę komunikacji, wpływając na stabilność instytucji demokratycznych, procesy wyborcze, oraz bezpieczeństwo narodowe. Rozdział przedstawia analizę regulacji prawnych dotyczących przeciwdziałania dezinformacji w Polsce oraz w Unii Europejskiej, ze szczególnym uwzględnieniem regulacji takich jak Digital Services Act, strategii UE dotyczących bezpieczeństwa informacyjnego oraz krajowych przepisów prawa. Celem rozdziału jest ocena skuteczności obowiązujących rozwiązań prawnych w kontekście zagrożeń bezpieczeństwa informacyjnego. Przeprowadzono

[1] https://orcid.org/0009-0009-2636-8501, email: zuzanna.jordan@protonmail.com

analizę aktów prawnych, literatury przedmiotu oraz strategii instytucjonalnych. Wskazano zarówno mocne strony istniejących regulacji (np. zwiększenie odpowiedzialności platform internetowych), jak i ich ograniczenia (np. brak precyzyjnych definicji i mechanizmów egzekucyjnych). Wnioski wskazują na potrzebę dalszego rozwoju ram prawnych oraz bliższej współpracy między państwami członkowskimi i sektorem prywatnym w celu skutecznego przeciwdziałania dezinformacji.

Słowa kluczowe: dezinformacja, bezpieczeństwo informacyjne, prawo, Digital Services Act, regulacje medialne

Abstract

Disinformation represents one of the key challenges to contemporary security systems and public order. In the era of rapid social media development and global information circulation, its effects extend far beyond communication, influencing the stability of democratic institutions, electoral processes, national security, and social cohesion. This chapter analyses legal regulations addressing disinformation in Poland and the European Union, with a particular focus on the Digital Services Act, EU information security strategies, and national regulations. The aim of the chapter is to assess the effectiveness of the existing legal framework in countering information security threats. Legal acts, relevant literature, and institutional strategies are analysed. The paper identifies both the strengths of the current regulations (e.g., increased accountability of online platforms) and their limitations (e.g., lack of precise definitions and enforcement mechanisms). The conclusions highlight the need for further development of legal frameworks and closer cooperation between EU Member States and the private sector to effectively counter disinformation.

Keywords: disinformation, information security, law, Digital Services Act, media regulation

Wstęp

Zjawisko dezinformacji w ostatnich latach stało się jednym z najpoważniejszych zagrożeń dla bezpieczeństwa informacyjnego zarówno w Polsce, jak i w całej Unii Europejskiej. Informacje rozchodzą się dziś szybciej niż kiedykolwiek wcześniej. Media społecznościowe, komunikatory, różnego rodzaju platformy internetowe umożliwiają błyskawiczne dotarcie z treściami do milionów odbiorców. Niestety, ten sam mechanizm jest

wykorzystywany do szerzenia fałszywych informacji, manipulowania opinią publiczną, czy wpływania na decyzje społeczne i polityczne. Dezinformacja przestała być wyłącznie problemem komunikacyjnym – obecnie stanowi realne zagrożenie dla stabilności instytucji demokratycznych, procesów wyborczych oraz bezpieczeństwa narodowego.

Unia Europejska i poszczególne państwa członkowskie zaczęły podejmować konkretne działania mające na celu przeciwdziałanie temu zjawisku. W ostatnich latach przyjęto m.in. Digital Services Act, który wprowadza nowe obowiązki dla dużych platform internetowych, mające ograniczyć skalę szkodliwych treści i zwiększyć ich odpowiedzialność. Oprócz tego pojawiły się różnego rodzaju strategie bezpieczeństwa informacyjnego na poziomie unijnym i krajowym. W Polsce działania te są prowadzone zarówno w ramach obowiązujących regulacji medialnych, jak i poprzez inicjatywy instytucjonalne, np. NASK czy Rządowe Centrum Bezpieczeństwa. Mimo tych wysiłków wiele problemów pozostaje nierozwiązanych. Wciąż brakuje precyzyjnych definicji pojęć związanych z dezinformacją, skutecznych mechanizmów egzekwowania prawa, a także odpowiedniego balansu między ochroną bezpieczeństwa a poszanowaniem wolności słowa.

Celem niniejszego rozdziału jest analiza obowiązujących regulacji prawnych dotyczących przeciwdziałania dezinformacji w Polsce oraz w Unii Europejskiej, a także ocena ich skuteczności w kontekście zagrożeń bezpieczeństwa informacyjnego. W opracowaniu zostaną omówione główne akty prawne i strategie, przedstawione ich mocne i słabe strony, a także zarysowane wyzwania oraz możliwe kierunki dalszych działań. Tekst opiera się na analizie aktów prawnych, dokumentów strategicznych, literatury naukowej oraz dostępnych raportów instytucjonalnych.

Kontekst prawny i strategiczny UE

Unia Europejska już od kilku lat uznaje dezinformację za realne zagrożenie dla bezpieczeństwa, stabilności politycznej i funkcjonowania demokratycznych instytucji. Szczególnie wyraźnie było to widać po 2016 roku, kiedy to różne kampanie dezinformacyjne zaczęły wpływać na wybory, referenda i debatę publiczną w wielu państwach członkowskich. W odpowiedzi UE rozpoczęła tworzenie ram prawnych oraz mechanizmów koordynacyjnych,

które mają przeciwdziałać rozprzestrzenianiu fałszywych treści i wzmacniać odporność społeczeństwa na manipulacje informacyjne.

Jednym z najważniejszych elementów tych działań jest Digital Services Act (DSA) – akt prawny, który zaczął obowiązywać w 2024 roku i stanowi kompleksową regulację dotyczącą funkcjonowania platform internetowych. DSA nie odnosi się wprost do pojęcia „dezinformacji", ale wprowadza szereg obowiązków, które mają pośrednio ograniczyć jej skalę i wpływ. Duże platformy (tzw. VLOP-y – very large online platforms), takie jak Facebook, YouTube czy X, muszą prowadzić regularne oceny ryzyka związanego z rozpowszechnianiem nielegalnych i szkodliwych treści. Są też zobowiązane do wdrażania skutecznych środków zaradczych, w tym m.in. mechanizmów moderacji, większej przejrzystości algorytmów oraz udostępniania danych niezależnym badaczom. W założeniu ma to zwiększyć odpowiedzialność platform i umożliwić skuteczniejsze reagowanie na kampanie dezinformacyjne (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065).

Kolejnym ważnym dokumentem jest Europejski Plan Działań na rzecz Demokracji (EDAP), przyjęty w 2020 roku. Plan ten zakłada m.in. wzmocnienie regulacji dotyczących reklamy politycznej w sieci, poprawę przejrzystości finansowania kampanii, a także rozwój niezależnych mediów i wsparcie dla organizacji fact-checkingowych (European Commission, 2020). W ramach EDAP duży nacisk położono na zwiększenie odporności społeczeństwa poprzez edukację medialną oraz promowanie krytycznego myślenia. Nie chodzi tylko o walkę z fałszywymi treściami „po fakcie", ale o budowanie długofalowej odporności obywateli na manipulację.

UE powołała również szereg struktur instytucjonalnych, które mają wspierać państwa członkowskie w reagowaniu na zagrożenia informacyjne. Ważną rolę odgrywa tu East StratCom Task Force, działająca w ramach Europejskiej Służby Działań Zewnętrznych (EEAS), która zajmuje się m.in. identyfikowaniem i analizowaniem kampanii dezinformacyjnych, głównie pochodzących z Rosji (European External Action Service, East StratCom Task Force, b.d.). Istotne znaczenie mają też tzw. Rapid Alert System – system szybkiego ostrzegania, który umożliwia wymianę informacji między instytucjami unijnymi i państwami członkowskimi w czasie rzeczywistym (European Commission, b.d.). Ma on pomóc w szybkim reagowaniu na zorganizowane kampanie dezinformacyjne, np. w okresach wyborczych czy podczas kryzysów.

W ostatnich latach UE zaczęła również kłaść większy nacisk na współpracę z sektorem prywatnym. Platformy internetowe są zobowiązane do uczestniczenia w Kodeksie postępowania w zakresie dezinformacji, który choć formalnie ma charakter dobrowolny, w praktyce stał się ważnym narzędziem nacisku regulacyjnego. Kodeks został zaktualizowany w 2022 roku, rozszerzając zakres obowiązków dotyczących przejrzystości reklam, walki z fałszywymi kontami i botami oraz wzmacniania współpracy z organizacjami fact-checkingowymi.

Podsumowując, działania Unii Europejskiej w zakresie przeciwdziałania dezinformacji opierają się na trzech głównych filarach: regulacji platform internetowych, strategiach wzmacniania odporności społecznej oraz koordynacji instytucjonalnej i międzypaństwowej. Choć DSA i powiązane inicjatywy stanowią znaczący krok naprzód, wyzwaniem pozostaje skuteczna egzekucja tych przepisów w praktyce oraz zapewnienie spójności działań między różnymi państwami członkowskimi.

Regulacje krajowe w Polsce

W Polsce nie funkcjonuje jeden kompleksowy akt prawny odnoszący się wprost do zjawiska dezinformacji. Regulacje w tym zakresie są rozproszone i zawarte w różnych aktach prawnych oraz dokumentach strategicznych, obejmujących zarówno sferę mediów, jak i bezpieczeństwa narodowego oraz działalności administracji publicznej. W praktyce przeciwdziałanie dezinformacji odbywa się w sposób pośredni – poprzez regulacje dotyczące rzetelności przekazu medialnego, odpowiedzialności nadawców, ochrony porządku publicznego czy zapewnienia bezpieczeństwa informacyjnego państwa.

Podstawowym aktem prawnym regulującym działalność tradycyjnych mediów w Polsce jest ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji. Nakłada ona na nadawców obowiązek zachowania rzetelności i obiektywizmu, przestrzegania zasady pluralizmu politycznego i społecznego oraz odpowiedzialności za treści przekazywane odbiorcom (Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji). Choć ustawa nie zawiera bezpośrednich przepisów dotyczących dezinformacji, stanowi podstawę do reagowania w przypadkach rozpowszechniania materiałów sprzecznych z prawem lub niezgodnych z zasadami etyki dziennikarskiej. Ważną rolę w tym kontekście

odgrywa Krajowa Rada Radiofonii i Telewizji (KRRiT), która ma uprawnienia nadzorcze i może nakładać sankcje na nadawców łamiących przepisy.

Dla mediów internetowych i prasy elektronicznej istotne znaczenie mają przepisy Prawa prasowego z 1984 r., wielokrotnie nowelizowane (Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe). Określają one m.in. obowiązki redaktorów naczelnych i wydawców w zakresie odpowiedzialności za publikowane treści oraz konieczność zachowania rzetelności dziennikarskiej. Choć prawo prasowe powstało w czasach przedcyfrowych, nadal stanowi punkt odniesienia przy ocenie odpowiedzialności za fałszywe lub wprowadzające w błąd informacje publikowane online.

W ostatnich latach coraz większe znaczenie w kontekście bezpieczeństwa informacyjnego mają również działania instytucjonalne i strategiczne. Ważną rolę odgrywa tu Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK), który prowadzi m.in. zespół CERT Polska zajmujący się reagowaniem na incydenty w cyberprzestrzeni oraz monitoringiem kampanii dezinformacyjnych (NASK – Państwowy Instytut Badawczy, 2022). NASK realizuje także programy edukacyjne i analityczne dotyczące rozpoznawania fałszywych treści, a jego raporty często służą administracji publicznej jako źródło wiedzy o zagrożeniach informacyjnych.

Istotnym elementem krajowego systemu przeciwdziałania dezinformacji są działania Rządowego Centrum Bezpieczeństwa (RCB), które prowadzi monitoring przestrzeni informacyjnej pod kątem pojawiających się narracji dezinformacyjnych, zwłaszcza w okresach kryzysowych (Rządowe Centrum Bezpieczeństwa, 2023). Współpracuje ono z innymi instytucjami państwowymi, służbami oraz mediami w celu szybkiego dementowania fałszywych informacji i ostrzegania społeczeństwa przed zagrożeniami.

Ważnym dokumentem strategicznym jest również Strategia Bezpieczeństwa Narodowego RP z 2020 roku, która wskazuje zagrożenia informacyjne jako istotny element współczesnych wyzwań dla bezpieczeństwa państwa. Strategia podkreśla konieczność wzmacniania odporności społeczeństwa na manipulacje informacyjne, rozwijania kompetencji medialnych oraz prowadzenia działań edukacyjnych i informacyjnych na poziomie centralnym i lokalnym (BBN, 2020).

Podsumowując, regulacje krajowe w Polsce w zakresie przeciwdziałania dezinformacji mają charakter pośredni i rozproszony. Opierają się głównie na istniejących przepisach medialnych, instrumentach nadzorczych oraz

działaniach strategicznych instytucji państwowych. Brakuje jednak jednolitych ram prawnych dedykowanych stricte temu zjawisku, co może utrudniać spójną i skuteczną reakcję na skoordynowane kampanie dezinformacyjne.

Analiza skuteczności regulacji

Ocena skuteczności obowiązujących regulacji prawnych dotyczących przeciwdziałania dezinformacji nie jest prosta. Zarówno w Unii Europejskiej, jak i w Polsce mamy do czynienia z rozbudowanym zestawem instrumentów prawnych, strategicznych i instytucjonalnych. Jednak to, w jakim stopniu te rozwiązania faktycznie przekładają się na ograniczanie szkodliwych treści i wzmocnienie odporności społeczeństwa, budzi sporo wątpliwości. Analiza doświadczeń z ostatnich lat, zwłaszcza w okresach kryzysowych, pozwala wskazać zarówno pozytywne efekty regulacji, jak i ich istotne ograniczenia.

Jednym z największych osiągnięć na poziomie unijnym jest zwiększenie odpowiedzialności dużych platform internetowych. Dzięki Digital Services Act wprowadzono m.in. obowiązek oceny ryzyka i podejmowania działań ograniczających rozprzestrzenianie treści nielegalnych i szkodliwych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065). W praktyce oznacza to, że platformy muszą współpracować z niezależnymi badaczami i instytucjami w celu identyfikowania zagrożeń informacyjnych. Widać to szczególnie po uruchomieniu pierwszych rocznych raportów transparentności – wiele firm zaczęło ujawniać dane dotyczące moderacji treści i stosowanych algorytmów. Choć to krok w dobrym kierunku, mechanizmy egzekucji przepisów wciąż są ograniczone. Komisja Europejska dopiero zaczyna nakładać pierwsze kary finansowe na podmioty łamiące regulacje DSA, a skuteczność tych działań będzie można ocenić dopiero w dłuższej perspektywie (European Commission, 2024).

Na poziomie krajowym działania regulacyjne są znacznie bardziej fragmentaryczne. W polskim porządku prawnym brak jednego kompleksowego aktu odnoszącego się wprost do zjawiska dezinformacji, a przeciwdziałanie jej odbywa się pośrednio poprzez różne regulacje dotyczące mediów, usług pośrednich i bezpieczeństwa informacyjnego. Jednocześnie doświadczenia unijne pokazują, że rozbieżne przepisy krajowe dotyczące dezinformacji online i innych zagrożeń społecznych utrudniają harmonizację oraz budowę spójnego systemu reagowania, co było jedną z przesłanek

przyjęcia Aktu o usługach cyfrowych (Dziedzic, 2024, s. 229-230). Warto przy tym podkreślić, że na gruncie polskich przepisów prawnych brak legalnej definicji dezinformacji (Dziedzic, 2024, s. 228).

Pandemia COVID-19 była jednym z pierwszych momentów, w których skuteczność regulacji została wystawiona na poważną próbę. W 2020 i 2021 roku w sieci pojawiła się ogromna liczba fałszywych treści dotyczących wirusa, szczepień, działań rządu i instytucji międzynarodowych. UE uruchomiła wówczas szereg działań w ramach systemu szybkiego ostrzegania oraz kampanii edukacyjnych, a Komisja Europejska prowadziła dialog z platformami w ramach Kodeksu postępowania w zakresie dezinformacji (European Commission, b.d.). Mimo tych działań, fałszywe informacje rozprzestrzeniały się szybciej niż rzetelne komunikaty. W Polsce wiele narracji dezinformacyjnych dotarło do milionów użytkowników w bardzo krótkim czasie. Widać było brak skutecznych mechanizmów szybkiego demaskowania i ograniczania zasięgu takich treści.

Podobna sytuacja miała miejsce po rozpoczęciu pełnoskalowej agresji Rosji na Ukrainę w lutym 2022 roku. Dezinformacja stała się wówczas jednym z głównych elementów działań hybrydowych, obok cyberataków i presji migracyjnej (European External Action Service, East StratCom Task Force, b.d.). UE uruchomiła m.in. system szybkiego ostrzegania oraz zintensyfikowała działania East StratCom Task Force. W Polsce zaobserwowano wzmożoną aktywność rosyjskich i prorosyjskich narracji, dotyczących m.in. rzekomego zagrożenia dla Polski, „ukrytej mobilizacji" czy deprecjonowania pomocy udzielonej uchodźcom. Choć instytucje państwowe, w tym RCB i NASK, starały się reagować, często były to działania spóźnione lub nie miały odpowiedniego zasięgu. Brakowało jednolitej strategii komunikacyjnej i skoordynowanej reakcji między różnymi podmiotami (NASK, 2022).

Warto też zauważyć, że skuteczność regulacji nie zależy wyłącznie od ich treści, ale także od poziomu edukacji medialnej społeczeństwa i zaufania obywateli do instytucji publicznych. Nawet najlepiej skonstruowane przepisy nie będą działały efektywnie, jeśli odbiorcy nie będą w stanie krytycznie oceniać treści lub nie będą wierzyć w oficjalne komunikaty. W tym zakresie zarówno UE, jak i Polska mają jeszcze sporo do zrobienia. Programy edukacyjne i informacyjne są potrzebne, jednak ich skuteczność zależy od lepszej koordynacji działań, stałych szkoleń oraz wsparcia instytucjonalnego i eksperckiego, zwłaszcza na poziomie lokalnym (Dwojnych, 2025, s. 33-34, 43).

Podsumowując, obecne regulacje prawne stanowią istotny krok naprzód w walce z dezinformacją, ale ich skuteczność jest ograniczona przez brak spójności, trudności w egzekwowaniu przepisów, opóźnienia w reagowaniu oraz niedostateczne działania edukacyjne. Przyszłe reformy powinny skupić się nie tylko na doprecyzowaniu przepisów i wzmocnieniu nadzoru nad platformami, ale także na budowaniu długofalowej odporności społecznej na fałszywe treści.

Wyzwania i rekomendacje

Choć w ostatnich latach zarówno Unia Europejska, jak i Polska podjęły istotne działania w zakresie regulacji przeciwdziałania dezinformacji, wciąż istnieje szereg wyzwań, które ograniczają skuteczność tych rozwiązań. Wyzwania te mają charakter zarówno systemowy, jak i operacyjny. Ich przezwyciężenie wymaga nie tylko zmian prawnych, ale także lepszej koordynacji działań instytucjonalnych oraz inwestycji w edukację i świadomość społeczną.

Pierwszym wyzwaniem jest niespójność i rozproszenie regulacji prawnych. Na poziomie unijnym DSA tworzy stosunkowo jednolite ramy dla dużych platform, ale nie obejmuje wszystkich aspektów walki z dezinformacją, a wiele szczegółów pozostaje w gestii państw członkowskich (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065). W Polsce natomiast brak jest jednego aktu prawnego poświęconego temu zjawisku – regulacje są rozsiane po różnych ustawach i dokumentach strategicznych. Taki stan rzeczy utrudnia stworzenie spójnego i przewidywalnego systemu przeciwdziałania dezinformacji.

Drugim wyzwaniem jest egzekwowanie przepisów w praktyce. Wiele obowiązków nałożonych na platformy w ramach DSA ma charakter ogólny i wymaga doprecyzowania w praktyce stosowania prawa. Komisja Europejska dopiero zaczyna realnie korzystać z uprawnień do nakładania sankcji finansowych, a krajowe organy nadzorcze nie zawsze dysponują odpowiednimi zasobami i kompetencjami, by skutecznie kontrolować przestrzeganie przepisów (European Commission, 2024). W Polsce dodatkowym problemem jest ograniczona jurysdykcja wobec zagranicznych podmiotów i brak szybkich mechanizmów reagowania na kampanie prowadzone z zewnątrz.

Kolejnym istotnym wyzwaniem jest koordynacja działań między różnymi podmiotami. Przeciwdziałanie dezinformacji wymaga współpracy wielu aktorów: instytucji państwowych, sektora prywatnego, organizacji pozarządowych, mediów i środowiska naukowego. W praktyce jednak działania te są często rozproszone i realizowane w sposób nieskoordynowany. Brakuje wyraźnie wyznaczonego centrum odpowiedzialnego za koordynację strategii informacyjnej państwa oraz szybką wymianę informacji między instytucjami (NASK, 2023). Efektem jest powielanie działań, brak spójnych komunikatów oraz trudności w budowaniu jednolitego przekazu wobec społeczeństwa.

Nie można też pominąć czynnika społecznego. Nawet najlepiej skonstruowane przepisy nie będą skuteczne, jeśli obywatele nie będą potrafili krytycznie ocenić ich treści. Poziom edukacji medialnej w Polsce wciąż pozostaje nierówny. W szkołach temat ten pojawia się głównie w formie doraźnych projektów lub fakultatywnych zajęć, a nie jako spójny element programu nauczania (Dwojnych, 2025, s. 33-34, 43). Brakuje też szeroko zakrojonych kampanii społecznych, które w przystępny sposób uczyłyby rozpoznawania fałszywych informacji, np. poprzez porównywanie źródeł, analizę języka emocjonalnego czy rozpoznawanie schematów narracyjnych wykorzystywanych w kampaniach dezinformacyjnych.

Na podstawie powyższych wyzwań można sformułować kilka kluczowych rekomendacji: tworzenie spójnych ram prawnych na poziomie krajowym, np. w formie odrębnej ustawy lub kompleksowej nowelizacji istniejących przepisów, która jasno określiłaby obowiązki instytucji, mechanizmy reagowania oraz współpracy w zakresie bezpieczeństwa informacyjnego. Wzmocnienie egzekucji przepisów DSA i stworzenie krajowego organu nadzorczego z realnymi kompetencjami oraz zapleczem technicznym. Taka instytucja mogłaby współpracować bezpośrednio z Komisją Europejską oraz platformami cyfrowymi. Wyznaczenie krajowego centrum koordynacji działań informacyjnych, które odpowiadałoby za monitoring, analizę i szybką reakcję na kampanie dezinformacyjne, łącząc działania NASK, RCB, służb, mediów publicznych i organizacji pozarządowych. Wzmocnienie edukacji medialnej poprzez wprowadzenie jej jako stałego elementu programu szkolnego oraz realizację ogólnokrajowych kampanii społecznych skierowanych do różnych grup wiekowych.

Podsumowując, przeciwdziałanie dezinformacji wymaga podejścia systemowego. Nie wystarczy samo zaostrzenie przepisów – potrzebne są skuteczne mechanizmy ich egzekwowania, lepsza współpraca instytucjonalna i szerokie działania edukacyjne. Dopiero połączenie tych elementów może realnie zwiększyć odporność społeczeństwa na fałszywe treści.

Podsumowanie

Dezinformacja stała się jednym z kluczowych wyzwań bezpieczeństwa informacyjnego współczesnych państw. Zarówno Unia Europejska, jak i Polska podejmują coraz bardziej zaawansowane działania regulacyjne i instytucjonalne, mające na celu ograniczenie wpływu fałszywych treści na społeczeństwo i system polityczny. W ostatnich latach widać istotny postęp – przede wszystkim dzięki przyjęciu Digital Services Act oraz rozwojowi strategii informacyjnych na poziomie europejskim i krajowym. Powstały także struktury analityczne i mechanizmy wymiany informacji, takie jak East StratCom Task Force czy Rapid Alert System, które wzmacniają zdolność do szybszego reagowania na zagrożenia.

Jednocześnie skuteczność tych rozwiązań pozostaje ograniczona. W praktyce regulacje są często trudne do egzekwowania, działania instytucji są rozproszone, a poziom edukacji medialnej w społeczeństwie nadal nie gwarantuje wysokiej odporności na manipulacje informacyjne. Doświadczenia pandemii COVID-19 i wojny w Ukrainie pokazały, że dezinformacja rozprzestrzenia się szybciej niż systemy państwowe i unijne są w stanie reagować.

Dlatego przeciwdziałanie temu zjawisku wymaga podejścia systemowego i wielowarstwowego. Potrzebne są nie tylko doprecyzowane i spójne ramy prawne, ale także silniejsze instytucje nadzorcze, lepsza koordynacja działań międzysektorowych oraz inwestycje w edukację i świadomość społeczną. Tylko takie połączenie może realnie zwiększyć odporność informacyjną i zmniejszyć wpływ wrogich narracji na społeczeństwo.

Literatura

1. BBN. (2020). *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa.
2. Dwojnych, A. (2025). *Przeciwdziałanie dezinformacji w przestrzeni Polski lokalnej – rekomendacje rozwiązań*. Warszawa: Sieć Badawcza Łukasiewicz.
3. Dziedzic, M. (2024). Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o sztucznej inteligencji. *Prawo i Więź*, 6(53), 223-238. https://doi.org/10.36128/PRIW.VI53.1103
4. European Commission. (2020). *European Democracy Action Plan*.
5. European Commission. (2020). *Fighting COVID-19 disinformation*.
6. European Commission. (2024). *First DSA enforcement actions*.
7. European Commission. (b.d.). *Rapid Alert System against disinformation*. Pobrano z: https://commission.europa.eu/strategy-and-policy/policies/media-and-digital/regulation-disinformation/rapid-alert-system_en (dostęp: 01.02.2026).
8. European External Action Service. (b.d.). *East StratCom Task Force*. Pobrano z: https://euvsdisinfo.eu (dostęp: 01.02.2026).
9. NASK – Państwowy Instytut Badawczy. (2022). *Raport o dezinformacji dotyczącej wojny w Ukrainie*.
10. NASK – Państwowy Instytut Badawczy. (2022). *Raport z działalności CERT Polska*.
11. NASK. (2023). *Raport o wyzwaniach w zakresie bezpieczeństwa informacyjnego*.
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Digital Services Act), Dz.U. UE L 277 z 27.10.2022.
13. Rządowe Centrum Bezpieczeństwa. (2023). *Raport o zagrożeniach informacyjnych*.
14. Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe, Dz.U. 1984 nr 5, poz. 24 z późn. zm.
15. Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji, Dz.U. 1993 nr 7, poz. 34 z późn. zm.

Justyna Wilczyńska-Baraniak[1]

Małgorzata Wilczyńska[2]

Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu

https://doi.org/10.29316/9788368103359_12

DEEPFAKE JAKO STRUKTURALNE ZAGROŻENIE DLA BEZPIECZEŃSTWA INFORMACJI

DEEPFAKES AS A STRUCTURAL THREAT TO INFORMATION SECURITY

Streszczenie

Rozdział analizuje technologię deepfake jako strukturalne zagrożenie dla bezpieczeństwa informacji, koncentrując się na konsekwencjach jej demokratyzacji. Punktem wyjścia jest obserwacja, że rozwój narzędzi open source, usług chmurowych oraz intuicyjnych interfejsów doprowadził do sytuacji, w której tworzenie deepfake-'ów nie wymaga dziś specjalistycznej wiedzy technicznej. Obniżenie progu wejścia umożliwia masową produkcję syntetycznych treści audiowizualnych, co znacząco zwiększa skalę nadużyć, w tym oszustw finansowych, manipulacji politycznej oraz naruszeń dóbr osobistych. W części empirycznej przedstawiono liczne przypadki podszywania się w czasie rzeczywistym, m.in. w Hongkongu, Wielkiej Brytanii,

[1] https://orcid.org/0009-0005-3148-8197, e-mail: justaw@o2.pl

[2] https://orcid.org/0000-0002-1969-3498, e-mail: malgorzata.wilczynska@pansjar.edu.pl

Singapurze i państwach UE. Przykłady te pokazują, że tradycyjne metody weryfikacji tożsamości oparte na obrazie i głosie tracą swoją wiarygodność, co prowadzi do poważnych strat finansowych i podważa zaufanie do komunikacji cyfrowej. Analiza wskazuje, że deepfake staje się narzędziem umożliwiającym obchodzenie systemów uwierzytelniania oraz realizację oszustw na masową skalę. W części regulacyjnej omówiono odpowiedź Unii Europejskiej, w szczególności AI Act, który wprowadza legalną definicję deepfake oraz obowiązek transparentności. W rozdziale podkreślono, że obowiązujące ramy prawne, w tym RODO, nie nadążają za dynamiką rozwoju technologii i nie zapewniają ochrony przed systemowymi skutkami dezinformacji. Wnioski wskazują na konieczność łączenia regulacji prawnych, rozwiązań technicznych oraz edukacji cyfrowej jako warunku skutecznego przeciwdziałania zagrożeniom wynikającym z demokratyzacji technologii deepfake. Celem rozdziału jest analiza mechanizmów obniżenia progu wejścia do tworzenia deepfake'ów oraz omówienie konsekwencji tego procesu dla bezpieczeństwa informacji, zaufania do mediów i skuteczności istniejących ram prawnych. Analiza demokratyzacji technologii deepfake pozwala lepiej zrozumieć, dlaczego współczesne zagrożenia informacyjne mają charakter masowy, trudny do kontrolowania i wykraczający poza tradycyjne ramy regulacyjne. Treści prezentowane w rozdziale opracowano z wykorzystaniem teoretycznych metod badawczych, wiodącą z nich była analiza krytyczna literatury przedmiotu, analiza kwerendy źródeł internetowych, jak również metoda analizy, syntezy, uogólnienia oraz wnioskowania

Słowa kluczowe: deepfake, bezpieczeństwo informacji, demokratyzacja technologii, treści audiowizualne, oszustwa finansowe, podszywanie się (impersonation), weryfikacja tożsamości, dezinformacja, zaufanie do komunikacji cyfrowej, regulacja sztucznej inteligencji (AI Act)

Abstract

This chapter examines deepfake technology as a structural threat to information security, with particular emphasis on the consequences of its rapid democratization. The analysis begins with the observation that the widespread availability of opensource tools, cloudbased services, and intuitive user interfaces has fundamentally lowered the technical threshold for producing synthetic audiovisual content. As the chapter notes, "creating deepfakes no longer requires specialized technical knowledge", which has enabled largescale misuse by individuals lacking advanced expertise. This shift has transformed deepfakes from isolated incidents into a systemic risk affecting both public and private institutions. The empirical section presents documented cases of realtime impersonation in Hong Kong, the United Kingdom, Singapore, and

EU member states. These incidents demonstrate that traditional identityverification methods based on facial and voice recognition “are losing their reliability”, resulting in substantial financial losses and undermining trust in digital communication. The cases illustrate how synthetic audio and video can be weaponized to bypass authentication mechanisms and facilitate fraud at scale. The regulatory analysis focuses on the European Union’s AI Act, which introduces a legal definition of deepfake and establishes transparency obligations for synthetic media. The chapter argues that existing legal frameworks, including the GDPR, do not adequately address the authenticity of digital content and fail to mitigate systemic risks such as disinformation and the liar’s dividend. The conclusion highlights the need for a combined strategy integrating legal regulation, technical safeguards, and AI literacy as essential components of an effective response to the challenges posed by the democratization of deepfake technology.

Keywords: deepfake, information security, democratization of technology, audiovisual content, financial fraud, impersonation, identity verification, disinformation, trust in digital communication, AI regulation (AI Act)

Wstęp

Deepfake to technologia oparta na metodach sztucznej inteligencji, wykorzystująca zaawansowane modele generatywne, w szczególności generatywne sieci przeciwstawne (GAN) oraz autoenkodery wariacyjne (VAE), do syntezy realistycznych treści audiowizualnych, takich jak obrazy, nagrania wideo oraz dźwięk. Termin *deepfake* wywodzi się z języka angielskiego i stanowi połączenie słów *deep*, odnoszącego się do technik głębokiego uczenia maszynowego (*deep learning*), oraz *fake*, oznaczającego treści fałszywe lub celowo zmanipulowane (NASK, 2025). Termin *deepfake* pojawił się w literaturze i dyskursie publicznym pod koniec 2017 roku, początkowo jako określenie nowej klasy syntetycznych treści audiowizualnych generowanych przy użyciu metod uczenia maszynowego. Geneza terminu *deepfake* wiąże się z działalnością anonimowego użytkownika platformy Reddit, posługującego się pseudonimem „deepfakes”, który właśnie pod koniec 2017 roku zapoczątkował społeczność internetową poświęconą tworzeniu i udostępnianiu syntetycznych materiałów audiowizualnych (Regan, 2025). To od jego nazwy użytkownika wywodzi się określenie, które z czasem zostało zaadaptowane do opisu całej klasy technologii generatywnych.

W niniejszym rozdziale szczególną uwagę poświęcono zagadnieniu demokratyzacji technologii deepfake jako jednemu z kluczowych wyzwań dla bezpieczeństwa informacji. Wybór tego obszaru analizy wynika z faktu, że powszechna dostępność narzędzi do generowania deepfake'ów, w tym rozwiązań open source oraz usług chmurowych, prowadzi do jakościowej zmiany skali i charakteru potencjalnych nadużyć. Demokratyzacja ta, choć sprzyja innowacjom, twórczości oraz zastosowaniom edukacyjnym, jednocześnie umożliwia masową produkcję treści manipulacyjnych przez osoby nieposiadające specjalistycznej wiedzy technicznej. Celem rozdziału jest zatem analiza mechanizmów obniżenia progu wejścia do tworzenia deepfake'ów oraz omówienie konsekwencji tego procesu dla bezpieczeństwa informacji, zaufania do mediów i skuteczności istniejących ram prawnych. Analiza demokratyzacji technologii deepfake pozwala lepiej zrozumieć, dlaczego współczesne zagrożenia informacyjne mają charakter masowy, trudny do kontrolowania i wykraczający poza tradycyjne ramy regulacyjne. Rozdział opiera się na analizie literatury naukowej, raportów branżowych oraz udokumentowanych przypadków nadużyć z lat 2024-2025. Dobór case studies został dokonany według dwóch kryteriów: (1) potwierdzona przez organy ścigania lub media wysokiej wiarygodności autentyczność zdarzenia oraz (2) reprezentatywność dla zjawiska demokratyzacji technologii deepfake, rozumianej jako obniżenie progu wejścia do generowania syntetycznych treści. Analiza obejmuje zarówno aspekty techniczne, jak i regulacyjne, co pozwala na uchwycenie strukturalnego charakteru zagrożeń dla bezpieczeństwa informacji. Treści prezentowane w rozdziale opracowano z wykorzystaniem teoretycznych metod badawczych, wiodącą z nich była analiza krytyczna literatury przedmiotu, analiza kwerendy źródeł internetowych, jak również metoda analizy, syntezy, uogólnienia oraz wnioskowania.

Geneza i rozwój technologii deepfake

W początkowym okresie deepfake polegał głównie na manipulacji wizerunkiem poprzez zastępowanie twarzy osób występujących w istniejących nagraniach wizerunkami osób publicznych. Mimo kontrowersyjnego charakteru tych praktyk, działalność ta przyczyniła się do gwałtownego wzrostu zainteresowania technologiami syntezy obrazu i wideo oraz zapoczątkowała szeroką debatę naukową, prawną i etyczną nad konsekwencjami rozwoju technologii deepfake (Etienne, 2021). Według raportu Deeptrace

technologia rozwija się bardzo szybko (Ajder, Patrini, Cavalli, Cullen, 2019). Na początku 2019 roku w Internecie zaprezentowano 7964 filmów deepfake, dziesięć miesięcy później ich liczba wynosiła 14678. (Toews, 2022). Szerokie zainteresowanie środowiska naukowego i opinii publicznej technologią deepfake zostało zapoczątkowane przez dwa przełomowe projekty badawcze: „*Face2Face"* (Thies i in., 2016). oraz „*Synthesizing Obama"* (Suwajanakorn, Seitz, KemelmacherShlizerman, 2017), które po raz pierwszy w sposób systematyczny zademonstrowały możliwość realistycznej syntezy mimiki i synchronizacji mowy, ujawniając potencjalne konsekwencje tej technologii dla wiarygodności treści audiowizualnych. Projekt Face2Face autorstwa zaprezentował możliwość interaktywnego przenoszenia mimiki twarzy z osoby źródłowej na osobę widoczną w nagraniu docelowym. System analizował ruchy twarzy mówiącego takie jak uśmiech, zmarszczenie brwi czy ruch ust, a następnie odwzorowywał je na twarzy osoby w nagraniu, generując wideo wyglądające jak autentyczne. Co istotne, technologia działała w czasie zbliżonym do rzeczywistego, co unaoczniło, że manipulacja obrazem wideo może być nie tylko realistyczna, lecz także szybka i trudna do wykrycia. Projekt ten stał się jednym z pierwszych dowodów na to, że możliwe jest tworzenie przekonujących fałszywych reakcji emocjonalnych lub wypowiedzi osób publicznych. Projekt *Synthesizing Obama* pokazał, że możliwe jest syntetyczne generowanie całych wypowiedzi osób publicznych (Suwajanakorn i in., 2017). Badacze wykorzystali setki godzin nagrań Baracka Obamy, aby nauczyć model charakterystycznych ruchów ust, mimiki i gestów byłego prezydenta USA. Następnie system potrafił zsynchronizować ruchy ust z dowolnym nagraniem audio, tworząc wideo wyglądające jak autentyczne przemówienie. Projekt ten wywołał szeroką debatę, ponieważ po raz pierwszy zaprezentowano technologię umożliwiającą przypisywanie osobom publicznym wypowiedzi, których nigdy nie wygłosiły. Od czasu tych dwóch projektów technologia deepfake znalazła zastosowanie w szerokim spektrum obszarów: od internetowych memów, poprzez sztukę, aż po przemysł filmowy (Chesney, Citron, 2019). Największe zainteresowanie opinii publicznej wzbudziły jednak zastosowania związane z treściami politycznymi, takie jak fałszywe nagrania przemówień Borisa Johnsona i Jeremy-'ego Corbyna opublikowane przez think tank Future Advocacy w kontekście wyborów powszechnych w Wielkiej Brytanii w 2019 roku (Future Advocacy, b.d.). W 2020 roku grupa aktywistów Extinction Rebellion udostępniła fałszywe nagranie premier Belgii, Sophie Wilmès, sugerujące możliwy związek

między wylesianiem a pandemią COVID19 (Galindo, 2020). Te szeroko komentowane przykłady, w połączeniu z szybkim postępem technologicznym w zakresie jakości deepfake'ów, wywołały poważne obawy w środowisku zajmującym się etyką sztucznej inteligencji. Eksperci zwracają uwagę, że największym zagrożeniem jest niemożność odróżnienia deepfake od prawdziwych treści (Etienne, 2021).

Deepfake jako zagrożenie dla bezpieczeństwa informacji

Technologie oparte na sztucznej inteligencji rozwijają się w zawrotnym tempie, wspierając niemal każdy aspekt naszego codziennego życia, od rozrywki i pracy po edukację i bezpieczeństwo. Jednak wraz z postępem rośnie także skala zagrożeń. Jednym z najbardziej niepokojących przykładów złośliwego wykorzystania sztucznej inteligencji przez cyberprzestępców jest technologia deepfake, generowanie realistycznych, lecz fałszywych treści wizualnych i dźwiękowych. Treści te są następnie wykorzystywane do dezinformacji, niszczenia reputacji i oszustw na niespotykaną dotąd skalę (Zegarow, 2025). Dynamiczny rozwój sztucznej inteligencji oprócz szeregu szans rozwojowych niesie ze sobą także zagrożenia dla praw i wolności osób fizycznych, w szczególności w postaci zjawiska tzw. deepfake'ów, w których generowane przez AI fałszywe obrazy, dźwięki i nagrania wideo, wydają się coraz bardziej wiarygodne, co zwiększa przestrzeń do nadużyć i odziaływania negatywnych konsekwencji tego typu treści dla osób fizycznych, których dane osobowe mogą być bezprawnie wykorzystywane (Zontek, 2025). Niemożność jednoznacznego odróżnienia deepfake od materiałów autentycznych stanowi jedno z kluczowych zagrożeń związanych z rozwojem technologii deepfake. W raporcie Deeptrace, wskazano, że jakość treści generowanych przy użyciu tej technologii osiągnęła poziom, na którym zarówno dla użytkowników indywidualnych, jak i dla systemów automatycznej detekcji staje się coraz trudniejsze wiarygodne rozróżnienie pomiędzy mediami autentycznymi a syntetycznymi *(„the quality of deepfake content has reached a level where it is increasingly difficult for both humans and automated systems to reliably distinguish between real and synthetic media")* (Ajder i in., 2019). Inne zagrożenia wynikające z technologii deepfake to: zjawisko „liar's dividend", dezinformacja polityczna, naruszenie dóbr osobistych, oszustwa finansowe i ataki socjotechniczne. Upowszechnienie deepfake'ów prowadzi do zjawiska określanego mianem „*liar's dividend"*, polegającego na możliwości

kwestionowania nawet autentycznych materiałów jako fałszywych (Chesney, Citron, 2019). W dłuższej perspektywie zjawisko to może osłabić zaufanie społeczne do mediów, instytucji publicznych oraz dowodów wykorzystywanych w postępowaniach sądowych. Deepfake'i stanowią szczególnie groźne narzędzie dezinformacji, zwłaszcza w kontekście politycznym. Mogą być wykorzystywane do generowania fałszywych wypowiedzi osób publicznych, co sprzyja manipulacji opinią publiczną i ingerencji w procesy demokratyczne. Jak wskazuje literatura, deepfake'i umożliwiają masową dystrybucję nieprawdziwych, lecz wysoce realistycznych treści audiowizualnych, co w konsekwencji prowadzi do osłabienia jakości dyskursu *demokratycznego („deepfakes have the potential to undermine democratic discourse by enabling the large-scale dissemination of false but highly convincing audiovisual information"* (Ajder i in., 2019). Deepfake w kontekście naruszeń dóbr osobistych - brak zgody na wykorzystywanie wizerunku, w szczególności w materiałach pornograficznych to obecnie kolejne najpowszechniejsze i jednocześnie najbardziej szkodliwe zastosowanie tej technologii. Skutki tego rodzaju nadużyć obejmują poważne konsekwencje psychologiczne, społeczne oraz reputacyjne dla osób, których wizerunek został wykorzystany bez ich zgody („*non-consensual deepfake pornography represents the most prevalent and harmful use of deepfake technology to date*") (Ajder i in., 2019). Deepfake jako narzędzie oszustw finansowych i ataków socjotechnicznych – Deepfake'i stanowią także istotne zagrożenie dla bezpieczeństwa informacji oraz ochrony tożsamości. Technologia ta jest coraz częściej wykorzystywana w oszustwach finansowych oraz atakach socjotechnicznych, w których syntetyczne nagrania głosu i obrazu służą do podszywania się pod konkretne osoby i omijania mechanizmów uwierzytelniania. Od zarania cyberbezpieczeństwa, najsłabszym ogniwem w każdym systemie obronnym był, jest i prawdopodobnie zawsze będzie człowiek. Atakujący doskonale o tym wiedzą, dlatego sztuka manipulacji, perswazji i oszustwa – czyli socjotechnika – od zawsze była ich najskuteczniejszą bronią (Gil, 2026). Jak wskazują analitycy Sensity AI, syntetyczne materiały audio i wideo mogą zostać wykorzystane jako narzędzie umożliwiające obchodzenie systemów weryfikacji tożsamości oraz realizację oszustw na masową skalę („*synthetic audio and video can be weaponized to bypass identity verification systems and facilitate fraud at scale*") (Sensity AI, 2021). Prawo często nie nadąża za szybkim rozwojem technologii. Istniejące regulacje dotyczące ochrony danych osobowych, prawa autorskiego czy zniesławienia nie zawsze obejmują specyfikę technologii deepfake. Zróżnicowane

podejścia legislacyjne utrudniają skuteczne egzekwowanie odpowiedzialności i zwalczanie nadużyć, zwłaszcza w kontekście transgranicznym (Afshari, Mohammadi, 2025). Obniżenie progu wejścia do tworzenia deepfake'ów, dzięki narzędziom open source i usługom chmurowym, stanowi paradoksalne wyzwanie. Z jednej strony sprzyja innowacjom, twórczości i zastosowaniom edukacyjnym, z drugiej umożliwia masową produkcję treści manipulacyjnych przez osoby bez specjalistycznej wiedzy (Ajder i in., 2019).

Tabela 1. Deepfake jako zagrożenie dla bezpieczeństwa informacji

Typ zagrożenia	Mechanizm deepfake	Przykład	Adekwatne środki prawne/ techniczne
Podszywanie się (impersonation)	Realtime deepfake: obraz + głos	Hongkong 2024: „wszyscy uczestnicy rozmowy, poza ofiarą, byli wygenerowani jako deepfake"	Weryfikacja poza kanałem, procedury potwierdzania tożsamości
Oszustwa finansowe	Klonowanie głosu, manipulacja wideo	Arup 2024; Singapur 2025	Zasada podwójnej autoryzacji, limity przelewów, szkolenia pracowników
Dezinformacja polityczna	Fałszywe wypowiedzi osób publicznych	Przykłady z UK i Belgii	Oznaczanie treści (AI Act art. 50), fact-checking, edukacja medialna
Naruszenia dóbr osobistych	Deepfake pornograficzny	Raport Deeptrace: „non-consensual deepfake pornography represents the most prevalent and harmful use"	Deepfake naruszający dobra osobiste może rodzić odpowiedzialność cywilną i karną. Kluczowe znaczenie ma jednak szybka reakcja: zgłoszenie treści do usunięcia, wykorzystanie procedur platform oraz bieżący monitoring internetu. W praktyce skuteczna ochrona zależy bardziej od natychmiastowego ograniczenia szkody niż od późniejszego dochodzenia roszczeń.

Źródło: opracowanie na podstawie: R. Chesney, D.K. Citron, „Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", California Law Review 2019, t. 107, s. 1753-1820; N. Afshari, A. Mohammadi, „The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media", Legal Studies in Digital Age 2023, t. 2, nr 2, s. 13-23; South China Morning Post, 4.02.2024; The Guardian, 17.05.2024; Singapore Police Force, 7.04.2025; Deeptrace, The State of Deepfakes: Landscape, Threats, and Impact, 2019.

Deepfake jako zagrożenie dla bezpieczeństwa informacji nie może być neutralizowany przy użyciu pojedynczego instrumentu. Skuteczna odpowiedź wymaga modelu trójfilarowego, łączącego regulacje prawne, odporność organizacyjnotechniczną oraz rozwój kompetencji w zakresie sztucznej inteligencji. Dopiero współdziałanie tych filarów pozwala ograniczyć strukturalne skutki demokratyzacji technologii deepfake i chronić zaufanie do komunikacji cyfrowej.

Demokratyzacja technologii deepfake

W erze, kiedy sztuczna inteligencja (AI) staje się coraz bardziej powszechna, istnieje rosnące zapotrzebowanie na demokratyzację dostępu do generatywnej sztucznej inteligencji (GAI). Jednak wraz z tą demokratyzacją pojawia się również potrzeba świadomości i odpowiedzialnego korzystania z tej potężnej technologii. Demokratyzacja oznacza, że coraz więcej osób ma dostęp do narzędzi opartych na sztucznej inteligencji, co z kolei rodzi wyzwania związane z etyką, prywatnością i bezpieczeństwem danych. Dlatego kluczowym elementem tego procesu jest edukacja społeczeństwa na temat zasad funkcjonowania i potencjalnych skutków AI (Integral Solution, b.d.). Demokratyzacja technologii *deepfake* oznacza, że tworzenie realistycznych, syntetycznych treści audiowizualnych przestało być domeną wąskiej grupy specjalistów. Jeszcze kilka lat temu generowanie takich materiałów wymagało zaawansowanej wiedzy technicznej, dostępu do specjalistycznego sprzętu oraz znacznych nakładów finansowych. Obecnie bariery te uległy istotnemu obniżeniu, co ma bezpośredni wpływ na skalę i charakter nadużyć związanych z wykorzystaniem deepfake'ów (Chesney, Citron, 2019). Jednym z kluczowych czynników tego procesu jest powszechna dostępność narzędzi typu open source, które można bezpłatnie pobrać i wykorzystać. Oprogramowanie to jest często wyposażone w gotowe instrukcje oraz uproszczone procedury, co sprawia, że jego obsługa nie wymaga specjalistycznego przygotowania informatycznego. W praktyce oznacza to, że każda osoba posiadająca podstawowe umiejętności cyfrowe może wygenerować materiał przypominający autentyczne nagranie wideo lub audio, bez konieczności rozumienia mechanizmów działania algorytmów sztucznej inteligencji. Z perspektywy bezpieczeństwa informacji istotne jest to, że otwarty charakter takich narzędzi utrudnia kontrolę nad ich wykorzystaniem,

a także sprzyja szybkiemu rozpowszechnianiu rozwiązań umożliwiających tworzenie coraz bardziej realistycznych treści manipulacyjnych (Ajder i in., 2019, s. 3-6). Kolejnym elementem obniżającym próg wejścia są usługi chmurowe oraz modele oferowane w formule „as a service". W tym modelu użytkownik nie musi posiadać własnej infrastruktury technicznej ani instalować specjalistycznego oprogramowania. Wystarczy dostęp do internetu oraz podstawowe dane wejściowe (np. nagranie głosu lub zdjęcia), aby w krótkim czasie wygenerować gotowy materiał. Z punktu widzenia prawa i regulacji szczególnie istotne jest to, że takie usługi działają globalnie, często poza jurysdykcją państwa, w którym dochodzi do nadużycia. Ułatwia to zarówno masową produkcję treści manipulacyjnych, jak i zdecydowanie utrudnioną identyfikację sprawcy oraz przypisania mu odpowiedzialności prawnej, zwłaszcza w przypadkach o charakterze transgranicznym (Ajder i in., 2019; Chesney, Citron, 2019). Najważniejszą konsekwencją opisanych zmian jest jednak fakt, że tworzenie deepfake'ów nie wymaga dziś specjalistycznej wiedzy technicznej. Nowoczesne narzędzia są projektowane w taki sposób, aby użytkownik mógł posługiwać się nimi intuicyjnie – poprzez wybór gotowych opcji, wgrywanie plików i zatwierdzanie rezultatów. W efekcie technologia deepfake staje się dostępna dla bardzo szerokiego kręgu użytkowników, w tym także dla osób działających w złej wierze. Prowadzi to do jakościowej zmiany zagrożeń: zamiast pojedynczych, incydentalnych przypadków manipulacji pojawia się zjawisko masowe, trudne do kontrolowania i jeszcze trudniejsze do skutecznego sankcjonowania w ramach istniejących instrumentów prawnych (Ajder i in., 2019; Chesney, Citron, 2019). Opisane obniżenie progu wejścia stanowi punkt wyjścia do dalszych rozważań nad eskalacją nadużyć związanych z deepfake'ami. Pokazuje ono, że problem nie leży wyłącznie w samej technologii, lecz w jej powszechnej dostępności, która wyprzedza zdolność systemów prawnych i instytucjonalnych do reagowania. Z tego względu demokratyzacja technologii deepfake powinna być traktowana jako czynnik strukturalny, determinujący zarówno skalę zagrożeń, jak i utrudnioną ochronę prawną (Chesney, Citron, 2019).

Studia przypadków (Case studies) nadużyć związanych z demokratyzacją technologii deepfake

Podszywanie się w rozmowach wideo w czasie rzeczywistym (*real-time deepfake*)

Jednym z najbardziej problematycznych przykładów nadużyć związanych z demokratyzacją technologii deepfake są przypadki podszywania się pod osoby funkcyjne podczas rozmów wideo prowadzonych na żywo, wykorzystywane w szczególności do wyłudzeń finansowych. W tego rodzaju sytuacjach sprawca jest w stanie w czasie rzeczywistym wygenerować obraz i głos osoby pełniącej określoną funkcję w organizacji, takiej jak dyrektor, członek zarządu czy bezpośredni przełożony, co znacząco zwiększa wiarygodność fałszywej komunikacji.

Z punktu widzenia praktyki organizacyjnej istotne jest, że ataki te nie polegają na przesyłaniu wcześniej przygotowanego nagrania, lecz na prowadzeniu interaktywnej rozmowy, która z perspektywy odbiorcy nie różni się od autentycznego spotkania online. Pozwala to sprawcy na bieżąco reagować na pytania rozmówcy i dostosowywać przekaz do sytuacji, co dodatkowo utrudnia wykrycie nadużycia. Skuteczność tego rodzaju podszywania się znacząco wzrasta w organizacjach, które opierają weryfikację tożsamości wyłącznie na cechach behawioralnych lub wizualnych, takich jak rozpoznanie twarzy, głosu czy charakterystycznego sposobu wypowiadania się, bez stosowania dodatkowych procedur potwierdzających. W konsekwencji decyzje o charakterze finansowym lub organizacyjnym mogą zostać podjęte na podstawie komunikacji, która sprawia wrażenie w pełni autentycznej, mimo że w rzeczywistości została wygenerowana syntetycznie.

Z perspektywy prawa i bezpieczeństwa informacji przypadki te pokazują, że biometria behawioralna przestaje być wystarczającym środkiem uwierzytelnienia, a zaufanie do form komunikacji audiowizualnej jako dowodu lub podstawy decyzji ulega istotnemu osłabieniu. Zjawisko to unaocznia również, w jaki sposób powszechna dostępność narzędzi deepfake prowadzi do jakościowej zmiany zagrożeń – od sporadycznych incydentów do realnego ryzyka systemowego dla funkcjonowania instytucji i obrotu gospodarczego.

Hongkong – fałszywa wideokonferencja z „CFO" (2024)

Jednym z najbardziej nagłośnionych przypadków podszywania się przy użyciu technologii deepfake była sprawa ujawniona przez policję w Hongkongu na początku 2024 r. Pracownik działu finansowego międzynarodowej spółki został zaproszony na wideokonferencję, w której uczestniczyły osoby wyglądające i brzmiące jak znani mu współpracownicy, w tym dyrektor finansowy spółki. Podczas spotkania polecono mu dokonanie pilnych przelewów na wskazane rachunki bankowe.

Pracownik początkowo podejrzewał próbę oszustwa, jednak po dołączeniu do rozmowy wideo i rozpoznaniu twarzy oraz głosów przełożonych uznał polecenie za autentyczne. W rezultacie dokonał 15 przelewów na łączną kwotę około 25 milionów dolarów amerykańskich. Dopiero późniejsza weryfikacja wykazała, że wszyscy uczestnicy rozmowy – poza ofiarą – byli wygenerowani jako deepfake, a wizerunki i głosy powstały na podstawie publicznie dostępnych materiałów. Sprawa została szeroko opisana w prasie azjatyckiej i międzynarodowej (Harvey Kong, 2024).

Przypadek ten pokazuje, że obecność rozmówcy w czasie rzeczywistym, a nawet udział wielu „uczestników", nie może być już traktowana jako wystarczające potwierdzenie tożsamości. Z perspektywy odpowiedzialności organizacyjnej istotne jest, że decyzje finansowe zostały podjęte na podstawie komunikacji, która wizualnie i głosowo spełniała wszystkie dotychczasowe kryteria autentyczności.

Arup – potwierdzona ofiara deepfake'ów (Wielka Brytania / Hongkong, 2024)

Kolejnym istotnym przykładem jest sprawa brytyjskiej firmy inżynieryjnej Arup, która publicznie potwierdziła, że padła ofiarą oszustwa wykorzystującego technologię deepfake. Pracownik spółki w Hongkongu został nakłoniony do przekazania około 20 milionów funtów brytyjskich po rozmowie wideo z osobami podszywającymi się pod kadrę kierowniczą. Spółka wskazała, że w oszustwie wykorzystano fałszywe obrazy i głosy, a komunikacja miała charakter przekonującego spotkania służbowego. Co istotne, Arup podkreślił, że nie doszło do naruszenia systemów informatycznych, a mechanizm oszustwa polegał wyłącznie na przełamaniu zaufania pracownika do komunikacji audiowizualnej. Sprawa Arup ma szczególne znaczenie,

ponieważ dotyczy dużej, profesjonalnej organizacji, posiadającej rozbudowane procedury bezpieczeństwa. Pokazuje to, że deepfake'i nie są zagrożeniem marginalnym ani ograniczonym do słabo zabezpieczonych podmiotów, lecz stanowią ryzyko systemowe dla obrotu gospodarczego (The Guardian, 2024).

Singapur – „narada kierownictwa" i przelew 499 tys. USD (2025)

W 2025 r. opisano również przypadek z Singapuru, w którym dyrektor finansowy spółki uczestniczył w wideokonferencji przypominającej naradę kierownictwa. W trakcie spotkania osoby wyglądające jak znani menedżerowie przedstawiły pilną potrzebę dokonania przelewu w związku z poufną transakcją. Dyrektor, działając w przekonaniu, że uczestniczy w autentycznym spotkaniu, zatwierdził przelew na kwotę około 499 tysięcy dolarów amerykańskich. Późniejsze ustalenia wykazały, że cała rozmowa została wygenerowana za pomocą technologii deepfake, a sprawcy posłużyli się wizerunkami i głosami opartymi na materiałach publicznych. Przypadek ten potwierdza, że technologia deepfake umożliwia skalowalne oszustwa, obejmujące zarówno bardzo wysokie, jak i „średnie" kwoty, a więc potencjalnie dotykające znacznie szerszego kręgu podmiotów (Tookitaki, 2025).

Studium przypadku nadużyć z wykorzystaniem deepfake'ów w państwach Unii Europejskiej

Zjawisko podszywania się przy użyciu technologii deepfake nie ogranicza się do państw trzecich ani do pojedynczych, incydentalnych zdarzeń, lecz znajduje swoje potwierdzenie również w praktyce państw członkowskich Unii Europejskiej. Przypadki opisywane w prasie europejskiej pokazują, że technologia ta jest wykorzystywana zarówno w obrocie gospodarczym, jak i w sferze publicznej, prowadząc do poważnych strat finansowych oraz podważenia zaufania do komunikacji cyfrowej (Reuters, 2025).

Jednym z najbardziej znaczących przykładów jest sprawa ujawniona we Włoszech w 2025 r., w której sprawcy posłużyli się wygenerowanym za pomocą technologii deepfake głosem ministra obrony w celu wyłudzenia środków finansowych od znanych przedsiębiorców. W rozmowach telefonicznych podszywano się pod przedstawicieli administracji publicznej,

powołując się na rzekome działania państwowe wymagające pilnego wsparcia finansowego. Co najmniej jeden z adresatów tych rozmów dokonał przelewu na kwotę około jednego miliona euro, pozostając w przekonaniu, że działa na podstawie autentycznego polecenia organu państwowego. Sprawa ta została nagłośniona w mediach międzynarodowych i stała się przedmiotem postępowania organów ścigania, którym udało się zablokować przekazane środki.

Przypadek ten pokazuje, że deepfake'i mogą być wykorzystywane do podszywania się nie tylko pod osoby prywatne lub kadrę zarządzającą przedsiębiorstw, lecz także pod przedstawicieli władzy publicznej. W konsekwencji zagrożone zostaje nie tylko bezpieczeństwo obrotu gospodarczego, lecz również zaufanie obywateli do instytucji państwowych i oficjalnych kanałów komunikacji.

W jednym z pierwszych szeroko opisywanych przypadków w Europie dyrektor spółki zależnej w UE otrzymał telefon od osoby, która brzmiała dokładnie jak prezes spółkimatki z Niemiec. Na podstawie rozmowy telefonicznej nakazano mu dokonanie pilnego przelewu ok. 220 tys. EUR. Dopiero później ustalono, że rozmowa została przeprowadzona przy użyciu technologii klonowania głosu. Sprawa ta jest często wskazywana w literaturze jako *początek fali deepfake'ów w oszustwach korporacyjnych w Europie,* pokazując, że problem istniał jeszcze przed masowym upowszechnieniem technologii deepfake (ZDNet, 2019).

Opisane przypadki pokazują, że podszywanie się w rozmowach wideo przy użyciu technologii deepfake nie ma charakteru hipotetycznego, lecz stanowi realne, powtarzalne zagrożenie, prowadzące do poważnych strat finansowych. Kluczowe jest to, że tradycyjne kryteria weryfikacji tożsamości oparte na obrazie i głosie tracą swoją wiarygodność, co wymusza zmianę standardów należytej staranności oraz uzasadnia interwencję regulacyjną, w tym rozwiązania prawne przyjęte w odniesieniu do deepfake w UE – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Artificial Intelligence Act), Dz. U. UE L 2024/1689, art. 3 pkt 60, art. 4, art. 50 ust. 2 (EUR-Lex, b.d.).

Powyższe dane empiryczne stanowią podstawę do interpretacji, że demokratyzacja technologii deepfake prowadzi do jakościowej zmiany zagrożeń.

Deepfake a prawo – wyzwania regulacyjne

Regulacja deepfake'ów w Rozporządzeniu o sztucznej inteligencji (AI Act) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji (AI Act) stanowi pierwszy kompleksowy akt prawa unijnego, który wprost odnosi się do zjawiska deepfake'ów jako systemowego zagrożenia dla zaufania do komunikacji cyfrowej. Ustawodawca unijny przyjął założenie, że problemem nie jest wyłącznie sama technologia, lecz powszechność jej stosowania oraz ryzyko wprowadzania odbiorców w błąd co do autentyczności treści audiowizualnych.

Definicja deepfake w AI Act (art. 3 pkt 60 AI Act) – AI Act wprowadza legalną definicję „deepfake", w której „deepfake" oznacza wygenerowane przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmiot (art. 3 pkt 60 AI Act). Definicja ta ma kluczowe znaczenie interpretacyjne, ponieważ pozwala objąć regulacją nie tylko treści tworzone w całości jako technologia deepfake, lecz także materiały częściowo zmodyfikowane, jeżeli mogą one wprowadzać odbiorcę w błąd co do ich rzeczywistego charakteru.

Obowiązek ujawniania treści deepfake (transparentność) – Centralnym mechanizmem regulacyjnym AI Act w odniesieniu do deepfake'ów jest obowiązek transparentności. Zgodnie z art. 50 AI Act, podmioty udostępniające lub stosujące systemy AI generujące lub modyfikujące treści audiowizualne są zobowiązane do poinformowania odbiorców, że dana treść została wygenerowana lub zmanipulowana przez AI, jeżeli mogłaby ona sprawiać wrażenie autentycznej - Motywy Rozporządzenia (UE) 2024/1689 dotyczące transparentności treści generowanych przez AI oraz ochrony odbiorców przed wprowadzaniem w błąd. Celem tego rozwiązania nie jest zakazanie deepfake'ów jako takich, lecz przywrócenie równowagi informacyjnej po stronie odbiorcy. Ustawodawca unijny uznał, że brak wiedzy o syntetycznym charakterze treści stanowi zasadnicze źródło ryzyka prawnego i społecznego, w tym ryzyka manipulacji, oszustw oraz naruszenia dóbr osobistych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Artificial Intelligence Act), art. 50 ust. 2, Dz. U. UE L 2024/1689 (EUR-Lex, b.d.).

Obowiązek kompetencji (AI literacy) – Istotnym uzupełnieniem obowiązku ujawniania jest wprowadzony w art. 4 AI Act obowiązek zapewnienia

odpowiedniego poziomu kompetencji w zakresie sztucznej inteligencji po stronie dostawców oraz podmiotów stosujących systemy AI. Przepis ten ma charakter horyzontalny i obejmuje również podmioty korzystające z narzędzi generujących treści deepfake.

Z perspektywy prawa oznacza to, że brak wiedzy technicznej lub nieświadomość ryzyk związanych z deepfake'ami nie może stanowić usprawiedliwienia dla podmiotów profesjonalnych. AI Act przesuwa ciężar odpowiedzialności z indywidualnego odbiorcy na organizacje, które decydują się wykorzystywać systemy AI w działalności gospodarczej lub instytucjonalnej.

Czas obowiązywania przepisów AI Act – AI Act został opublikowany w Dzienniku Urzędowym UE w 2024 r. i wszedł w życie 20 dni po publikacji. Z uwagi na zakres regulacji przewidziano jednak stopniowe stosowanie przepisów. Przepisy ogólne, w tym definicje oraz obowiązek AI literacy, zaczęły obowiązywać wcześniej. Obowiązki dotyczące transparentności deepfake'ów, w tym art. 50, stosuje się od 2 sierpnia 2026 r. Oznacza to, że podmioty działające na rynku unijnym mają określony czas na dostosowanie procedur organizacyjnych i komunikacyjnych do nowych wymogów**.**

Deregulacja („Omnibus") a regulacja deepfake w AI Act

W debacie publicznej oraz eksperckiej towarzyszącej wdrażaniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji (AI Act) pojawiły się pytania o wpływ równolegle zapowiadanych inicjatyw deregulacyjnych Komisji Europejskiej, określanych zbiorczo mianem pakietu „Omnibus", na zakres i trwałość obowiązków przewidzianych w tym akcie. W szczególności dotyczy to regulacji odnoszących się do treści typu deepfake, które już na etapie prac legislacyjnych zostały uznane za istotne zagrożenie dla zaufania do komunikacji cyfrowej.

Pod pojęciem „Omnibus deregulacyjny" rozumie się zapowiadany w latach 2024-2025 pakiet inicjatyw Komisji Europejskiej mających na celu ograniczenie nadmiernych obciążeń administracyjnych, uproszczenie obowiązków sprawozdawczych oraz poprawę konkurencyjności przedsiębiorstw działających na rynku wewnętrznym Unii Europejskiej. Należy podkreślić, że Omnibus nie stanowi jednego, spójnego aktu prawnego, lecz zbiór propozycji o zróżnicowanym charakterze normatywnym, obejmujących m.in. zapowiedzi legislacyjne, przeglądy istniejących regulacji oraz instrumenty

typu soft law. Zakres tych inicjatyw koncentruje się przede wszystkim na obszarach takich jak raportowanie niefinansowe, regulacje ESG czy wybrane obowiązki compliance.

Na obecnym etapie brak jest jednak jakichkolwiek podstaw do twierdzenia, że inicjatywy deregulacyjne Omnibus wpływają na regulację deepfake'ów zawartą w AI Act. Rozporządzenie to zostało przyjęte jako akt o charakterze horyzontalnym i systemowym, którego celem jest ochrona interesów publicznych o fundamentalnym znaczeniu, w tym zaufania do rynku, ochrony konsumentów oraz praw podstawowych. Przepisy odnoszące się do deepfake'ów, w szczególności legalna definicja zawarta w art. 3 pkt 60 AI Act oraz obowiązek transparentności przewidziany w art. 50 AI Act, nie zostały objęte żadnym projektem uchylenia, zawieszenia ani modyfikacji w ramach zapowiadanych działań deregulacyjnych. Nie istnieje również akt prawa wtórnego ani projekt legislacyjny, który zmieniałby obowiązek ujawniania syntetycznego charakteru treści audiowizualnych generowanych lub modyfikowanych przez systemy AI.

Trwałość regulacji deepfake w AI Act znajduje silne uzasadnienie aksjologiczne i funkcjonalne. Deepfake'i zostały bowiem zakwalifikowane przez unijnego prawodawcę nie jako zwykłe obciążenie administracyjne dla przedsiębiorców, lecz jako zjawisko stwarzające ryzyko systemowe dla zaufania publicznego. Obowiązek transparentności przewidziany w art. 50 AI Act służy ochronie odbiorcy przed wprowadzaniem w błąd i odnosi się bezpośrednio do takich wartości jak integralność rynku wewnętrznego, bezpieczeństwo obrotu gospodarczego, ochrona konsumentów oraz poszanowanie praw podstawowych, w tym prawa do informacji i autonomii decyzyjnej. Są to obszary, które Komisja Europejska konsekwentnie wyłącza z zakresu deregulacji, uznając je za nienegocjowalne elementy porządku prawnego Unii.

W konsekwencji inicjatywy deregulacyjne mogą wywierać jedynie pośredni wpływ na praktykę stosowania przepisów dotyczących deepfake-'ów, nie zaś na ich obowiązywanie normatywne. Możliwy wpływ Omnibusa może przejawiać się na poziomie interpretacyjnym, w szczególności poprzez akcentowanie zasady proporcjonalności w sposobie realizacji obowiązków transparentności, większą rolę wytycznych Komisji Europejskiej oraz organów nadzorczych, a także promowanie technicznych form samoregulacji, takich jak standardy branżowe czy rozwiązania typu watermarking.

Nie oznacza to jednak zniesienia ani osłabienia obowiązku ujawniania treści deepfake, lecz jedynie potencjalne zróżnicowanie form jego wykonania.

Powyższe prowadzi do wniosku, że regulacja deepfake'ów w AI Act stanowi trwały element unijnego porządku prawnego, odporny na bieżące inicjatywy deregulacyjne. Deepfake nie jest bowiem traktowany jako koszt regulacyjny, lecz jako ryzyko strukturalne dla bezpieczeństwa informacji i zaufania do komunikacji cyfrowej, co uzasadnia utrzymanie rygorystycznych obowiązków transparentności niezależnie od zmian w innych obszarach prawa unijnego.

Deepfake a ochrona danych osobowych (GDPR)

Rozwój technologii deepfake rodzi istotne pytania dotyczące zakresu i skuteczności ochrony przewidzianej w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 (GDPR) (EUR-Lex, b.d.).

Mogłoby się wydawać, że regulacja ochrony danych osobowych stanowi wystarczający instrument przeciwdziałania nadużyciom związanym z wykorzystywaniem wizerunku, głosu lub innych cech osoby fizycznej w technologii deepfake. Pogłębiona analiza prowadzi jednak do wniosku, że GDPR jedynie częściowo obejmuje zjawisko deepfake i nie odpowiada na jego kluczowe ryzyka systemowe. GDPR chroni dane osobowe, ale nie chroni prawdziwości ani autentyczności treści, co stanowi lukę w kontekście deepfake. (European Data Protection Board, 2024). GDPR nie przeciwdziała skutecznie dezinformacji, manipulacji ani erozji zaufania, ponieważ koncentruje się na relacji administrator – dane, a nie na skutkach społecznych mediów syntetycznych. (European Parliament Tackling deepfakes in European policy, 2021).

Analiza prowadzi jednak do wniosku, że GDPR jedynie częściowo obejmuje zjawisko deepfake i nie odpowiada na jego kluczowe ryzyka systemowe.

Po pierwsze, choć wizerunek twarzy, nagranie głosu oraz cechy biometryczne wykorzystywane w technologii deepfake co do zasady mieszczą się w definicji danych osobowych, a niekiedy również danych biometrycznych w rozumieniu GDPR, regulacja ta koncentruje się na legalności przetwarzania danych, a nie na skutkach społecznych i informacyjnych generowanych treści syntetycznych. GDPR chroni dane osobowe jako takie, lecz nie zapewnia

ochrony prawdziwości ani autentyczności treści, co stanowi zasadniczą lukę w kontekście deepfake'ów, których istotą jest wytworzenie realistycznej, lecz fałszywej reprezentacji osoby mogącej wprowadzać odbiorców w błąd.

Po drugie, GDPR nie przeciwdziała skutecznie dezinformacji, manipulacji ani erozji zaufania do komunikacji audiowizualnej. Mechanizmy ochrony danych osobowych nie są projektowane z myślą o zapobieganiu zjawiskom takim jak masowa dystrybucja deep fake, manipulacja opinią publiczną czy tzw. *liar's dividend*, polegający na możliwości kwestionowania autentycznych materiałów jako rzekomo wygenerowanych przez sztuczną inteligencję. Ochrona danych osobowych nie jest bowiem instrumentem służącym ochronie integralności dyskursu publicznego ani zaufania do informacji jako takiej.

Po trzecie, model odpowiedzialności przyjęty w GDPR opiera się na możliwości identyfikacji administratora danych oraz skutecznego egzekwowania wobec niego obowiązków. W praktyce deepfake'i są jednak często tworzone i rozpowszechniane w środowisku transgranicznym, anonimowo lub przy wykorzystaniu zdecentralizowanych platform, co znacząco ogranicza realną skuteczność instrumentów takich jak prawo do usunięcia danych czy prawo do sprzeciwu. Usunięcie danych źródłowych nie prowadzi ponadto do usunięcia skutków ich wcześniejszego wykorzystania, zwłaszcza gdy modele generatywne zostały już wytrenowane, a treści weszły do obiegu informacyjnego.

Powyższe ograniczenia tłumaczą, dlaczego GDPR nie może być traktowane jako wystarczający instrument reagowania na zagrożenia związane z deepfake'ami. Ochrona przed skutkami tej technologii wymaga bowiem nie tylko kontroli nad danymi osobowymi, lecz także regulacji ukierunkowanych na transparentność treści, ochronę odbiorcy przed wprowadzaniem w błąd oraz przeciwdziałanie ryzykom systemowym dla zaufania do komunikacji cyfrowej. Z tego względu unijny prawodawca zdecydował się na przyjęcie odrębnych regulacji w AI Act, które uzupełniają, a nie zastępują, mechanizmy ochrony danych osobowych przewidziane w GDPR. (European Data Protection Board, 2024; European Parliament – STOA, 2021; Levitt, 2024).

Na podstawie przedstawionych regulacji można stwierdzić, że istniejące ramy prawne nie zapewniają ochrony przed systemowymi skutkami dezinformacji – co potwierdza obserwacja, że RODO nie nadąża za dynamiką rozwoju technologii i nie zapewnia ochrony przed systemowymi skutkami dezinformacji.

Od ochrony danych osobowych do ochrony zaufania informacyjnego: ewolucja podejścia Unii Europejskiej.

Analiza ograniczeń GDPR w kontekście technologii deepfake prowadzi do szerszego wniosku o charakterze systemowym. Regulacja ochrony danych osobowych została zaprojektowana w odmiennym paradygmacie ryzyk. GDPR koncentruje się na relacji administrator-dane oraz na ochronie jednostki przed nieuprawnionym przetwarzaniem informacji dotyczących jej osoby. Tymczasem technologia deepfake generuje zagrożenia, które wykraczają poza sferę indywidualnej prywatności i obejmują bezpieczeństwo informacyjne, wiarygodność komunikacji oraz zaufanie do treści audiowizualnych jako podstawy podejmowania decyzji.

W tym sensie deepfake ujawnia granice paradygmatu ochrony danych osobowych jako podstawowego instrumentu reagowania na nowe zagrożenia informacyjne. Nawet pełna zgodność z wymogami GDPR nie zapobiega bowiem erozji zaufania do komunikacji cyfrowej, masowej dezinformacji ani możliwości kwestionowania autentycznych treści jako rzekomo wygenerowanych przez sztuczną inteligencję. Ochrona danych osobowych nie jest narzędziem zaprojektowanym do ochrony prawdziwości, autentyczności ani integralności informacji jako takiej.

Na tym tle Rozporządzenie o sztucznej inteligencji (AI Act) należy postrzegać nie jako konkurencyjną wobec GDPR regulację, lecz jako kolejny etap ewolucji unijnego podejścia do ryzyk technologicznych. AI Act przesuwa punkt ciężkości z ochrony danych osobowych sensu stricto na ochronę odbiorcy informacji oraz stabilności środowiska informacyjnego. Wprowadzenie legalnej definicji deepfake oraz obowiązku transparentności treści technologii deepfake stanowi odpowiedź na ryzyka, których GDPR nie był w stanie objąć ze względu na swój zakres przedmiotowy i aksjologiczny.

Na podstawie dokonanej analizy można stwierdzić stopniowe przejście od regulacji skoncentrowanej na ochronie jednostki przed nadużyciami w przetwarzaniu danych do regulacji ukierunkowanej na ochronę zaufania publicznego, integralności rynku oraz autonomii decyzyjnej odbiorców treści cyfrowych. AI Act nie zastępuje GDPR, lecz je uzupełnia, odpowiadając na jakościowo nowe zagrożenia związane z generatywną sztuczną inteligencją, w tym z masową produkcją treści, które mogą sprawiać wrażenie autentycznych, mimo że zostały wygenerowane za pomocą technologii deepfake.

Deepfake w kontekście prawa autorskiego

Rozwój technologii deepfake rodzi istotne wyzwania na gruncie prawa autorskiego (Ustawa o prawie autorskim i prawach pokrewnych, 1994, art. 1, art. 2, art. 16, art. 17), zarówno w zakresie legalności wykorzystywania materiałów źródłowych, jak i statusu prawnego treści wygenerowanych syntetycznie. Problematyka ta dotyczy w szczególności relacji pomiędzy twórcą pierwotnego utworu, osobą, której wizerunek lub głos są wykorzystywane, a podmiotem generującym deepfake (European Copyright Society, 2023).

W pierwszej kolejności należy zwrócić uwagę, że proces tworzenia deepfake'ów niemal zawsze opiera się na wykorzystaniu istniejących utworów, takich jak nagrania wideo, materiały audio, fotografie czy wystąpienia publiczne (WIPO, 2019-2023). Materiały te, o ile spełniają przesłanki twórczości, podlegają ochronie na gruncie prawa autorskiego. Ich pobieranie, kopiowanie oraz przetwarzanie w celu trenowania modeli generatywnych może stanowić zwielokrotnianie i opracowanie utworu, wymagające zgody uprawnionego, chyba że znajduje zastosowanie jedna z ustawowych licencji lub wyjątków.

W praktyce problematyczne jest w szczególności trenowanie modeli AI na publicznie dostępnych materiałach audiowizualnych, bez zgody autorów. Choć w debacie pojawiają się argumenty odwołujące się do dozwolonego użytku lub analiz tekstów i danych (text and data mining), zakres tych wyjątków jest ograniczony i nie zawsze obejmuje wykorzystanie utworów w celu generowania realistycznych, konkurencyjnych treści audiowizualnych. W konsekwencji deepfake'i mogą prowadzić do naruszenia majątkowych praw autorskich, a w niektórych przypadkach również autorskich praw osobistych, zwłaszcza gdy wygenerowana treść zniekształca sens, kontekst lub wymowę pierwotnego utworu. Odrębną kwestią pozostaje status prawny samego deepfake'a jako utworu (Gervais, 2019). Zgodnie z dominującym poglądem, treści wygenerowane w pełni autonomicznie przez system AI nie korzystają z ochrony prawa autorskiego, ponieważ brak jest elementu twórczości człowieka. W praktyce jednak wiele deepfake'ów powstaje przy istotnym udziale użytkownika, który dobiera materiały źródłowe, parametry generowania oraz dokonuje selekcji efektów. W takich przypadkach możliwe jest uznanie deepfake'a za utwór zależny lub utwór inspirowany, co dodatkowo komplikuje relacje prawnoautorskie i utrudnia jednoznaczne przypisanie odpowiedzialności (Barta, Markiewicz, 2023; Samuelson, 2017).

Z perspektywy bezpieczeństwa informacji istotne jest, że prawo autorskie nie zostało zaprojektowane jako instrument ochrony przed dezinformacją. Nawet skuteczna ochrona praw twórców nie zapobiega bowiem rozpowszechnianiu treści syntetycznych, które formalnie nie naruszają praw autorskich, a jednocześnie mogą wprowadzać odbiorców w błąd co do autentyczności przekazu. Oznacza to, że prawo autorskie pełni w kontekście deepfake'ów funkcję jedynie częściowo ochronną i nie odpowiada na kluczowe ryzyka systemowe.

Deepfake a zniesławienie i ochrona dóbr osobistych

Technologia deepfake stanowi szczególnie poważne wyzwanie w obszarze zniesławienia oraz naruszenia dóbr osobistych, ponieważ umożliwia przypisywanie osobom fizycznym wypowiedzi, zachowań lub cech, których w rzeczywistości nigdy nie przejawiały. W przeciwieństwie do tradycyjnych form fałszu, deepfake'y charakteryzują się wysokim stopniem realizmu, co znacząco zwiększa ich siłę oddziaływania oraz potencjał szkodliwy: Kodeks cywilny – art. 23-24 (ochrona dóbr osobistych); Kodeks karny – art. 212 (zniesławienie), art. 216 (zniewaga). Europejska Konwencja Praw Człowieka – art. 8 i art. 10 (prawo do prywatności vs. wolność wypowiedzi).

Na gruncie prawa cywilnego deepfake może prowadzić do naruszenia takich dóbr osobistych jak cześć, dobre imię, reputacja, wizerunek czy prawo do tożsamości. Wygenerowanie i rozpowszechnienie realistycznego nagrania wideo lub audio, sugerującego określone wypowiedzi lub działania danej osoby, może wywołać trwałe skutki reputacyjne, niezależnie od późniejszego sprostowania. Szczególnie niebezpieczne są sytuacje, w których deepfake funkcjonuje w obiegu informacyjnym przez krótki czas, lecz zdąży wywrzeć znaczący wpływ na opinię publiczną.

W kontekście prawa karnego deepfake'y mogą realizować znamiona zniesławienia lub zniewagi, zwłaszcza gdy przypisują osobie cechy lub działania mogące ją poniżyć w opinii publicznej albo narazić na utratę zaufania potrzebnego do wykonywania określonej funkcji. Charakterystyczną cechą deepfake'ów jest jednak utrudniona identyfikacja sprawcy, często działającego anonimowo, transgranicznie lub przy użyciu zdecentralizowanych platform. W praktyce znacząco ogranicza to skuteczność klasycznych instrumentów odpowiedzialności karnej.

Szczególną kategorię stanowią deepfake'i naruszające dobra osobiste o charakterze intymnym, tworzone i rozpowszechniane bez zgody osoby, której wizerunek lub głos zostały wykorzystane. Skutki takich działań wykraczają poza sferę reputacyjną i obejmują poważne konsekwencje psychologiczne, społeczne oraz zawodowe. W tych przypadkach deepfake staje się narzędziem przemocy informacyjnej, a jego realizm potęguje doznaną krzywdę.

Z perspektywy systemowej kluczowe jest to, że zniesławienie przy użyciu deepfake różni się jakościowo od tradycyjnych form pomówienia. Odbiorca ma bowiem do czynienia nie z opinią lub relacją, lecz z pozornie bezpośrednim „dowodem" w postaci obrazu lub głosu. W rezultacie dochodzi do podważenia zaufania nie tylko do konkretnej osoby, lecz także do komunikacji audiowizualnej jako takiej. Zjawisko to wpisuje się w szerszy problem erozji zaufania informacyjnego, który nie może być skutecznie rozwiązany wyłącznie za pomocą klasycznych instytucji prawa cywilnego i karnego.

W konsekwencji deepfake ujawnia ograniczenia tradycyjnych konstrukcji zniesławienia, opartych na założeniu, że fałszywość przekazu da się stosunkowo łatwo wykazać, a jego autor zidentyfikować. W warunkach masowej produkcji realistycznych treści syntetycznych założenia te przestają być aktualne, co uzasadnia potrzebę uzupełnienia ochrony dóbr osobistych o rozwiązania systemowe, takie jak obowiązek transparentności treści, podnoszenie kompetencji cyfrowych oraz mechanizmy prewencji organizacyjnej (Ajder i in., 2019; WEF, 2024).

Podsumowanie

Analiza technologii deepfake przeprowadzona w niniejszym opracowaniu prowadzi do wniosku, że demokratyzacja tej technologii stanowi czynnik strukturalny współczesnych zagrożeń informacyjnych, a nie jedynie uboczny efekt postępu technologicznego. Obniżenie progu wejścia do tworzenia realistycznych treści poprzez dostępność narzędzi open source, usług chmurowych oraz intuicyjnych interfejsów spowodowało jakościową zmianę charakteru ryzyka. Deepfake przestał być technologią niszową, wymagającą specjalistycznej wiedzy i zaplecza technicznego, a stał się

narzędziem powszechnie dostępnym, zdolnym do masowego oddziaływania na środowisko informacyjne.

Demokratyzacja technologii deepfake oznacza, że zagrożenia związane z manipulacją treściami audiowizualnymi nie mają już charakteru incydentalnego, lecz przybierają formę zjawiska systemowego. Skala potencjalnych nadużyć wykracza poza możliwości reagowania opartych wyłącznie na odpowiedzialności ex post, takich jak dochodzenie roszczeń cywilnych czy ściganie karne sprawców. W warunkach masowej produkcji i dystrybucji treści syntetycznych tradycyjne instrumenty prawne okazują się niewystarczające, a sama identyfikacja sprawcy często staje się niemożliwa. W konsekwencji demokratyzacja deepfake'ów należy postrzegać jako czynnik strukturalnie zmieniający architekturę bezpieczeństwa informacji, a nie jedynie jako nowe narzędzie wykorzystywane w ramach istniejących schematów zagrożeń. W tym kontekście kluczowym wnioskiem jest konieczność łączenia trzech komplementarnych obszarów działań: regulacji prawnych, edukacji w zakresie kompetencji cyfrowych i sztucznej inteligencji (AI literacy) oraz rozwiązań technicznych. Żaden z tych elementów, rozpatrywany w oderwaniu od pozostałych, nie jest w stanie skutecznie przeciwdziałać zagrożeniom wynikającym z masowego wykorzystania deepfake'ów.

Po pierwsze, regulacje prawne, w szczególności przyjęte na poziomie Unii Europejskiej Rozporządzenie o sztucznej inteligencji (AI Act), stanowią niezbędne ramy normatywne dla reagowania na ryzyka związane z deepfake'ami. Wprowadzenie legalnej definicji deepfake oraz obowiązku transparentności należy postrzegać jako próbę przywrócenia równowagi informacyjnej po stronie odbiorcy. Regulacja ta nie zmierza do zakazania technologii jako takiej, lecz do ograniczenia jej potencjału manipulacyjnego poprzez wymóg ujawniania charakteru jej treści. Jednocześnie analiza wykazuje, że prawo nawet w swojej najbardziej nowoczesnej postaci nie jest w stanie samodzielnie zagwarantować bezpieczeństwa informacji w środowisku cyfrowym, w którym treści mogą być generowane i rozpowszechniane z ogromną szybkością.

Po drugie, edukacja i rozwój kompetencji w zakresie AI (AI literacy) stanowią kluczowy element prewencji. Obowiązek zapewnienia odpowiedniego poziomu kompetencji, przewidziany w AI Act, sygnalizuje przesunięcie odpowiedzialności z indywidualnego odbiorcy na organizacje i instytucje korzystające z systemów AI. W praktyce oznacza to

konieczność systematycznego budowania świadomości ryzyk związanych z deepfake'ami, zarówno wśród pracowników sektora publicznego i prywatnego, jak i w społeczeństwie jako całości. Brak wiedzy technicznej lub nieumiejętność krytycznej oceny treści audiowizualnych przestają być kwestią indywidualnej ostrożności, a stają się czynnikiem ryzyka organizacyjnego i systemowego.

Po trzecie, nieodzowne są rozwiązania techniczne, obejmujące zarówno systemy wykrywania deepfake, jak i mechanizmy oznaczania, uwierzytelniania oraz śledzenia pochodzenia treści. W warunkach, w których generowanie deepfake'ów odbywa się w skali masowej i w czasie rzeczywistym, wykrywanie nie może opierać się wyłącznie na ludzkiej percepcji czy manualnej weryfikacji. Rozwiązania techniczne powinny być traktowane nie jako narzędzie opcjonalne, lecz jako integralny element infrastruktury bezpieczeństwa informacji, porównywalny do systemów ochrony przed złośliwym oprogramowaniem czy filtrów antyspamowych.

Zestawienie tych trzech obszarów prowadzi do kluczowego wniosku o konieczności podejścia systemowego do bezpieczeństwa informacji. Deepfake nie jest bowiem wyłącznie problemem technologicznym, prawnym czy etycznym, lecz zjawiskiem, które podważa fundamenty zaufania do komunikacji audiowizualnej jako takiej. Erozja tego zaufania ma bezpośrednie konsekwencje dla funkcjonowania rynku, instytucji publicznych, procesów decyzyjnych oraz demokracji. Odpowiedzią na te wyzwania nie może być fragmentaryczna interwencja, lecz skoordynowany model łączący regulacje, edukację i technologię.

Podsumowując, analiza demokratyzacji technologii deepfake pozwala lepiej zrozumieć, dlaczego współczesne zagrożenia informacyjne mają charakter masowy, trudny do kontrolowania i wykraczający poza tradycyjne ramy regulacyjne. Deepfake nie jest jedynie kolejnym narzędziem manipulacji, lecz symptomem głębszej transformacji środowiska informacyjnego, w którym autentyczność przestaje być oczywista, a zaufanie wymaga aktywnej ochrony. W tym sensie wyzwania związane z deepfake'ami stanowią jeden z kluczowych testów zdolności systemów prawnych, organizacyjnych i technologicznych do adaptacji w erze generatywnej sztucznej inteligencji.

Literatura

1. Afshari, N., Mohammadi, A. (2023). *The Legal Implications of Deepfake Technology: Privacy, Defamation, and the Challenge of Regulating Synthetic Media*, Legal Studies in Digital Age, t. 2, nr 2, s. 13-23; s. 16-19. Pobrano z: https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019 (dostęp: 15.02.2026).
2. Ajder, H., Patrini, G., Cavalli, F., Cullen, L., (2019). *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace Labs., Amsterdam. Pobrano z: regmedia.co.uk.; https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (dostęp: 15.02.2026).
3. Barta, J., Markiewicz, R. (2023). *Prawo autorskie*, Wolters Kluwer, Warszawa.
4. Chesney, R., Citron, D. (2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, t. 107, nr 6, s. 1753-1820. Publisher University of California Berkeley School of Law. Pobrano z: https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security (dostęp: 10.03.2026; Pobrano z: https://scholarship.law.bu.edu/faculty_scholarship/640/ (dostęp: 15.02.2026).
5. European Commission. (2020). *European Commission – Joint Research Centre (JRC) Artificial Intelligence and Disinformation: Assessment of Risks and Countermeasures (2020).* Pobrano z: https://publications.jrc.ec.europa.eu/repository/handle/JRC122150, (dostęp: 15.02.2026).
6. European Copyright Society. (2023). *Opinion on AI Training and Copyright*, Copyright and Generative AI: Opinion of the European Copyright Society (online) (dostęp: 15.02.2026). dokument został przyjęty merytorycznie w 2023 r., natomiast oficjalnie opublikowany w 2025 r. przez European Copyright Society.
7. European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. (przyjęta: 17 grudnia 2024 r., opublikowana: 18 grudnia 2024 r.). Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models | European Data Protection Board (online), (dostęp: 15.02.2026).

8. European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* Adopted on 17 December 2024. Pobrano z: https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf (dostęp: 15.02.2026); EDPB (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. 18 December 2024.* Pobrano z: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en (dostęp: 15.02.2026).
9. EUR-Lex. (b.d.). Document 32024R1689; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 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). Pobrano z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689 (dostęp: 15.02.2026); https://sip.lex.pl/akty-prawne/dzienniki-UE/rozporzadzenie-2024-1689-w-sprawie-ustanowienia-zharmonizowanych-przepisow-72359064 (dostęp: 15.02.2026); ELI: http://data.europa.eu/eli/reg/2024/1689/oj (dostęp: 15.02.2026); https://eur-lex.europa.eu/eli/reg/2024/1689/oj (dostęp: 15.02.2026).
10. EUR-Lex. (b.d.). Document 32016R0679, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) – Dz.U. UE L 119 z 4 maja 2016, s. 1-88. Pobrano z: https://eur-lex.europa.eu/eli/reg/2016/679/oj (dostęp: 15.02.2026).
11. EUR-Lex. (b.d.). Document 32024R1689; ELI: http://data.europa.eu/eli/reg/2024/1689/oj; Pobrano z: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (dostęp: 15.02.2026).

12. European Parliament – STOA. (2021). *Tackling deepfakes in European policy*. Study, Scientific Foresight Unit (STOA), DirectorateGeneral for Parliamentary Research Services (EPRS), Brussels. Tackling deepfakes in European policy | Think Tank | European Parliament (online), (dostęp: 15.02.2026).
13. European Parliament Tackling deepfakes in European policy. (2021). Pobrano z: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_BRIE%282021%29690039%28ANN%29_EN.pdf (dostęp: 15.02.2026).
14. Etienne, H. (2021). The future of online trust (and why Deepfake is advancing it). W: J. MacIntyre, L. Medsker (red.), *AI and Ethics* (s. 553-562). Springer. https://doi.org/10.1007/s43681-021-00072-1
15. Future Advocacy. (2019). *Deepfakes*, Deepfakes - Future Advocacy, Pobrano z: https://futureadvocacy.com/case-studies/deepfakes/ (dostęp: 15.02.2026).
16. Galindo, G. (2020). *XR Belgium posts deepfake of Belgian premier linking Covid19 with climate crisis*. The Brussels Times. Pobrano z: https://www.brusselstimes.com/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis (dostęp: 15.02.2026).
17. Gervais, D. (2019), *The Machine as Author*, Iowa Law Review, t. 105.
18. Gil, Ł. (2026). *Socjotechnika 2.0 – Nowe trendy w atakach na czynnik ludzki*, Pobrano z: https://nflo.pl/baza-wiedzy/socjotechnika-nowe-trendy-ataki/ (dostęp: 15.02.2026).
19. Harvey Kong. (2024). Hong Kong Police / South China Morning Post (2024), *'Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting*. South China Morning Post „ '*Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting",* 4 February 2024. Pobrano z: https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage (dostęp: 15.02.2026).
20. Integral Solution (b.d.). *Demokratyzacja Generatywnej Sztucznej Inteligencji (GAI),* https://integralsolutions.pl/demokratyzacja-generatywnej-ai-gai/ (dostęp: 15.02.2026).

21. Lumen, C. (2025). *Deepfakes and the Limits of Law: A Comparative Analysis of Regulatory Frameworks in the U.S., EU, and China*.
22. Levitt, A. (2024). *Navigating Privacy in the Age of AI: Evaluating the Adequacy of the GDPR and CCPA to Combat Deepfake Technology*, NHSJS.
23. NASK. (2025). *Deepfaki – prawdziwy problem z fałszywą rzeczywistością*. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy. Pobrano z: https://www.nask.pl/magazyn/deepfaki-prawdziwy-problem-z-falszywa-rzeczywistoscia (dostęp: 15.02.2026).
24. Regan, G. (2025). A Brief History of Deepfakes — Reality Defender. Pobrano z: https://www.realitydefender.com/insights/history-of-deepfakes (dostęp: 15.02.2026).
25. Reuters. (2025). *Scammer defrauds Italian businessman of €1m using AI voice*. Pobrano z: https://www.reuters.com/world/europe/scammer-defrauds-italian-businessman-1m-using-ai-voice-2025-02-13/ (dostęp: 15.02.2026).
26. Rmero Moreno, F. (2024). *Generative AI and deepfakes: a human rights approach to tackling harmful content*, International Review of Law, Computers & Technology.
27. European Commission. (2020). *Artificial Intelligence and Disinformation (White Paper on AI)*
28. Samuelson, P. (2017). *Allocating Ownership Rights in ComputerGenerated Works*, University of Pittsburgh Law Review.
29. Sensity AI. (2019-2024). *Deepfakes and Identity Fraud*.
30. Suwajanakorn, S., Seitz, S. M., Kemelmacher-Shlizerman, I. (2017). *Synthesizing Obama: Learning Lip Sync from Audio*, W: Proceedings of the ACM Transactions on Graphics (TOG), t. 36, nr 4, 2017, art. 95. Publisher: Association for Computing Machinery, New York United States.
31. Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., Nießner, M., (2016). *Face2Face: RealTime Face Capture and Reenactment of RGB Videos*, W: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (s. 2387-2395). Publisher: IEEE Institute of Electrical and Electronics Engineers. Pobrano z: https://ieeexplore.ieee.org/document/7780631 (dostęp: 10.03.2026).

32. The Guardian. (2024). „*UK engineering firm Arup falls victim to £20m deepfake scam”.* Pobrano z: https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video (dostęp: 15.02.2026).
33. Tookitaki. (2025). *The CEO Wasn't Real: Inside Singapore's $499K. Deepfake Video Scam*. Pobrano z: https://www.tookitaki.com/blog/deepfake-ceo-scam-singapore-2025.
34. Toews, R. (2022). *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared,* Forbes. Pobrano z: https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/ (dostęp: 15.02.2026).
35. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. z 2025 r. poz. 24. Pobrano z: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19940240083/U/D19940083Lj.pdf (dostęp: 15.02.2026).
36. WEF. (2024). *Global Risks Report.* Pobrano z: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf?_gl=1*jr4w0n*_up*MQ..*_gs*MQ..&gclid=EAIaIQobChMItuLJqrqXkwMVFBiiAx2mbTr3EAAYAiAAEgJXU_D_BwE&gbraid=0AAAAAoVy5F7Kuvrf-kac-tATd1bVSjEwgp (dostęp: 15.02.2026).
37. WIPO. (2019). *Artificial Intelligence and Intellectual Property*, World Intellectual Property Organization Geneva, Switzerland. Pobrano z: https://www.wipo.int/en/web/technology-trends/artificial_intelligence/story; https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf (dostęp: 11.03.2026).
38. ZDNet. (2019). „Forget email: scammers use CEO voice 'deepfakes' to con workers into wiring cash". Pobrano z: https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/ (dostęp: 15.02.2026); *Wall Street Journal* ((cyt. za ZDNet).
39. Zegarow, P. (2025). *Deepfaki – prawdziwy problem z fałszywą rzeczywistością,* NASK. Pobrano z: https://www.nask.pl/magazyn/deepfaki-prawdziwy-problem-z-falszywa-rzeczywistoscia (dostęp: 15.02.2026).
40. Zontek, K. (2025). *Deepfake – zagrożenia i środki ochrony,* AURACO. Pobrano z: https://auraco.pl/blog/deepfake-zagrozenia-i-srodki-ochrony/ (dostęp: 15.02.2026).

Zuzanna Jordan[1], Wojciech Kołakowski[2]

https://doi.org/10.29316/9788368103359_13

PRAWNA ODPOWIEDZIALNOŚĆ PODMIOTÓW ZA NARUSZENIA CYBERBEZPIECZEŃSTWA

LEGAL LIABILITY OF ENTITIES FOR CYBERSECURITY BREACHES

Streszczenie

Rozwój technologii cyfrowych oraz powszechne wykorzystanie systemów teleinformatycznych przez podmioty publiczne i prywatne spowodowały wzrost znaczenia cyberbezpieczeństwa jako przedmiotu regulacji prawnej. Opracowanie podejmuje analizę prawnej odpowiedzialności podmiotów za naruszenia cyberbezpieczeństwa, ze szczególnym uwzględnieniem normatywnych podstaw tej odpowiedzialności oraz jej zróżnicowanego charakteru. Omówiono obowiązki prawne wynikające z przepisów prawa krajowego i unijnego, w tym dyrektywy NIS 2 oraz ustawy o krajowym systemie cyberbezpieczeństwa. Przedstawiono również skutki prawne naruszeń cyberbezpieczeństwa oraz formy odpowiedzialności administracyjnej, cywilnoprawnej i karnej. Celem opracowania jest wykazanie, że naruszenia cyberbezpieczeństwa stanowią zdarzenia prawnie relewantne, rodzące wielopoziomowe

[1] https://orcid.org/0009-0009-2636-8501, email: zuzanna.jordan@protonmail.com
[2] https://orcid.org/0009-0009-3300-1580, email: wgkkolakowski@gmail.com

konsekwencje prawne. W opracowaniu zastosowano metodę analizy dogmatyczno-prawnej, polegającą na badaniu treści obowiązujących aktów normatywnych regulujących cyberbezpieczeństwo oraz odpowiedzialność prawną za naruszenia obowiązków w tym zakresie. Analizie poddano w szczególności przepisy prawa Unii Europejskiej oraz prawa krajowego odnoszące się do funkcjonowania krajowego systemu cyberbezpieczeństwa. Uzupełniająco wykorzystano analizę piśmiennictwa prawniczego, w zakresie istotnym dla określenia charakteru i zakresu odpowiedzialności prawnej za naruszenia cyberbezpieczeństwa

Słowa kluczowe: cyberbezpieczeństwo, odpowiedzialność prawna, naruszenie cyberbezpieczeństwa, systemy teleinformatyczne, prawo cyberbezpieczeństwa

Abstract

The development of digital technologies and the widespread use of ICT systems by public and private entities have resulted in an increase in the importance of cybersecurity as a subject of legal regulation. The study provides an analysis of the legal liability of entities for cybersecurity breaches, with particular emphasis on the normative bases of this liability and its diverse nature. Legal obligations arising from the provisions of national and EU law, including the NIS 2 Directive and the Act on the National Cybersecurity System, are discussed. The legal consequences of cybersecurity breaches and forms of administrative, civil and criminal liability are also presented. The aim of the study is to demonstrate that cybersecurity breaches are legally relevant events that have multi-level legal consequences. The study uses the method of dogmatic and legal analysis, which consists in examining the content of the applicable normative acts regulating cybersecurity and legal liability for breaches of obligations in this regard. In particular, the provisions of European Union law and national law relating to the functioning of the national cybersecurity system were analysed. In addition, the analysis of legal literature was used to the extent relevant to determining the nature and scope of legal liability for cybersecurity breaches.

Keywords: cybersecurity, legal liability, cybersecurity breach, ICT systems, cybersecurity law

Wstęp

Postępująca cyfryzacja życia społecznego i gospodarczego sprawiła, że systemy teleinformatyczne stały się podstawowym narzędziem realizacji

zadań publicznych oraz prowadzenia działalności gospodarczej. Przetwarzanie informacji, świadczenie usług oraz komunikacja coraz częściej odbywają się w cyberprzestrzeni, co zwiększa znaczenie zagadnień związanych z bezpieczeństwem funkcjonowania systemów informacyjnych. Jednocześnie rozwój technologiczny wiąże się z narastającą liczbą zagrożeń, które mogą prowadzić do naruszeń cyberbezpieczeństwa.

Cyberbezpieczeństwo zostało ujęte w obowiązujących regulacjach prawnych jako przedmiot ochrony wymagający podejmowania określonych działań prewencyjnych oraz reakcyjnych. Ustawodawca unijny oraz krajowy nałożył na wybrane podmioty obowiązki zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności obowiązki w zakresie zarządzania ryzykiem oraz zdolności do zapobiegania incydentom i reagowania na nie (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 21-23). Naruszenie tych obowiązków może skutkować powstaniem odpowiedzialności prawnej, niezależnie od tego, czy do naruszenia doszło na skutek działania, czy zaniechania podmiotu zobowiązanego.

Warto zauważyć, że cyberbezpieczeństwo nie jest już postrzegane wyłącznie jako zagadnienie techniczne (Chiara, 2024, s. 2-3). Obowiązujące regulacje prawne nadają mu charakter normatywny, czyniąc z niego element porządku prawnego podlegający ocenie z punktu widzenia zgodności zachowania podmiotów z prawem. Naruszenia cyberbezpieczeństwa mogą prowadzić do zakłócenia ciągłości działania usług, naruszenia praw osób fizycznych, a w określonych przypadkach również do zagrożenia interesu publicznego (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2, art. 8).

Celem niniejszego opracowania jest analiza prawnej odpowiedzialności podmiotów za naruszenia cyberbezpieczeństwa. Opracowanie koncentruje się na identyfikacji obowiązków prawnych związanych z zapewnieniem cyberbezpieczeństwa oraz na omówieniu konsekwencji prawnych wynikających z ich naruszenia. W opracowaniu zastosowano metodę analizy dogmatycznoprawnej, polegającą na badaniu treści obowiązujących aktów normatywnych regulujących zagadnienia cyberbezpieczeństwa.

Cyberbezpieczeństwo jako przedmiot ochrony prawnej i źródło obowiązków

Pojęcie cyberbezpieczeństwa nie posiada jednolitego, uniwersalnego znaczenia funkcjonującego we wszystkich porządkach prawnych. Jego treść normatywna jest kształtowana przez akty prawa krajowego oraz unijnego, które ujmują cyberbezpieczeństwo jako przedmiot ochrony prawnej wymagający podejmowania określonych działań organizacyjnych i technicznych. W tym ujęciu cyberbezpieczeństwo stanowi element bezpieczeństwa państwa, bezpieczeństwa informacji oraz bezpieczeństwa obrotu gospodarczego. Na gruncie prawa krajowego definicja cyberbezpieczeństwa została zawarta w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zgodnie z art. 2 pkt 4 tej ustawy cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz usług z nimi powiązanych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 4). Definicja ta wskazuje jednoznacznie, że cyberbezpieczeństwo nie ogranicza się wyłącznie do ochrony danych jako takich, lecz obejmuje również ciągłość i prawidłowość funkcjonowania systemów oraz usług opartych na technologiach informacyjnych. Ujęcie normatywne cyberbezpieczeństwa akcentuje jego charakter funkcjonalny. Nie jest ono rozumiane jako stan absolutnego bezpieczeństwa, lecz jako zdolność systemów informacyjnych do przeciwstawiania się zagrożeniom oraz do reagowania na incydenty. Tym samym cyberbezpieczeństwo przyjmuje postać dynamicznego procesu, którego celem jest ograniczanie ryzyka naruszeń oraz minimalizowanie ich skutków prawnych i faktycznych (Terebiński, 2018, s. 216-218).

Podobne podejście zostało przyjęte na poziomie prawa Unii Europejskiej. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (tzw. dyrektywa NIS 2) posługuje się pojęciem cyberbezpieczeństwa w kontekście bezpieczeństwa sieci i systemów informatycznych, kładąc nacisk na obowiązek zapewnienia wysokiego wspólnego poziomu ochrony w całej Unii (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022) (Chronowska-Sioła, 2025, s. 15-16) (Skoczylas, 2025, s. 231-233). Regulacja ta traktuje cyberbezpieczeństwo jako wartość podlegającą ochronie prawnej ze względu na znaczenie systemów informacyjnych dla funkcjonowania gospodarki, administracji publicznej oraz społeczeństwa. Normatywne

ujęcie cyberbezpieczeństwa prowadzi do wniosku, że jego zapewnienie nie ma charakteru fakultatywnego. Obowiązujące przepisy prawa nakładają na określone podmioty konkretne obowiązki, których celem jest utrzymanie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych. Naruszenie tych obowiązków skutkuje powstaniem konsekwencji prawnych, niezależnie od tego, czy doszło do rzeczywistej szkody. Cyberbezpieczeństwo funkcjonuje zatem w porządku prawnym jako przedmiot regulacji o charakterze prewencyjnym, a jednocześnie jako podstawa odpowiedzialności prawnej w przypadku wystąpienia naruszeń.

Cyberbezpieczeństwo, ujmowane w perspektywie normatywnej, pozostaje w ścisłym związku z pojęciem bezpieczeństwa prawnego oraz ochroną interesu publicznego. Funkcjonowanie współczesnych państw i gospodarek opiera się w znacznym stopniu na niezawodności systemów teleinformatycznych, które służą realizacji zadań publicznych, świadczeniu usług kluczowych oraz przetwarzaniu informacji o istotnym znaczeniu społecznym. Zakłócenia w tym obszarze mogą prowadzić do naruszenia stabilności porządku prawnego oraz osłabienia zaufania do instytucji publicznych i prywatnych. Bezpieczeństwo prawne rozumiane jest w doktrynie jako stan, w którym adresaci norm prawnych mogą racjonalnie przewidywać skutki swoich działań oraz polegać na stabilnym i skutecznym funkcjonowaniu systemu prawa (Chałubińska-Jentkiewicz, 2022, s. 23-25). Naruszenia cyberbezpieczeństwa, polegające przykładowo na zakłóceniu działania systemów administracji publicznej lub infrastruktury informacyjnej, mogą prowadzić do sytuacji, w których realizacja praw i obowiązków wynikających z przepisów prawa staje się utrudniona lub niemożliwa. W tym ujęciu cyberbezpieczeństwo stanowi warunek faktyczny skuteczności obowiązujących norm prawnych. Z perspektywy interesu publicznego cyberbezpieczeństwo pełni funkcję ochronną wobec wartości o fundamentalnym znaczeniu, takich jak bezpieczeństwo państwa, porządek publiczny czy ochrona praw obywateli.

Ustawodawca krajowy, wprowadzając regulacje dotyczące krajowego systemu cyberbezpieczeństwa, wskazuje wprost na konieczność zapewnienia nieprzerwanego i bezpiecznego świadczenia usług kluczowych oraz cyfrowych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 1 ust. 1, art. 3). Oznacza to, że cyberbezpieczeństwo nie jest wyłącznie interesem indywidualnym podmiotów eksploatujących systemy informacyjne, lecz stanowi dobro o charakterze publicznym. Również prawo

Unii Europejskiej traktuje cyberbezpieczeństwo jako element wspólnego interesu państw członkowskich. Celem regulacji unijnych jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, co uzasadnione jest transgranicznym charakterem zagrożeń występujących w cyberprzestrzeni (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, motyw 1, art. 1). Ataki cybernetyczne rzadko ograniczają się do terytorium jednego państwa, a ich skutki mogą oddziaływać na funkcjonowanie rynku wewnętrznego oraz bezpieczeństwo obywateli Unii (Chałubińska-Jentkiewicz, 2022, s. 24-25). Uznanie cyberbezpieczeństwa za element interesu publicznego uzasadnia ingerencję ustawodawcy w sferę działalności podmiotów publicznych i prywatnych poprzez nałożenie na nie określonych obowiązków. Obowiązki te mają charakter prewencyjny i służą ograniczeniu ryzyka wystąpienia incydentów, a jednocześnie stanowią podstawę do przypisania odpowiedzialności prawnej w przypadku ich naruszenia. W konsekwencji cyberbezpieczeństwo funkcjonuje w porządku prawnym jako wartość chroniona, której naruszenie może prowadzić do negatywnych konsekwencji nie tylko dla danego podmiotu, lecz także dla szeroko rozumianego interesu publicznego.

Ujęcie cyberbezpieczeństwa jako elementu bezpieczeństwa prawnego oraz interesu publicznego prowadzi do konieczności jego normatywnego zabezpieczenia poprzez nałożenie na określone podmioty konkretnych obowiązków prawnych. Obowiązki te nie mają charakteru wyłącznie deklaratywnego, lecz stanowią normatywnie określone powinności, których realizacja podlega ocenie z punktu widzenia legalności zachowania adresatów norm prawnych. Na gruncie prawa krajowego podstawowym aktem regulującym obowiązki w zakresie cyberbezpieczeństwa jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustawodawca wskazuje w niej kategorie podmiotów zobowiązanych do zapewnienia bezpieczeństwa systemów informacyjnych, w szczególności operatorów usług kluczowych oraz dostawców usług cyfrowych. Nałożone na te podmioty obowiązki obejmują m.in. podejmowanie działań zapobiegających incydentom, zapewnienie zdolności do wykrywania zagrożeń oraz reagowania na naruszenia cyberbezpieczeństwa (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 8 ust. 1-3, art. 11) (Chronowska-Sioła, 2025, s. 18-19) (Szpor, 2019, s. 42-45). Charakterystyczną cechą obowiązków w zakresie cyberbezpieczeństwa jest ich prewencyjny charakter. Prawo

nie ogranicza się bowiem do reakcji na skutki incydentów, lecz zobowiązuje podmioty do podejmowania działań z wyprzedzeniem, w szczególności poprzez zarządzanie ryzykiem związanym z funkcjonowaniem systemów informacyjnych. Oznacza to, że odpowiedzialność prawna może powstać również w sytuacji, gdy do naruszenia doszło na skutek niewystarczających działań zapobiegawczych, a nie bezpośredniego naruszenia przepisów o charakterze technicznym. Podobne podejście przyjęto w prawie Unii Europejskiej. Dyrektywa NIS 2 rozszerza krąg podmiotów objętych regulacją oraz wzmacnia obowiązki związane z zarządzaniem cyberbezpieczeństwem, kładąc nacisk na odpowiedzialność organizacyjną i systemową. Regulacja ta zakłada, że zapewnienie cyberbezpieczeństwa stanowi element należytej staranności podmiotów objętych jej zakresem, a niedopełnienie wynikających z niej obowiązków może prowadzić do zastosowania środków nadzorczych oraz sankcji (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 20-23). Istotne znaczenie ma również fakt, że obowiązki w zakresie cyberbezpieczeństwa mają charakter ciągły. Nie ograniczają się one do jednorazowego wdrożenia określonych rozwiązań, lecz wymagają stałego monitorowania zagrożeń, aktualizacji środków ochrony oraz dostosowywania procedur do zmieniającego się środowiska teleinformatycznego. W konsekwencji naruszenie cyberbezpieczeństwa może wynikać zarówno z braku reakcji na incydent, jak i z zaniechania aktualizacji lub utrzymania odpowiedniego poziomu zabezpieczeń. Ukształtowanie cyberbezpieczeństwa jako przedmiotu obowiązków prawnych stanowi podstawę do dalszej analizy odpowiedzialności prawnej podmiotów. Skoro bowiem ustawodawca nakłada na określone podmioty konkretne powinności, to ich niewykonanie lub nienależyte wykonanie otwiera drogę do przypisania odpowiedzialności, niezależnie od tego, czy naruszenie miało charakter zawiniony. Tym samym cyberbezpieczeństwo funkcjonuje w porządku prawnym jako obszar normatywnie zorganizowany, w którym obowiązki i odpowiedzialność pozostają ze sobą w ścisłym związku.

Naruszenie cyberbezpieczeństwa jako zdarzenie prawnie relewantne

Analiza odpowiedzialności prawnej podmiotów za naruszenia cyberbezpieczeństwa wymaga w pierwszej kolejności ustalenia, czym w sensie

normatywnym jest samo naruszenie cyberbezpieczeństwa. Pojęcie to nie ma charakteru potocznego ani technicznego, lecz zostało ukształtowane przez przepisy prawa, które nadają mu określone znaczenie prawne i wiążą z nim konkretne konsekwencje normatywne. Na gruncie prawa krajowego kluczowe znaczenie ma definicja incydentu zawarta w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zgodnie z art. 2 pkt 5 tej ustawy incydent oznacza zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Definicja ta ma charakter szeroki i obejmuje zarówno zdarzenia, które już spowodowały zakłócenia w funkcjonowaniu systemów informacyjnych, jak i takie, które potencjalnie mogą do nich doprowadzić (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 5) (Skoczylas, 2025, s. 233-234). Powyższe ujęcie wskazuje, że naruszenie cyberbezpieczeństwa nie jest ograniczone wyłącznie do sytuacji wystąpienia realnej szkody. Już samo wystąpienie zdarzenia stwarzającego zagrożenie dla poufności, integralności, dostępności lub autentyczności danych bądź usług może zostać zakwalifikowane jako incydent w rozumieniu przepisów prawa. Tym samym ustawodawca przyjmuje prewencyjny model ochrony cyberbezpieczeństwa, w którym znaczenie prawne mają również zdarzenia o charakterze potencjalnym. Prawo unijne posługuje się zbliżoną konstrukcją pojęciową. Dyrektywa NIS 2 definiuje incydent jako zdarzenie zagrażające dostępności, autentyczności, integralności lub poufności przechowywanych, przesyłanych lub przetwarzanych danych albo usług oferowanych przez sieci i systemy informatyczne. Regulacja ta kładzie nacisk na skutki zdarzenia dla funkcjonowania usług oraz na jego wpływ na bezpieczeństwo systemów informacyjnych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 6 pkt 6). Istotnym elementem normatywnego rozumienia naruszenia cyberbezpieczeństwa jest jego oderwanie od winy podmiotu zobowiązanego. Przepisy prawa nie uzależniają kwalifikacji danego zdarzenia jako naruszenia od zawinionego działania lub zaniechania. Oznacza to, że naruszenie cyberbezpieczeństwa może wystąpić również w sytuacji, gdy podmiot dochował należytej staranności, lecz mimo to doszło do incydentu. Kwestia winy nabiera znaczenia dopiero na etapie oceny odpowiedzialności prawnej. Naruszenie cyberbezpieczeństwa pełni zatem w porządku prawnym funkcję zdarzenia prawnie relewantnego, które uruchamia określone obowiązki po stronie podmiotów zobowiązanych, w szczególności obowiązki zgłoszeniowe, informacyjne oraz

naprawcze. Jednocześnie stanowi ono punkt wyjścia do oceny, czy doszło do naruszenia obowiązków prawnych w zakresie zapewnienia cyberbezpieczeństwa, a w konsekwencji – do przypisania odpowiedzialności prawnej.

Naruszenia cyberbezpieczeństwa nie stanowią jednorodnej kategorii zdarzeń. Obowiązujące regulacje prawne różnicują je ze względu na skalę, skutki oraz znaczenie dla funkcjonowania systemów informacyjnych i świadczonych usług. Zróżnicowanie to ma istotne znaczenie prawne, ponieważ determinuje zakres obowiązków podmiotów zobowiązanych oraz możliwe konsekwencje prawne związane z wystąpieniem danego naruszenia. Na gruncie prawa krajowego ustawodawca posługuje się kategorią incydentów, wprowadzając jednocześnie ich gradację. Ustawa o krajowym systemie cyberbezpieczeństwa wyróżnia m.in. incydenty poważne oraz incydenty krytyczne, których wystąpienie wiąże się ze zwiększonym poziomem zagrożenia dla ciągłości działania usług kluczowych lub systemów informacyjnych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 6-8, art. 12). Kryteria kwalifikacji danego zdarzenia do określonej kategorii incydentów obejmują w szczególności liczbę użytkowników dotkniętych skutkami zdarzenia, czas trwania zakłócenia oraz jego wpływ na bezpieczeństwo publiczne lub porządek publiczny. Powyższa klasyfikacja pełni funkcję normatywną, a nie wyłącznie opisową. Zakwalifikowanie naruszenia jako incydentu o określonym charakterze rodzi po stronie podmiotów zobowiązanych konkretne obowiązki prawne, w tym obowiązki niezwłocznego zgłoszenia zdarzenia właściwym organom oraz podjęcia działań zmierzających do ograniczenia jego skutków. Im wyższy stopień zagrożenia związany z naruszeniem cyberbezpieczeństwa, tym szerszy zakres ingerencji organów publicznych oraz intensywniejsze środki nadzorcze. Również prawo Unii Europejskiej przyjmuje zróżnicowane podejście do naruszeń cyberbezpieczeństwa. Dyrektywa NIS 2 posługuje się pojęciem incydentu znaczącego, którego kwalifikacja uzależniona jest od wpływu zdarzenia na świadczenie usług, zakresu oddziaływania oraz potencjalnych skutków transgranicznych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 6 pkt 7, art. 23). Ujęcie to podkreśla funkcjonalny charakter naruszeń cyberbezpieczeństwa, koncentrując się nie tyle na przyczynie zdarzenia, ile na jego skutkach dla systemów i użytkowników. Znaczenie prawne rozróżnienia poszczególnych rodzajów naruszeń cyberbezpieczeństwa polega również na tym, że wpływa ono na zakres

odpowiedzialności prawnej podmiotów. Nie każde naruszenie prowadzi automatycznie do zastosowania sankcji, jednak każde może stanowić podstawę do oceny czy podmiot wywiązał się z nałożonych na niego obowiązków w zakresie zapewnienia cyberbezpieczeństwa. W przypadku incydentów o większej wadze ustawodawca przewiduje dalej idące konsekwencje, w tym możliwość nałożenia kar administracyjnych lub zastosowania środków nadzorczych. W konsekwencji rodzaje naruszeń cyberbezpieczeństwa należy postrzegać jako element systemu oceny prawnej zachowania podmiotów zobowiązanych. Klasyfikacja ta pozwala na proporcjonalne reagowanie na zagrożenia, z jednej strony zapewniając ochronę interesu publicznego, z drugiej zaś uwzględniając stopień ryzyka oraz faktyczne skutki danego zdarzenia. Stanowi to istotne ogniwo łączące pojęcie naruszenia cyberbezpieczeństwa z mechanizmami odpowiedzialności prawnej.

Wystąpienie naruszenia cyberbezpieczeństwa nie pozostaje bez znaczenia w sferze prawnej. Przepisy prawa wiążą z takim zdarzeniem określone skutki normatywne, które aktualizują się niezależnie od dalszej oceny odpowiedzialności podmiotu zobowiązanego. Naruszenie cyberbezpieczeństwa stanowi bowiem zdarzenie prawnie relewantne, uruchamiające po stronie podmiotów objętych regulacją szereg obowiązków o charakterze publicznoprawnym. Na gruncie prawa krajowego podstawowym skutkiem prawnym naruszenia cyberbezpieczeństwa jest powstanie obowiązku podjęcia działań zmierzających do obsługi incydentu. Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na podmioty zobowiązane obowiązek niezwłocznego wykrywania, rejestrowania oraz obsługi incydentów, w tym podejmowania działań naprawczych i zapobiegawczych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 8 ust. 1 pkt 1-3, art. 11 ust. 1). Obowiązki te mają charakter bezwzględny i aktualizują się z chwilą wystąpienia zdarzenia spełniającego ustawowe kryteria incydentu. Kolejnym istotnym skutkiem prawnym naruszenia cyberbezpieczeństwa jest obowiązek zgłoszeniowy. W przypadku incydentów o określonym stopniu istotności podmioty zobowiązane są do przekazania informacji właściwym organom, w szczególności zespołom reagowania na incydenty bezpieczeństwa komputerowego. Celem tego obowiązku jest umożliwienie koordynacji działań na poziomie krajowym oraz ograniczenie potencjalnych skutków naruszenia dla innych podmiotów i użytkowników systemów informacyjnych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie

cyberbezpieczeństwa, 2018, art. 12 ust. 1-3). Naruszenie cyberbezpieczeństwa może również prowadzić do intensyfikacji nadzoru ze strony organów publicznych. W sytuacjach uzasadnionych charakterem lub skalą incydentu organy właściwe mogą podejmować działania kontrolne, wydawać zalecenia lub polecenia dotyczące sposobu usunięcia skutków naruszenia oraz zapobiegania jego powtórzeniu. Działania te mają charakter prewencyjno-naprawczy i nie stanowią jeszcze sankcji w ścisłym znaczeniu tego słowa. Warto podkreślić, że skutki prawne naruszenia cyberbezpieczeństwa mają charakter autonomiczny względem odpowiedzialności prawnej. Oznacza to, że samo wystąpienie naruszenia rodzi określone obowiązki, niezależnie od tego, czy w dalszym etapie zostanie stwierdzone naruszenie przepisów skutkujące nałożeniem sankcji. Innymi słowy, obowiązki reakcyjne i zgłoszeniowe pełnią funkcję zabezpieczającą interes publiczny, a nie represyjną. Analogiczne rozwiązania przyjęto na poziomie prawa Unii Europejskiej. Dyrektywa NIS 2 przewiduje obowiązki zgłaszania incydentów w określonych terminach oraz obowiązek przekazywania informacji umożliwiających ocenę skutków naruszenia dla świadczenia usług (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 23). Regulacja ta wzmacnia znaczenie reakcji na incydent jako elementu systemu cyberbezpieczeństwa, traktując naruszenie nie tylko jako problem podmiotu, którego dotyczy, lecz jako potencjalne zagrożenie o szerszym oddziaływaniu. Skutki prawne naruszenia cyberbezpieczeństwa stanowią zatem istotne ogniwo pomiędzy samym zdarzeniem a oceną odpowiedzialności prawnej podmiotu. To właśnie na tym etapie możliwe jest ustalenie czy podmiot dochował obowiązków w zakresie reagowania na incydent, co w dalszej kolejności może mieć decydujące znaczenie dla przypisania odpowiedzialności administracyjnej, cywilnej lub innej formy odpowiedzialności prawnej.

Formy odpowiedzialności prawnej za naruszenia cyberbezpieczeństwa

Odpowiedzialność administracyjnoprawna stanowi podstawowy i najczęściej stosowany mechanizm reakcji państwa na naruszenia cyberbezpieczeństwa. Jej celem nie jest represja sensu stricto, lecz zapewnienie skutecznego wykonywania obowiązków nałożonych na podmioty zobowiązane oraz ochrona interesu publicznego poprzez zapobieganie dalszym naruszeniom.

Odpowiedzialność ta realizowana jest w ramach stosunków administracyjnoprawnych, z udziałem organów właściwych do spraw cyberbezpieczeństwa. Na gruncie prawa krajowego odpowiedzialność administracyjnoprawna za naruszenia cyberbezpieczeństwa została ukształtowana przede wszystkim w ustawie o krajowym systemie cyberbezpieczeństwa. Ustawa ta przewiduje możliwość nałożenia na podmioty zobowiązane administracyjnych kar pieniężnych w przypadku niewykonania lub nienależytego wykonania obowiązków określonych w jej przepisach (Cătană, 2025, s. 37-39). Sankcje te mają charakter publicznoprawny i są nakładane w drodze decyzji administracyjnej przez właściwy organ (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 73-75). Charakterystyczną cechą odpowiedzialności administracyjnoprawnej w obszarze cyberbezpieczeństwa jest jej w znacznym stopniu obiektywny charakter. Ustawodawca nie uzależnia możliwości nałożenia kary administracyjnej wyłącznie od wykazania winy podmiotu, lecz od stwierdzenia naruszenia obowiązków ustawowych. Oznacza to, że kluczowe znaczenie ma ocena zgodności zachowania podmiotu z nałożonymi na niego obowiązkami, a nie subiektywne nastawienie czy intencja działania. W ramach odpowiedzialności administracyjnoprawnej istotną rolę odgrywa zasada proporcjonalności (Cătană, 2025, s. 45-47).

Organ nakładający karę powinien uwzględnić charakter, wagę i czas trwania naruszenia, a także jego skutki dla bezpieczeństwa systemów informacyjnych i interesu publicznego. Ustawa przewiduje możliwość miarkowania wysokości kary administracyjnej, co pozwala na dostosowanie reakcji organu do stopnia zagrożenia wywołanego naruszeniem cyberbezpieczeństwa (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 76). Odpowiedzialność administracyjnoprawna może być również poprzedzona lub uzupełniona środkami o charakterze nadzorczym. Organy właściwe są uprawnione do wydawania zaleceń, żądania usunięcia stwierdzonych nieprawidłowości oraz podejmowania innych działań zmierzających do przywrócenia zgodności z prawem. Dopiero w przypadku braku realizacji tych obowiązków lub poważnego naruszenia przepisów możliwe jest sięgnięcie po sankcje finansowe. Podobne rozwiązania zostały przyjęte na poziomie prawa Unii Europejskiej. Dyrektywa NIS 2 przewiduje obowiązek ustanowienia przez państwa członkowskie skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych za naruszenia

obowiązków w zakresie cyberbezpieczeństwa. Regulacja ta wzmacnia rolę odpowiedzialności administracyjnoprawnej jako podstawowego instrumentu egzekwowania norm dotyczących bezpieczeństwa sieci i systemów informatycznych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 34). W konsekwencji odpowiedzialność administracyjnoprawna pełni kluczową funkcję w systemie ochrony cyberbezpieczeństwa. Stanowi ona mechanizm zapewniający realną skuteczność norm prawnych poprzez możliwość zastosowania bezpośrednich środków władczych wobec podmiotów naruszających obowiązki ustawowe. Jednocześnie jej prewencyjny charakter sprawia, że ma ona na celu nie tylko reagowanie na naruszenia, lecz także zapobieganie ich występowaniu w przyszłości.

Obok odpowiedzialności administracyjnoprawnej naruszenia cyberbezpieczeństwa mogą rodzić również odpowiedzialność cywilnoprawną. Ma ona odmienny charakter i funkcję, gdyż jej celem jest przede wszystkim ochrona interesów prywatnych podmiotów, które poniosły szkodę w wyniku naruszenia, a także kompensacja doznanych strat. Odpowiedzialność cywilnoprawna realizowana jest w ramach stosunków prawa prywatnego i co do zasady dochodzona jest przed sądem powszechnym. Podstawą odpowiedzialności cywilnoprawnej za naruszenia cyberbezpieczeństwa są ogólne przepisy prawa cywilnego dotyczące odpowiedzialności odszkodowawczej. W zależności od okoliczności sprawy może ona przybrać postać odpowiedzialności deliktowej albo kontraktowej. W pierwszym przypadku naruszenie cyberbezpieczeństwa stanowi czyn niedozwolony, w wyniku którego poszkodowany doznał szkody. W drugim – naruszenie obowiązków związanych z zapewnieniem cyberbezpieczeństwa może być traktowane jako nienależyte wykonanie zobowiązania umownego. Charakterystyczną cechą odpowiedzialności cywilnoprawnej w omawianym obszarze jest konieczność wykazania przesłanek odpowiedzialności, w szczególności powstania szkody, bezprawności zachowania, związku przyczynowego oraz – co do zasady – winy podmiotu odpowiedzialnego. Naruszenie cyberbezpieczeństwa samo w sobie nie przesądza jeszcze o odpowiedzialności cywilnej, lecz może stanowić zdarzenie wywołujące szkodę lub zwiększające ryzyko jej wystąpienia. Szkody wynikające z naruszeń cyberbezpieczeństwa mogą mieć zarówno charakter majątkowy, jak i niemajątkowy. Do szkód majątkowych zaliczyć można m.in. straty finansowe spowodowane przerwą w działalności, utratą danych lub koniecznością przywrócenia systemów informatycznych

do prawidłowego funkcjonowania. Szkody niemajątkowe mogą natomiast dotyczyć naruszenia dóbr osobistych, takich jak prywatność czy dobre imię, zwłaszcza w sytuacjach związanych z nieuprawnionym ujawnieniem informacji. Istotnym zagadnieniem w kontekście odpowiedzialności cywilnoprawnej jest relacja pomiędzy obowiązkami publicznoprawnymi a standardem należytej staranności wymaganym w stosunkach prywatnoprawnych. Obowiązki nałożone na podmioty w przepisach dotyczących cyberbezpieczeństwa mogą pełnić funkcję punktu odniesienia przy ocenie, czy dany podmiot dochował należytej staranności. Ich naruszenie może zatem pośrednio wpływać na ocenę bezprawności lub winy w postępowaniu cywilnym. Odpowiedzialność cywilnoprawna za naruszenia cyberbezpieczeństwa pełni funkcję uzupełniającą wobec odpowiedzialności administracyjnoprawnej. Podczas gdy sankcje administracyjne służą ochronie interesu publicznego, odpowiedzialność cywilna koncentruje się na naprawieniu szkody wyrządzonej konkretnemu podmiotowi. Obie formy odpowiedzialności mogą funkcjonować równolegle, gdyż realizują odmienne cele i oparte są na różnych podstawach prawnych.

Odpowiedzialność karna za naruszenia cyberbezpieczeństwa stanowi najbardziej represyjną formę reakcji prawnej na zachowania zagrażające bezpieczeństwu systemów informacyjnych. Jej zastosowanie ograniczone jest do przypadków, w których naruszenie cyberbezpieczeństwa przybiera postać czynu zabronionego określonego w przepisach prawa karnego. Z tego względu odpowiedzialność karna pełni w systemie ochrony cyberbezpieczeństwa funkcję subsydiarną wobec odpowiedzialności administracyjnoprawnej i cywilnoprawnej. Na gruncie prawa krajowego podstawowe typy czynów zabronionych związanych z naruszeniami cyberbezpieczeństwa zostały uregulowane w Kodeksie karnym. Przepisy te penalizują m.in. nieuprawnione uzyskanie dostępu do informacji, zakłócanie pracy systemów informatycznych, niszczenie lub modyfikowanie danych oraz ingerencję w funkcjonowanie sieci teleinformatycznych (Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, 1997, art. 267-269b). Odpowiedzialność karna w tym zakresie ma na celu ochronę poufności, integralności i dostępności informacji, a także stabilności systemów informacyjnych. Charakterystyczną cechą odpowiedzialności karnej jest jej ścisłe powiązanie z zasadą winy. Przypisanie odpowiedzialności karnej wymaga wykazania, że sprawca działał umyślnie albo – w przypadkach przewidzianych przez ustawę – nieumyślnie.

Sam fakt wystąpienia naruszenia cyberbezpieczeństwa nie przesądza zatem o odpowiedzialności karnej określonego podmiotu. Konieczne jest ustalenie, że zachowanie sprawcy wypełnia znamiona konkretnego typu czynu zabronionego. W kontekście odpowiedzialności karnej istotne znaczenie ma również rozróżnienie pomiędzy sprawcą bezpośredniego ataku a podmiotem zobowiązanym do zapewnienia cyberbezpieczeństwa. Odpowiedzialność karna dotyczy co do zasady osób fizycznych, które dopuściły się czynu zabronionego, a nie podmiotów jako takich. Tym samym brak zapewnienia odpowiedniego poziomu cyberbezpieczeństwa przez organizację nie prowadzi automatycznie do odpowiedzialności karnej, chyba że możliwe jest przypisanie konkretnej osobie fizycznej zachowania wypełniającego znamiona przestępstwa. Należy również podkreślić, że odpowiedzialność karna nie służy egzekwowaniu obowiązków o charakterze prewencyjnym. Jej funkcją jest reagowanie na najpoważniejsze naruszenia cyberbezpieczeństwa, które godzą w podstawowe dobra prawne, takie jak bezpieczeństwo informacji, porządek publiczny czy interesy majątkowe. Z tego względu prawo karne pełni rolę środka ostatecznego, stosowanego w sytuacjach, w których inne formy odpowiedzialności okazują się niewystarczające. W systemie ochrony cyberbezpieczeństwa odpowiedzialność karna stanowi zatem element uzupełniający, skoncentrowany na zwalczaniu najcięższych form naruszeń. Jej znaczenie polega przede wszystkim na funkcji odstraszającej oraz ochronie podstawowych wartości, podczas gdy zasadniczy ciężar zapewnienia cyberbezpieczeństwa oraz reagowania na incydenty spoczywa na instrumentach administracyjnoprawnych i organizacyjnych.

Podsumowanie

Przeprowadzona analiza prowadzi do wniosku, że cyberbezpieczeństwo stanowi obecnie istotny przedmiot regulacji prawnej, a jego naruszenie nie jest wyłącznie problemem technicznym, lecz zdarzeniem o doniosłych konsekwencjach normatywnych. Obowiązujące regulacje krajowe i unijne jednoznacznie nadają cyberbezpieczeństwu status dobra prawnie chronionego, którego ochrona służy zarówno interesom indywidualnym, jak i interesowi publicznemu. W opracowaniu wykazano, że naruszenie cyberbezpieczeństwa funkcjonuje w porządku prawnym jako zdarzenie prawnie relewantne, uruchamiające określone skutki prawne niezależnie od dalszej

oceny odpowiedzialności podmiotu zobowiązanego. Już samo wystąpienie incydentu aktualizuje obowiązki o charakterze reakcyjnym i informacyjnym, co potwierdza prewencyjny model ochrony przyjęty przez ustawodawcę. Model ten koncentruje się nie tylko na sankcjonowaniu naruszeń, lecz również na minimalizowaniu ich skutków oraz zapobieganiu eskalacji zagrożeń. Analiza form odpowiedzialności prawnej prowadzi do wniosku, że zasadniczą rolę w systemie ochrony cyberbezpieczeństwa odgrywa odpowiedzialność administracyjnoprawna. To ona stanowi podstawowy instrument egzekwowania obowiązków nałożonych na podmioty zobowiązane oraz zapewnienia skuteczności norm prawa cyberbezpieczeństwa.

Odpowiedzialność cywilnoprawna pełni natomiast funkcję kompensacyjną, chroniąc interesy podmiotów, które poniosły szkodę w wyniku naruszenia. Odpowiedzialność karna, ze względu na swój represyjny charakter i konieczność wykazania winy, ma znaczenie uzupełniające i znajduje zastosowanie jedynie w przypadku najpoważniejszych naruszeń. W świetle powyższych ustaleń należy stwierdzić, że odpowiedzialność prawna za naruszenia cyberbezpieczeństwa ma charakter wielopoziomowy i zróżnicowany, co pozwala na elastyczne i proporcjonalne reagowanie na zagrożenia występujące w cyberprzestrzeni. Jednocześnie takie ukształtowanie systemu odpowiedzialności wymaga od podmiotów objętych regulacją stałego monitorowania obowiązków prawnych oraz podejmowania działań wykraczających poza minimalne wymogi formalne. Z perspektywy de lege ferenda zasadne wydaje się dalsze doprecyzowywanie relacji pomiędzy obowiązkami publicznoprawnymi a standardem należytej staranności w prawie prywatnym, w szczególności w kontekście odpowiedzialności cywilnoprawnej. Ponadto istotnym kierunkiem rozwoju regulacji powinno być wzmacnianie mechanizmów prewencyjnych, w tym promowanie kultury zgodności z prawem cyberbezpieczeństwa oraz zwiększanie świadomości prawnej podmiotów zobowiązanych.

Podsumowując, cyberbezpieczeństwo należy postrzegać jako trwały i dynamiczny element współczesnego porządku prawnego. Skuteczność ochrony w tym obszarze zależy nie tylko od treści obowiązujących regulacji, lecz również od ich konsekwentnego egzekwowania oraz właściwego rozumienia odpowiedzialności prawnej jako instrumentu służącego ochronie zarówno interesu publicznego, jak i praw jednostki.

Literatura

1. Cătană, E. L. (2025). An administrative law approach of cybersecurity rules: The case of Romania in the context of EU and international law. *Studia Iuridica Lublinensia*, *34*(1), 37-47.
2. Chałubińska-Jentkiewicz, K. (2022). Cyberspace as an area of legal regulation. W: K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (red.), *Cybersecurity in Poland: Legal aspects* (s. 23-25). Springer.
3. Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, *53*, 1-10.
4. Chronowska-Sioła, E. (2025). Unijna dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych. *Cybersecurity and Law*, *2*(14), 15-19.
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS 2) (2022). *Dziennik Urzędowy Unii Europejskiej*, L 333, 1-137.
6. Ottis, R., Lorents, P. (2010). Cyberspace: Definition and implications. W: *Proceedings of the 5th International Conference on Information Warfare and Security* (s. 1-10). Academic Conferences Ltd.
7. Skoczylas, D. (2025). The NIS 2 Directive and the cybersecurity of public administrations. *Discourse of Law and Administration*, *1*, 231-234.
8. Szpor, G. (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wolters Kluwer.
9. Terebiński, B. (2018). Bezpieczeństwo teleinformatyczne jako podstawa funkcjonowania współczesnego państwa. *Obronność – Zeszyty Naukowe*, *1*(25), 216-218.
10. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (2018). *Dziennik Ustaw*, poz. 1560 ze zm.
11. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (1997). *Dziennik Ustaw*, nr 88, poz. 553 ze zm.

Barbara Drapikowska[1], Sylwia Borawska[2]
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103359_14

ODPORNOŚĆ INFORMACYJNA POKOLENIA Z – CZYNNIKI KSZTAŁTUJĄCE ŚWIADOMOŚĆ I PODATNOŚĆ NA DEZINFORMACJĘ W ERZE CYFROWEJ

GENERATION Z INFORMATION RESILIENCE – FACTORS SHAPING AWARENESS AND SUSCEPTIBILITY TO MISINFORMATION IN THE DIGITAL AGE

Streszczenie

Niniejszy rozdział ma charakter teoretyczno-empiryczny, a jego celem jest określenie poziomu odporności informacyjnej pokolenia Z w kontekście współczesnych zagrożeń dezinformacyjnych. Główny problem badawczy sformułowano w postaci pytania: jaki poziom odporności informacyjnej prezentują przedstawiciele pokolenia Z? W części teoretycznej przedstawiono istotę odporności informacyjnej jako kategorii badawczej oraz scharakteryzowano pokolenie Z jako aktywnych

[1] https://orcid.org/0000-0002-6852-2791, e-mail: b.drapikowska@akademia.mil.pl
[2] https://orcid.org/0009-0006-6851-9492, e-mail: borawska.sylwia@o2.pl

i intensywnych uczestników środowiska cyfrowego. Natomiast część empiryczna prezentuje wyniki badań własnych przeprowadzonych wśród studentów pokolenia Z, obejmujących analizę świadomości dezinformacji, praktyk weryfikacyjnych oraz emocjonalnych reakcji na manipulacje informacyjne. W badaniu empirycznym zastosowano metodę sondażu diagnostycznego realizowanego techniką ankiety, prowadzonej na przełomie 2024 i 2025 roku, w którym udział wzięli studenci z Polski, Ukrainy oraz programu Erasmus. Uzyskane wyniki pozwoliły na dokonanie porównań między grupami oraz ocenę odporności informacyjnej młodych odbiorców informacji w kontekście ich doświadczeń społeczno-kulturowych.

Słowa kluczowe: odporność informacyjna, pokolenie Z, dezinformacja, bezpieczeństwo informacyjne

Abstract

This chapter has a theoretical and empirical character and aims to determine the level of information resilience of Generation Z in the context of contemporary disinformation threats. The main research problem was formulated in the form of the following question: what level of information resilience is presented by representatives of Generation Z? The theoretical part presents the essence of information resilience as a research category and characterizes Generation Z as active and intensive participants in the digital environment. The empirical part, in turn, presents the results of the authors' own research conducted among Generation Z students, including an analysis of their awareness of disinformation, verification practices, and emotional reactions to information manipulation. The empirical study employed the diagnostic survey method using a questionnaire technique conducted at the turn of 2024 and 2025. The study involved students from Poland, Ukraine, and participants of the Erasmus programme. The obtained results made it possible to compare the groups and assess the level of information resilience among young information recipients in the context of their socio-cultural experiences.

Keywords: information resilience, Generation Z, disinformation, information security

Wstęp

Współczesna przestrzeń komunikacyjna rozwija się w warunkach silnego nasycenia informacją oraz dynamicznych zmian technologicznych. Towarzyszy temu wzrost zjawiska dezinformacji, które prowadzi do

zaburzenia procesów poznawczych i społecznych odbiorców, szczególnie młodych użytkowników cyberprzestrzeni (Pennycook, Rand, 2021).

W Polsce problem dezinformacji przybrał w ostatnich latach wymiar masowy. W badaniach przeprowadzonych w 2021 roku aż 86% respondentów deklarowało, że zdarzyło im się zetknąć z treścią, którą uznali za fałszywą lub wątpliwą. Obszary najczęściej dotknięte dezinformacją to klimat i energetyka oraz zdrowie (Chałubińska-Jentkiewicz, Soler, Makuch, 2023), co sugeruje, że ekspozycja na to zjawisko często dotyczy sfer kluczowych z punktu widzenia debaty publicznej i bezpieczeństwa informacyjnego.

Według raportu *Dezinformacja oczami Polaków. Edycja 2024* aż 84% dorosłych deklaruje, że zetknęło się z fake newsem, a znaczący odsetek przyznaje, że uwierzył przynajmniej w jedną fałszywą informację (Laboratorium Badań Mediów UW & Fundacja Digital Poland, 2024). Jednocześnie analizy środowisk eksperckich, takich jak *Disinformation Landscape in Poland* pokazują, że dezinformacja rozprzestrzenia się poprzez złożone sieci narracji, wykorzystując media społecznościowe, kanały alternatywne oraz emocjonalizację przekazów. To oznacza, że przestała być ona wyłącznie problemem pojedynczych treści, a stała się zjawiskiem systemowym, groźnym dla spójności informacyjnej i funkcjonowania debaty publicznej. Wobec tego rośnie znaczenie odporności informacyjnej, zarówno na poziomie jednostki, jak i całego społeczeństwa (Zadroga, 2023).

Jedną z grup szczególnie narażonych na oddziaływanie dezinformacji są ludzi młodzi, intensywnie korzystający z Internetu i mediów społecznościowych, tj. pokolenie Z, które traktuje przestrzeń cyfrową jako naturalne środowisko życia społecznego i informacyjnego. Badania wskazują, że młodzi użytkownicy Internetu, znacznie częściej niż starsze pokolenia, polegają na treściach pochodzących z platform społecznościowych, co zwiększa ekspozycję na treści nierzetelne, zmanipulowane lub całkowicie fałszywe (Cywiński, 2024). Jednocześnie mimo bardzo wysokich deklaratywnych umiejętności technologicznych, osoby z pokolenia Z nierzadko cechuje zbyt duża pewność siebie w ocenie wiarygodności informacji, co sprzyja pochopnemu udostępnianiu niezweryfikowanych treści (LBM UW & FDP, 2024). To sprawia, że ocena poziomu odporności informacyjnej młodych osób, a zwłaszcza studentów jako aktywnych uczestników cyfrowego ekosystemu, staje się kluczowa dla zrozumienia dynamiki zagrożeń w polskiej infosferze. Niniejszy rozdział jest próbą podjęcia tego zagadnienia.

Główny problem badawczy został skonstruowany w postaci pytania: jaki poziom odporności informacyjnej prezentują przedstawiciele pokolenia Z? Na tej podstawie skonstruowano problematykę szczegółową obejmującą następujące kwestie:

1. Jak definiuje się odporność informacyjną w ujęciu aktualnych badań i strategii europejskich?
2. Jakie cechy i kompetencje charakteryzują pokolenie Z jako odbiorców informacji w środowisku cyfrowym?
3. Jak przedstawiają się wyniki badań dotyczące odporności informacyjnej pokolenia Z w zakresie świadomości dezinformacji, praktyk weryfikacji informacji oraz emocjonalnego odbioru manipulacji informacyjnych?

W kolejnych częściach rozdziału podjęto próbę rozwiązania przyjętych problemów badawczych poprzez analizę teoretyczną oraz prezentację wyników badań własnych.

Odporność informacyjna jako mechanizm ochrony przed dezinformacją

W raporcie Organizacji Współpracy i Rozwoju w Europie (OECD, 2024) podkreślono, że dezinformacja zagraża funkcjonowaniu demokracji i procesów obywatelskich, a odporność informacyjna jest środkiem ochrony integralności debaty publicznej. Równocześnie, z perspektywy Unii Europejskiej (UE, 2021), odporność informacyjna stanowi element ochrony procesów demokratycznych i stabilności społecznej, co realizowane jest m.in. poprzez wzmacnianie świadomego udziału obywateli w sferze informacyjnej, zwiększanie transparentności platform cyfrowych oraz przeciwdziałanie dezinformacji.

W opinii UE (2021) fundamentalnym filarem skutecznej walki z dezinformacją jest wzmocnienie pozycji obywateli jako aktywnych uczestników infosfery, co zakłada nie tylko regulacje dla platform internetowych, ale też budowanie ich świadomości i umiejętności krytycznej analizy informacji. Przewiduje się, że programy edukacyjne, transparentność treści oraz narzędzia ułatwiające weryfikację będą kluczowe, by użytkownicy mogli samodzielnie rozpoznawać treści fałszywe lub manipulacyjne, oceniać

wiarygodność źródeł i podejmować świadome decyzje informacyjne. W ten sposób odporność informacyjna przestaje być jedynie zadaniem instytucji, a staje się zintegrowaną strategią uczestnictwa obywatelskiego w demokracji.

Z kolei w myśl polityki Komisji Europejskiej, odporność informacyjna jest integralnym elementem szeroko rozumianego systemu ochrony przed zagrożeniami hybrydowymi oraz kryzysami informacyjnymi, obejmującymi dezinformację, manipulacje online i obce ingerencje informacyjne. W ramach tej strategii UE podejmuje działania regulacyjne (np. systemy odpowiedzialności platform internetowych), promuje przejrzystość reklam politycznych oraz wspiera inicjatywy edukacyjne i budujące kompetencje cyfrowe i medialne obywateli (Komisja Europejska, 2025a). Jednocześnie wspiera pluralizm mediów i wolność dziennikarską, uznając, że dostęp do rzetelnych i różnorodnych źródeł jest fundamentem odporności społecznej (Komisja Europejska, 2025b). W ten sposób odporność informacyjna staje się nie tylko kwestią indywidualnej wiedzy czy krytycyzmu, lecz elementem kolektywnej odporności demokratycznych społeczeństw na działania dezinformacyjne.

W literaturze naukowej odporność informacyjna (ang. *information resilience*) jest postrzegana jako koncepcja obejmująca zdolność jednostek oraz społeczeństw do funkcjonowania i adaptacji w obliczu zaburzeń informacyjnych, takich jak dezinformacja czy przeciążenie informacyjne. Zakłada ona zarówno trwałość i dostępność informacji, jak i kompetencje użytkowników w zakresie jej selekcji, oceny oraz wykorzystania w procesach decyzyjnych. Tym samym łączy wymiar techniczny, czyli zapewnienie ciągłości i jakości zasobów informacyjnych, z wymiarem społecznym i poznawczym, odnoszącym się do krytycznej analizy, interpretacji i neutralizowania treści fałszywych (Ferraz, Helal, 2024).

Co więcej, badacze problemu również podkreślają, że odporność informacyjna obejmuje wielowymiarowy zestaw zdolności, zarówno na poziomie indywidualnym, instytucjonalnym, jak i społecznym, które umożliwiają krytyczne rozpoznawanie i weryfikację informacji, budowanie kolektywnej odporności obywateli oraz tworzenie mechanizmów przeciwdziałania propagandzie i manipulacji. Można zatem przyjąć, że informacyjna odporność powinna być traktowana jako element bezpieczeństwa narodowego i społecznego, tj. umiejętność odróżniania prawdy od fałszu, świadomego korzystania z mediów, a także współpracy między państwem, instytucjami, mediami

i obywatelami. P. Uusikylä i inni (2024) postulują, by strategia odporności informacyjnej była integralną częścią polityki bezpieczeństwa i przygotowania na kryzysy, co jest szczególnie ważne w dobie intensywnych działań informacyjnych, cyberzagrożeń i operacji dezinformacyjnych.

W podobnym tonie swoje refleksje prezentują M. Dragomir i inni (2024), argumentując, że odporność informacyjna to wielowymiarowa cecha, która zależy zarówno od strukturalnych cech państwa (tj. systemy medialne, instytucje dystrybucji wiedzy, regulacje), jak i od działań i kompetencji obywateli (tj. wiedza, zaufanie do mediów i instytucji, nawyki informacyjne). Opierając badania na czterech europejskich krajach (tj. Austria, Czechy, Finlandia, Hiszpania), ukazano, że ogólnoeuropejskie strategie walki z dezinformacją nie zawsze zwiększają odporność na poziomie narodowym, a skuteczna polityka wymaga lokalnej, kontekstualnej diagnozy stanu odporności informacyjnej w danym kraju.

Również w obszarze polskich badań nad dezinformacją coraz częściej podnosi się, że skuteczne przeciwdziałanie manipulacji wymaga nie tylko doraźnych działań, ale też budowania systemowej odporności informacyjnej społeczeństwa. T. Gergelewicz (2022) wskazuje, że istotnym elementem tej odporności jest rozwijanie u obywateli kompetencji medialnych i informacyjnych, czyli umożliwiających weryfikowanie źródeł, selekcję treści oraz krytyczne ocenianie komunikatów, co pozwala m.in. „neutralizować skutki fałszywej narracji" i ograniczać wpływ dezinformacji. Ponadto Autor postuluje, że na poziomie instytucjonalnym konieczne są programy edukacyjne i kampanie społeczne, które ułatwią obywatelom poruszanie się w infosferze, charakteryzującej się nadmiarem informacji i rosnącym ryzykiem manipulacji, co czyni odporność informacyjną kluczowym aspektem zarówno bezpieczeństwa informacyjnego, jak i ochrony demokracji.

Z kolei K. Gorazdowski (2024) w swoich analizach wskazuje, że zjawisko fake newsów w Polsce przyjęło charakter instytucjonalny. Innymi słowy, dezinformacja stała się nie tylko problemem pojedynczych błędnych treści, lecz systemowym zagrożeniem dla społeczeństwa obywatelskiego i procesów decyzyjnych. Rozdział podkreśla, że mechanizmy dezinformacyjne wpływają na postawy obywateli, osłabiają zaufanie do mediów oraz instytucji, a także zniekształcają debatę publiczną, co w konsekwencji wymaga budowania społeczeństwa odporniejszego informacyjnie. Z tego powodu Autor postuluje potrzebę edukacji medialnej, zwiększenia

transparentności źródeł informacji i aktywnego kształtowania postaw krytycznych, jako kluczowych elementów strategii przeciwdziałania negatywnym skutkom dezinformacji.

Podsumowując ten wątek należy zaakcentować, że współcześnie coraz częściej podkreśla się znaczenie odporności informacyjnej jako zdolności jednostki oraz społeczeństwa do przeciwdziałania manipulacji oraz zachowania autonomii poznawczej i społecznej. Informacyjna odporność może być rozumiana jako umiejętność krytycznego przetwarzania informacji, odbudowy zaufania społecznego i adaptacji w warunkach zalewu dezinformacją.

Pokolenie Z jako kluczowi uczestnicy środowiska informacyjnego

W niniejszym opracowaniu przyjęto, że ramy czasowe pokolenia Z to lata 1995-2009 (Rogozińska-Pawelczyk, Cewińska, Lubrańska, Oleksiak, Striker, 2029). Reprezentanci urodzeni w tym czasie bardzo sprawnie komunikują się za pośrednictwem mediów społecznościowych oraz bez większych trudności przechodzą ze świata rzeczywistego do wirtualnego. Co więcej, uważają oni, że oba wymienione światy wzajemnie się uzupełniają. Dorastali w czasach, gdy dostęp do różnych informacji był łatwo osiągalny. Byli stymulowani przez rodziców, nauczycieli oraz wychowawców różnymi materiałami i pomocami wspierającymi ich rozwój, dzięki czemu wcześnie pozyskali wysoce cenione kompetencje. Osoby wywodzące się z pokolenia Z nie boją się ryzyka i szybko podejmują różnego rodzaju decyzje. Przedstawiciele pokolenia Z dorastali w okresie niskiej dynamiki zmian społecznych, która nie przyczyniła się do ukształtowania wyrazistości pokoleniowej. Nie pamiętają oni czasów, kiedy Polska nie należała do Unii Europejskiej czy Sojuszu Północnoatlantyckiego, dla tej grupy osób Polska do tych dwóch organizacji należy od zawsze (Rogozińska-Pawelczyk i in., 2019).

Pokolenie Z to pierwsza generacja wychowana w pełni w cyfrowym ekosystemie, z powszechnym dostępem do Internetu, smartfonów i mediów społecznościowych. To sprawia, że członkowie tej grupy funkcjonują w przestrzeni informacyjnej w sposób intensywny i ciągły, a media cyfrowe stanowią dla nich podstawowe źródło wiedzy o świecie (Cywiński, 2024). Wysoki poziom kompetencji technicznych nie zawsze przekłada się jednak na umiejętność krytycznej weryfikacji treści, co prowadzi do zjawiska „iluzji

kompetencji" (ang. *overconfidence*) – przekonania o własnej informacyjnej sprawczości przy jednoczesnej podatności na manipulację przekazem (Lyons, Montgomery, Nyhan, Reifler, 2021).

Badania wskazują, że młodzi użytkownicy Internetu częściej niż starsze pokolenia polegają na mediach społecznościowych jako głównym źródle informacji, co przyspiesza konsumpcję treści kosztem ich refleksyjnej oceny (Newman, Fletcher, Robertson, Eddy, Nielsen, 2024) Algorytmizacja przepływu informacji, wysoki poziom emocjonalizacji przekazów oraz łatwość nieświadomego udostępniania treści wzmacniają ryzyko ekspozycji na dezinformację i podważają trafność ocen poznawczych tej grupy (LBM UW & FDP, 2024). Pokolenie Z staje się więc z jednej strony najbardziej aktywną, angażującą się i wpływową grupą uczestników infosfery, a z drugiej – grupą szczególnie podatną na oddziaływanie treści fałszywych, co czyni badania nad ich odpornością informacyjną szczególnie istotnymi.

Z uwagi na fakt, że pokolenie Z jest określane jako pierwsza generacja w pełni ukształtowana w środowisku nasyconym technologią cyfrową, przekłada się to na wysoki poziom biegłości informatycznej oraz umiejętność wykonywania wielu aktywności jednocześnie – tzw. multitaskingu (Tapscott, 2010). Internet stanowi dla tej grupy podstawowe narzędzie rozwoju kompetencji, które w dużej mierze zastąpiło tradycyjne materiały drukowane (Sadowski, 2023). Młodzi użytkownicy preferują dostęp do wiedzy w formie mobilnej, np. za pomocą smartfona, tabletu lub laptopa, co sprzyja szybkiemu przyswajaniu informacji, ale także skraca czas refleksji nad treściami (Newman i in., 2024).

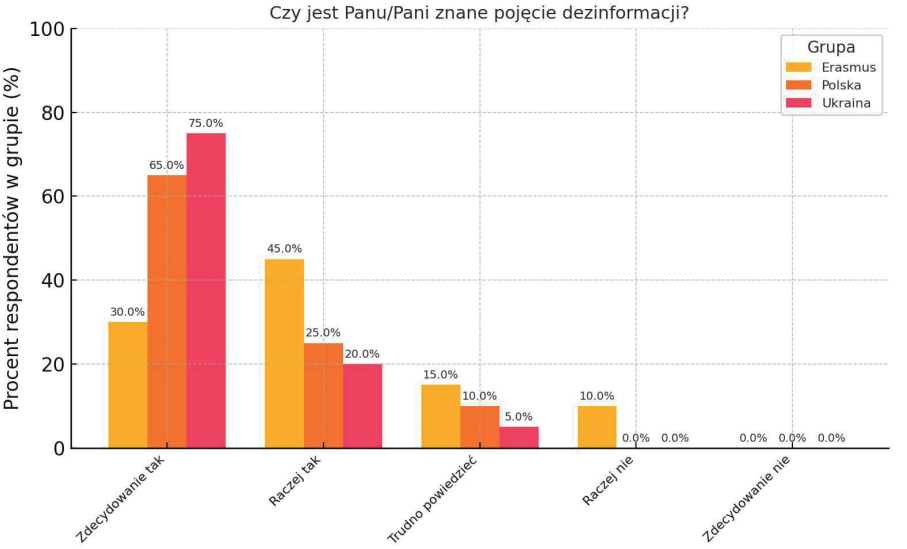
Przedstawiciele pokolenia Z chętnie uczestniczą w kursach online i szkoleniach zdalnych, traktując je jako naturalną formę zdobywania wykształcenia i rozwijania kwalifikacji zawodowych, które postrzegają jako kluczowe w przyszłych procesach rekrutacyjnych (Gajewska, 2021). Równocześnie intensywna obecność tej grupy w mediach społecznościowych prowadzi do budowania własnej tożsamości wirtualnej, nierzadko równie istotnej jak funkcjonowanie w świecie offline (Cywiński, 2024).

Odporność informacyjna pokolenia Z w świetle wyników badań

Świadomość zjawiska dezinformacji wśród respondentów

Badanie zostało przeprowadzone na przełomie 2024 i 2025 roku, w okresie wzmożonej aktywności dezinformacyjnej w Europie oraz rosnącego znaczenia mediów społecznościowych i narzędzi generatywnej sztucznej inteligencji jako źródeł informacji. Kontekst ten nadaje analizie szczególnego znaczenia, ponieważ pozwala ocenić odporność informacyjną młodych dorosłych w warunkach dynamicznych zmian krajobrazu informacyjnego.

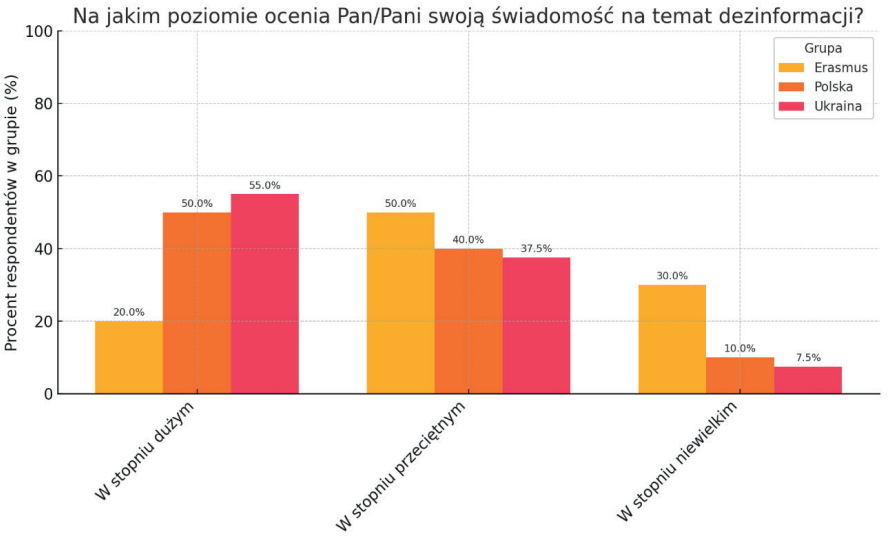
Wyniki badania wskazują, że świadomość zagrożeń dezinformacyjnych wśród reprezentantów pokolenia Z jest stosunkowo wysoka, jednak różnicuje się znacząco ze względu na narodowość respondentów. Studenci z Ukrainy wykazują najwyższy poziom wiedzy o dezinformacji – aż 75% z nich zadeklarowało, że „zdecydowanie" zna to pojęcie, a kolejne 20% wskazało odpowiedź „raczej tak". Wśród studentów z Polski znajomość zjawiska również jest duża (65% – „zdecydowanie tak", 25% – „raczej tak"). Natomiast studenci z programu Erasmus charakteryzują się wyraźnie niższym poziomem rozpoznania problemu – jedynie 30% z nich zadeklarowało pełną znajomość terminu, a 15% przyznaje, że trudno im określić swoją wiedzę w tym zakresie. Dane pozyskane w tym fragmencie badanej rzeczywistości zaprezentowane zostały na Rysunku 1.



Rysunek 1. Znajomość pojęcia dezinformacji wśród respondentów

Źródło: opracowanie własne.

Podobne różnice uwidaczniają się w samoocenie świadomości dezinformacji. Aż 55% studentów z Ukrainy oraz 50% studentów z Polski ocenia swoją wiedzę jako wysoką, podczas gdy wśród studentów Erasmus taką odpowiedź zaznaczyło jedynie 20%. Co więcej, aż 30% tej ostatniej grupy wskazało niski poziom świadomości, co może świadczyć o mniejszym poczuciu zagrożenia lub ograniczonej styczności z operacjami informacyjnymi wpływającymi bezpośrednio na bezpieczeństwo społeczne. Dokładne dane pozyskane w tym obszarze zaprezentowane zostały na Rysunku 2.



Rysunek 2. Poziom świadomości na temat dezinformacji wśród respondentów

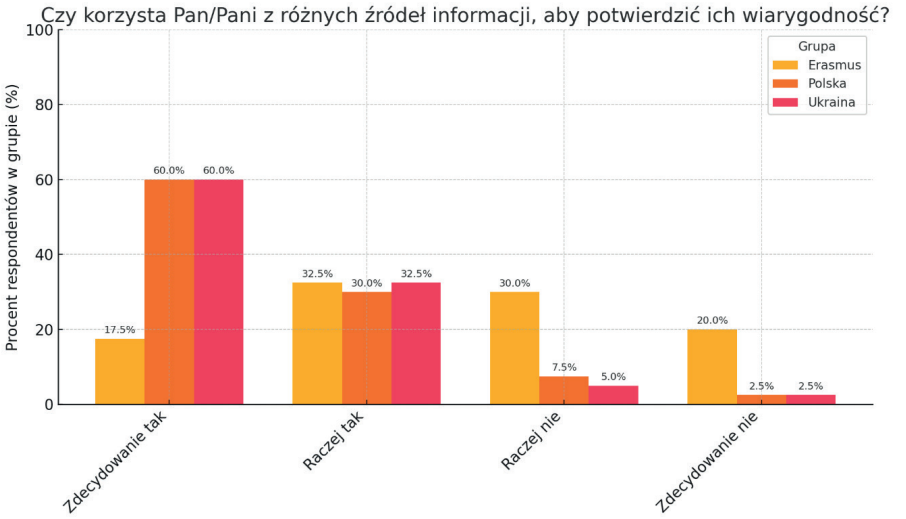
Źródło: opracowanie własne.

Wyniki te potwierdzają wcześniejsze ustalenia literaturowe wskazujące, że samo pojęcie dezinformacji jest znane młodym odbiorcom, ale jego rozumienie i ciężar znaczeniowy zależą od kontekstu geopolitycznego, w którym funkcjonują. W przypadku studentów z Ukrainy realne doświadczenie wojny informacyjnej wzmacnia czujność, motywację do rozpoznawania zagrożeń oraz świadomość wpływu manipulacji medialnych na bezpieczeństwo państwa i jednostki. Tymczasem u studentów z Polski świadomość ta ma częściej charakter abstrakcyjny, a u studentów zagranicznych z kolei fragmentaryczny i mniej ugruntowany.

Szczególnie istotne z perspektywy odporności informacyjnej jest to, że pomimo względnie wysokiej deklaratywnej wiedzy, u części badanych może występować zjawisko „iluzji kompetencji", rozumiane jako nadmierna pewność własnych umiejętności przy braku praktycznych nawyków weryfikacyjnych. Oznacza to, że świadomość dezinformacji nie zawsze idzie w parze z realną zdolnością do jej identyfikacji. Warto podkreślić, że sama znajomość pojęcia dezinformacji nie stanowi jeszcze gwarancji odporności informacyjnej, dopiero praktyczne kompetencje krytycznej analizy i weryfikacji treści pełnią funkcję ochronną.

Praktyki informacyjne i weryfikacja wiarygodności informacji

Analiza wyników wskazuje, że osoby z pokolenia Z podejmują działania związane z weryfikacją informacji, choć poziom ich zaangażowania różni się znacząco między grupami narodowościowymi. Największą determinację w potwierdzaniu wiarygodności treści wykazują respondenci z Ukrainy oraz z Polski – po 60% badanych z obu grup odpowiedziało, że „zdecydowanie" korzysta z różnych źródeł informacji w celu sprawdzenia prawdziwości materiałów. W grupie Erasmus taką odpowiedź udzieliło jedynie 17,5% osób, a 30% przyznało, że raczej nie sięga po dodatkowe źródła. Na Rysunku 3 znajdują się dokładne dane potwierdzające tę kwestię.

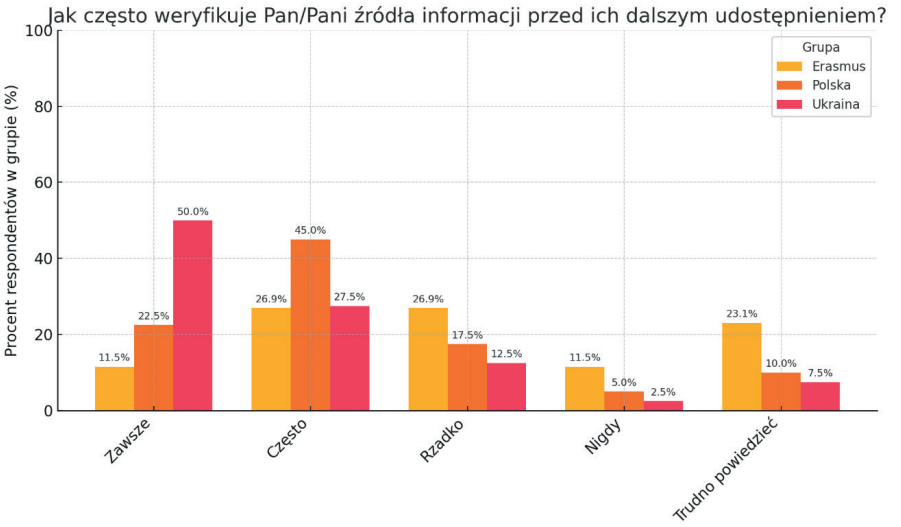


Rysunek 3. Korzystanie z różnych źródeł informacji wśród respondentów

Źródło: opracowanie własne.

Wyniki takie mogą sugerować niższą czujność poznawczą wobec potencjalnie manipulacyjnych treści. Jeszcze wyraźniejsze różnice widoczne są w odpowiedziach dotyczących weryfikacji treści przed ich udostępnieniem. Aż 50% respondentów z Ukrainy deklaruje, że zawsze sprawdza źródło informacji, zanim przekaże je dalej. Wśród Polaków postawa ta występuje u 22,5%, natomiast w grupie Erasmus jedynie u 11,5%. Co istotne, 26,9% tej grupy rzadko sprawdza prawdziwość treści, a 23,1% deklaruje, że trudno im to ocenić, co sugeruje brak utrwalonych nawyków krytycznej konsumpcji

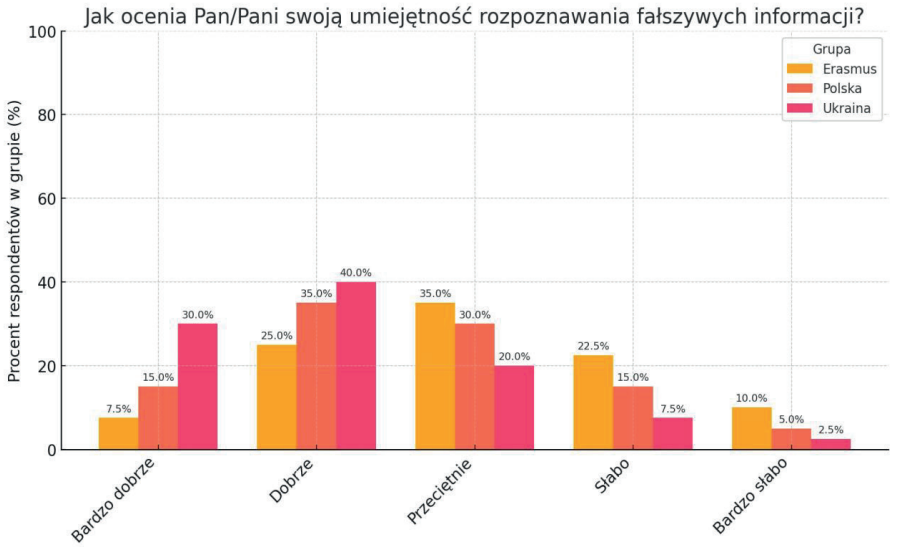
informacji. Dokładniejsze dane statystyczne dotyczące tej kwestii zaprezentowane zostały na Rysunku 4.



Rysunek 4. Częstotliwość weryfikacji źródeł informacji przed jej udostępnieniem

Źródło: opracowanie własne.

Wyniki dotyczące samooceny umiejętności rozpoznawania fałszywych informacji wskazują z kolei, że studenci często przeceniają swoje kompetencje. Większość badanych określiła swoje zdolności w tym zakresie jako „przeciętne" lub „dobre", przy czym najwyżej oceniają je studenci z Ukrainy (40% – „dobrze"), a najniżej – studenci z grupy Erasmus (7,5% – „bardzo dobrze"). Jednocześnie zauważalne jest, że żaden z respondentów nie wskazał całkowitego braku takich umiejętności, co potwierdzają dane umieszczone na Rysunku 5.

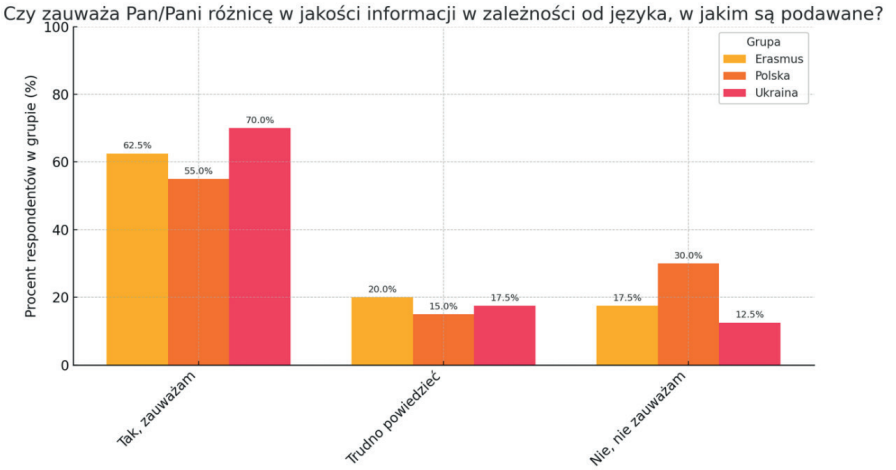


Rysunek 5. Ocena umiejętności rozpoznawania informacji przez respondentów

Źródło: opracowanie własne.

Powyższe wyniki mogą stanowić ponowne potwierdzenie opisywanego w literaturze zjawiska „iluzji kompetencji", czyli jak było powiedziane wcześniej, przekonania o odporności informacyjnej bez realnego zabezpieczenia jej praktyką.

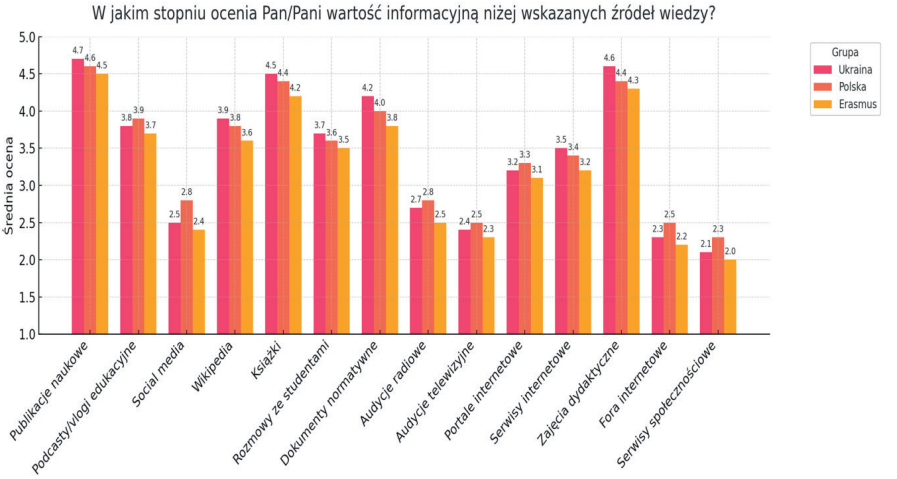
Warto również zwrócić uwagę na aspekt jakości treści i języka komunikacji. W badaniu wykazano, że znacząca część respondentów dostrzega różnice w wiarygodności i jakości informacji w zależności od języka przekazu (Ukraina – 70%, Polska – 55%, Erasmus – 62,5%). Wynik ten wskazuje, że młodzi odbiorcy podejmują próby budowania heurystyk oceny informacji także na poziomie kompetencji językowych i międzykulturowych. Dokładniejsze dane statystyczne pozyskane w tym fragmencie badania zaprezentowano na Rysunku 6.



Rysunek 6. Różnica jakości informacji w zależności od języka przekazu

Źródło: opracowanie własne.

Dodatkową perspektywę oferuje ocena źródeł informacji. Wyniki pokazują, że studenci z Ukrainy częściej wskazują źródła eksperckie (np. publikacje naukowe) jako bardziej wartościowe, podczas gdy w grupie Erasmus wyżej oceniane są social media i treści nieprofesjonalne, co może wzmacniać narażenie na przekazy zmanipulowane lub niezweryfikowane. Na Rysunku 7 przedstawiono dokładne dane statystyczne dotyczące tej kwestii.



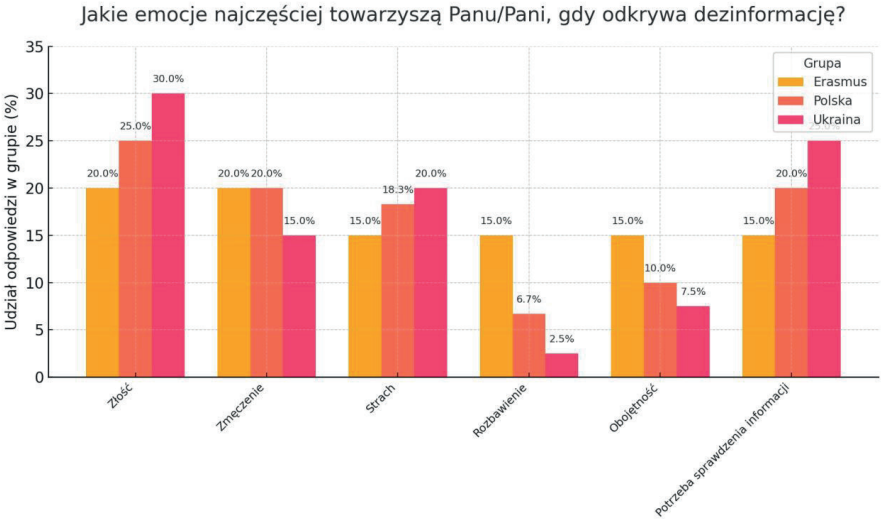
Rysunek 7. Stopień oceny wartości informacji różnych źródeł wiedzy

Źródło: opracowanie własne.

Podsumowując ten wątek, można przyznać, że pokolenie Z jest aktywne w środowisku informacyjnym, jednak ich odporność zależy przede wszystkim od utrwalonych nawyków krytycznych, a te kształtują się najlepiej tam, gdzie zagrożenie jest realnie doświadczane. Badani wykazują pewien poziom zwyczajów weryfikacyjnych, jednak w dużej mierze są one przypadkowe i nieregularne, co znacznie obniża ich odporność na wpływy dezinformacyjne. Można zatem wnioskować, że pokolenie Z deklaruje świadomość zagrożeń i umiarkowaną pewność swoich kompetencji, lecz brakuje im konsekwencji i spójnych praktyk weryfikacyjnych, szczególnie w środowisku mediów społecznościowych.

Odbiór emocjonalny informacji i podatność na manipulację

Ostatnim elementem oceny odporności informacyjnej badanych studentów była analiza ich reakcji emocjonalnych na kontakt z dezinformacją oraz ocena działań podejmowanych przez uczelnie w zakresie edukacji związanej z zagrożeniami informacyjnymi. Wyniki pokazują, że emocjonalny odbiór fałszywych treści ma wyraźny wymiar negatywny. Najczęściej deklarowanymi emocjami były: złość (30% studentów z Ukrainy, 25% z Polski i 20% z Erasmus), zniesmaczenie oraz poczucie potrzeby sprawdzenia informacji – szczególnie silne u badanych z Ukrainy (25%) i Polski (20%). Jednocześnie stosunkowo niewielki odsetek respondentów, zwłaszcza w grupie Erasmus, odczuwa obojętność wobec dezinformacji, co może świadczyć o większej czujności emocjonalnej wobec manipulacji medialnych. Dane dotyczące reakcji emocjonalnych zaprezentowane zostały na Rysunku 8.

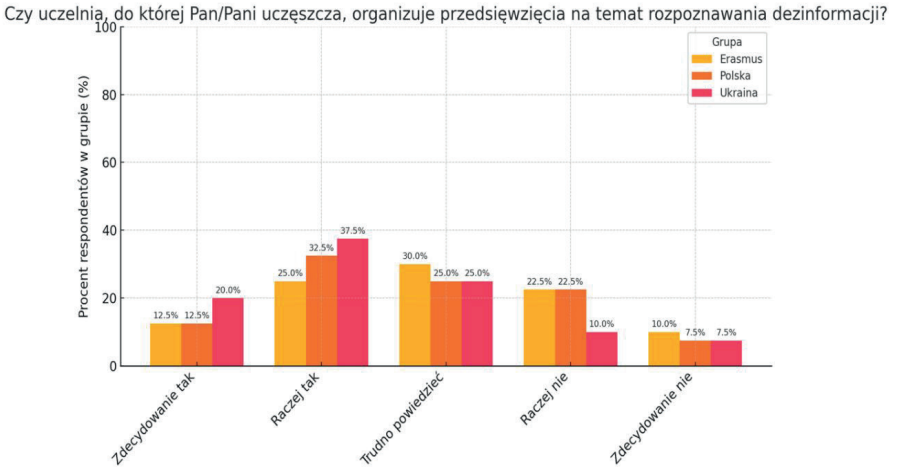


Rysunek 8. Najczęściej towarzyszące emocje przy odkryciu dezinformacji wśród respondentów

Źródło: opracowanie własne.

Analiza emocji jest ważna z perspektywy odporności informacyjnej, ponieważ, jak wskazują badania, silne emocje mogą zarówno sprzyjać, jak i utrudniać racjonalne przetwarzanie informacji. Złość i irytacja mogą zwiększać motywację do sprawdzenia treści, jednak nadmierne emocjonalne pobudzenie utrudnia zachowanie krytycznego myślenia (Lewandowsky, Ecker, Seifert, Schwarz, Cook, 2017).

Drugim ocenianym obszarem było wsparcie instytucjonalne oferowane przez uczelnie. Wyniki pokazują, że studenci rzadko mają kontakt z inicjatywami edukacyjnymi dotyczącymi dezinformacji. Uszczegóławiając, w Polsce 37,5% ankietowanych deklaruje, że uczelnia „raczej" prowadzi takie działania, lecz już 30% nie potrafi jednoznacznie tego ocenić. W grupie Erasmus oraz studentów z Ukrainy rozkłady odpowiedzi są podobne, tj. dominują deklaracje niepewności lub wskazania na brak inicjatyw (22-25%). Jedynie nieliczni ankietowani (ok. 12%) dostrzegają zdecydowane działania uczelni w tym zakresie, co zobrazowane zostały na Rysunku 9.



Rysunek 9. Organizacja przedsięwzięć związanych z rozpoznawaniem dezinformacji w uczelniach respondentów

Źródło: opracowanie własne.

Powyższe wyniki dają podstawę by sądzić, że edukacja związana z odpornością informacyjną nadal zależy głównie od indywidualnej aktywności i samoświadomości studenta, a nie od systemowego wsparcia, co ogranicza skuteczność ochrony społecznej przed manipulacjami w infosferze.

Porównanie poziomu odporności informacyjnej – kontekst międzykulturowy

Analiza wyników pozwala stwierdzić, że poziom odporności informacyjnej badanych różni się w zależności od narodowości. Ankietowani z Ukrainy wykazują najwyższy poziom czujności informacyjnej, co przejawia się zarówno w deklarowanej świadomości dezinformacji, jak i częstszej weryfikacji źródeł oraz silniejszych reakcjach emocjonalnych na potencjalnie fałszywe treści. Do tej grupy ekspozycja na realne działania propagandowe i wojenne operacje informacyjne przekłada się na bardziej wykształcone mechanizmy obronne w środowisku cyfrowym.

Osoby z Polski plasują się na poziomie umiarkowanym, czyli posiadają świadomość zagrożeń i podstawowe kompetencje oceny wiarygodności informacji, jednak częściej postrzegają dezinformację jako zjawisko

abstrakcyjne, rzadziej bezpośrednio zagrażające ich bezpieczeństwu. W efekcie wykazują mniejszą konsekwencję w stosowaniu strategii weryfikacyjnych, co wpływa na obniżenie poziomu odporności informacyjnej.

Najniższy poziom odporności informacyjnej obserwujemy u uczestników programu Erasmus, którzy częściej traktują treści informacyjne z dystansem i humorem, a decyzje o wiarygodności opierają na emocjach lub opiniach otoczenia. W tej grupie wysoka biegłość technologiczna nie przekłada się automatycznie na umiejętności krytyczne, co wzmacnia podatność na manipulacje informacyjne.

Podsumowując należy podkreślić, że kontekst społeczno-polityczny silnie determinuje poziom odporności informacyjnej pokolenia Z.

Podsumowanie

Celem rozdziału była ocena poziomu odporności informacyjnej pokolenia Z w kontekście współczesnych zagrożeń dezinformacyjnych. Przeprowadzone analizy pozwalają stwierdzić, że odporność informacyjna pokolenia Z jest zjawiskiem wielowymiarowym, obejmującym elementy poznawcze, emocjonalne i behawioralne.

W części teoretycznej wykazano, że odporność ta stanowi kluczowy zasób chroniący jednostkę przed wpływem dezinformacji, umożliwiając jej świadome uczestnictwo w środowisku informacyjnym i zachowanie autonomii poznawczej. Współcześnie odporność informacyjna zyskuje status fundamentu bezpieczeństwa demokratycznego, będąc pochodną zarówno indywidualnych kompetencji medialnych, jak i systemowych działań państwa oraz instytucji europejskich.

Pokolenie Z, które funkcjonuje w warunkach permanentnego kontaktu z informacją, charakteryzuje wysoki poziom biegłości technicznej i sprawność korzystania z mediów cyfrowych. Jednocześnie szybki i często bezrefleksyjny sposób konsumpcji treści sprzyja uproszczeniom poznawczym i obniża skuteczność mechanizmów oceny wiarygodności. Wynika z tego, że mimo dużej świadomości zagrożeń młodzi użytkownicy cyberprzestrzeni mogą odczuwać „iluzję kompetencji", czyli poczucie odporności nieuwiarygodnione praktyką krytycznego sprawdzania źródeł.

Zrealizowane badania własne pozwoliły określić poziom odporności informacyjnej przedstawicieli pokolenia Z oraz wskazać obszary

wymagające wsparcia edukacyjnego. Największą świadomość dezinformacji deklarują osoby z Ukrainy, co wynika z ich bezpośredniego doświadczenia zagrożeń informacyjnych w kontekście wojny. Badani z Polski prezentują poziom umiarkowany, natomiast najniższy poziom czujności informacyjnej zauważono w grupie Erasmus, gdzie praktyki weryfikacyjne mają charakter sporadyczny i często intuicyjny.

Wyniki dotyczące odbioru emocjonalnego wskazują, że dominują emocje negatywne takie jak złość czy zniesmaczenie, co może zwiększać motywację do sprawdzania informacji, choć jednocześnie duże pobudzenie emocjonalne może obniżać racjonalność decyzji. Wszyscy badani wykazują stosunkowo niewielką świadomość działań edukacyjnych realizowanych przez uczelnie, co sugeruje brak systemowego wsparcia dla rozwijania odporności informacyjnej.

Zestawienie uzyskanych wyników prowadzi do wniosku, że kontekst społeczno-polityczny stanowi istotny czynnik różnicujący odporność informacyjną pokolenia Z. Ekspozycja na realne zagrożenia wzmacnia mechanizmy obronne, natomiast brak poczucia zagrożenia osłabia motywację do krytycznej oceny treści. Dlatego szkolnictwo wyższe powinno odgrywać bardziej aktywną rolę w procesie edukacyjnym, oferując narzędzia i działania wzmacniające kompetencje weryfikacyjne studentów, szczególnie w obszarze funkcjonowania mediów społecznościowych i algorytmizacji przekazu. Wnioski te wskazują na konieczność integracji edukacji medialnej z programami nauczania oraz rozwijania inicjatyw angażujących, które pozwoliłyby młodym odbiorcom budować odporność informacyjną w sposób świadomy i konsekwentny.

Ograniczeniem prowadzonych badań jest niewielka liczebność próby oraz jej zawężenie do studentów, co nie pozwala na pełne uogólnianie wyników na całe pokolenie Z. W przyszłości warto poszerzyć zakres analiz o inne grupy wiekowe i środowiskowe, a także zastosować metody oceniające rzeczywiste kompetencje weryfikacyjne, takie jak testy identyfikacji fałszywych treści. W kontekście rozwoju narzędzi sztucznej inteligencji rekomendowane jest również prowadzenie badań nad podatnością młodych odbiorców na dezinformację generowaną przez technologie AI oraz nad możliwością wykorzystania AI jako narzędzia wspierającego odporność informacyjną.

Literatura

1. Chałubińska-Jentkiewicz, K., Soler, U., Makuch, A. (2023). Disinformation in Polish Society in 2021 – Trends, Topics, Channels of Transmission*, Polish Political Science Yearbook*, 52(1), 93-107.
2. Cywiński, A. (2024). Students in Poland in the face of the fake news phenomenon in the context of the war in Ukraine. *Dyskurs Młodych Andragogów*, 25(1), 45-60.
3. Dragomir, M., Rúas-Araújo, J., Horowitz, M. (2024). Beyond online disinformation: assessing national information resilience in four European countries. *Humanities and Social Sciences Communications,* 11(1), 101, https://doi.org/10.1057/s41599-024-02605-5
4. Ferraz, T. V., Helal, D. (2024). Informational resilience: a literature review. Revista *Digital de Biblioteconomia e Ciência da Informação*, 22, 1-21, https://doi.org/10.20396/rdbci.v22i00.8674921/en
5. Gajewska, M. (2021). Pokolenie Z na rynku pracy. Szanse i zagrożenia. *Marketing i Rynek*, 5, 21-29.
6. Gergelewicz, T. (2022). Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery. *Cybersecurity and Law*, 1(7), 72-84.
7. Gorazdowski, K. (2024). Dezinformacja w Polsce w kontekście fake newsów i ich wpływu na społeczeństwo, *Studia Administracji i Bezpieczeństwa*, 17(1), 223-251.
8. Komisja Europejska. (2025a). *A strengthened EU Code of Practice on Disinformation*. Pobrano z: https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en (dostęp: 20.03.2026).
9. Komisja Europejska. (2025b). *Strategic communication and countering foreign information manipulation and interference*. Pobrano z: https://commission.europa.eu/topics/countering-information-manipulation_en (dostęp: 20.03.2026).
10. Laboratorium Badania Mediów Uniwersytetu Warszawskiego & Fundacja DigitalPoland. (2024). *Dezinformacja oczami Polaków. Edycja 2024.* Warszawa.

11. Lewandowsky, S., Ecker, U., Seifert, C., Schwarz, N., Cook, J. (2017). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Journal of Applied Research in Memory and Cognition*, 6(4), 353-369, https://doi.org/10.1016/j.jarmac.2017.09.008
12. Lyons, B. A., Montgomery, J. M., Guess, A. M., Nyhan, B., Reifler, J. (2021). Overconfidence in news judgments is associated with false news susceptibility. *Proceedings of the National Academy of Sciences* 118(23), e2019527118, https://doi.org/10.1073/pnas.2019527118
13. Newman, N., Fletcher, R., Robertson, C. T., Eddy, K., Nielsen, R. K. (2024). *Digital News Report 2024,* Oxford: Reuters Institute for the Study of Journalism.
14. OECD. (2024). *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, Paris: OECD Publishing.
15. Pennycook, G., Rand, D. G. (2021). The Psychology of Fake News. *Trends in Cognitive Sciences*, 25/5, 388-402, https://doi.org/10.1016/j.tics.2021.02.007
16. Rogozińska-Pawelczyk, A., Cewińska, J., Lubrańska, A., Oleksiak, P., Striker, M. (2019). *Pokolenia wobec wartości i zagrożeń współczesnych organizacji.* Łódź: Wydawnictwo Uniwersytetu Łódzkiego.
17. Sadowski, M. (2023). Pokolenie Z w polskiej przestrzeni cyfrowej – nawyki i preferencje medialne. *Studia Medioznawcze*, 4(75), 22-35.
18. Tapscott, D. (2010). *Cyfrowa dorosłość. Jak pokolenie sieci zmienia nasz świat.* Warszawa: Wydawnictwa Akademickie i Profesjonalne.
19. Unia Europejska. (2021). *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Wytyczne Komisji Europejskiej w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji, COM(2021)*, 262 final, Bruksela.
20. Uusikylä, P., Jalonen, H., Kallunki, V., Keinänen, A., Sommarberg, S. (2024) Introduction to Information Resilience in the Context of National Preparedness. W: P. Uusikylä, H. Jalonen, A. Jokipii, (red.), *Information Resilience and Comprehensive Security. Information Technology and Global Governance* (1-18). Palgrave Macmillan, https://doi.org/10.1007/978-3-031-66196-9_1
21. Zadroga, M. (2023). *Disinformation Landscape in Poland.* DisinfoLab / EU.

Katarzyna Bakalarczyk-Burakowska[1]

Marcin Mazurek[2]

Akademia Wymiaru Sprawiedliwości, Warszawa

https://doi.org/10.29316/9788368103359_15

DEZINFORMACJA JAKO NARZĘDZIE WSPÓŁCZESNEJ WOJNY HYBRYDOWEJ

DISINFORMATION AS A TOOL OF MODERN HYBRID WARFARE

Streszczenie

Przedmiotem pracy jest dezinformacja jako ważne narzędzie współczesnej wojny hybrydowej. Celem rozdziału jest zaprezentowanie jej istoty, form i metod oddziaływania w kontekście toczącej się od 2014 roku wojny hybrydowej Rosji z kilkoma krajami Europy, w tym z Polską. Dezinformacja w połączeniu z operacjami wpływu oraz ograniczonymi atakami kinetycznymi, odgrywa istotną rolę w koncepcji wojny hybrydowej, która w ostatnich latach przybiera postać wojny kognitywnej. Ten rodzaj wojny ma na celu nie tylko dezinformowanie, ale wpływanie na sposób postrzegania rzeczywistości przez określone społeczeństwo lub jego grupy, aby osłabić umowę społeczną, która wiąże państwo i jego członków; aktor hybrydowy

[1] https://orcid.org/0000-0002-2649-0779, e-mail:katarzyna.burakowska@onet.eu

[2] https://orcid.org/0000-0002-8159-3762, e-mail: marcin.mazurek@aws.edu.pl

próbuje podważyć zaufanie między instytucjami państwowymi a ludźmi. W rezultacie państwo traci swoją legitymację. Problem badawczy sprowadza się do pytania: W jakim stopniu działania dezinformacyjne realizowane w ramach wojny hybrydowej wpływają negatywnie na funkcjonowanie państw i niszcząco na świadomość społeczną? W badaniach przyjęto teoretyczną metodę analizy dokumentów, wspartą metodą komparatystyczną oraz syntezą, analogią, metodami statystycznymi, indukcją i dedukcją. Badania wykazały, że nowe zagrożenia stanowią prawdziwe wyzwania dla państw demokratycznych, w których istnieje wiele luk i słabości, jak m.in. polaryzacja polityczna, słabości systemu medialnego, brak należytej edukacji w zakresie bezpieczeństwa oraz niedostateczna współpraca instytucji i organizacji pozarządowych w zakresie zwalczania dezinformacji. Istnieje potrzeba tworzenia i wdrażania takich koncepcji przeciwdziałania dezinformacji, które powinny stanowić holistyczne podejście obronne wobec wrogich operacji wpływu, wrogich narracji i być oparte na trzech filarach: skutecznej komunikacji, edukacji anty-dezinformacyjnej i aktywnym zwalczaniu dezinformacji.

Słowa kluczowe: dezinformacja, wojna hybrydowa, wojna kognitywna, narracje dezinformacyjne

Abstract

This paper examines disinformation as a key tool in contemporary hybrid warfare. The aim of the chapter is to present its nature, forms, and methods of influence in the context of Russia's ongoing hybrid war with several European countries, including Poland, since 2014. Disinformation, combined with influence operations and limited kinetic attacks, plays a significant role in the concept of hybrid warfare, which in recent years has taken the form of cognitive warfare. This type of warfare aims not only to disinform but also to influence the perception of reality by a specific society or its groups, weakening the social contract that binds the state and its members. The hybrid actor attempts to undermine trust between state institutions and the people. As a result, the state loses its legitimacy. The research question boils down to the following: To what extent do disinformation activities carried out as part of hybrid warfare negatively impact the functioning of states and disrupt public awareness? The research adopted a theoretical method of document analysis, supported by comparative methods, synthesis, analogy, statistical methods, induction, and deduction. The research has shown that new threats pose real challenges to democratic states, where there are many gaps and weaknesses, such as political polarization, weaknesses in the media system, lack of proper security education, and insufficient cooperation between institutions and non-governmental organizations in

combating disinformation. There is a need to create and implement such concepts of countering disinformation, which should constitute a holistic defensive approach against hostile influence operations and hostile narratives and be based on three pillars: effective communication, anti-disinformation education and active combating of disinformation.

Keywords: disinformation, hybrid warfare, cognitive warfare, disinformation narratives

Wstęp

Pojęcie „wojna hybrydowa" od 2014 r. na stałe weszło do terminologii współczesnych konfliktów, bowiem wówczas Rosja, nie bacząc na międzynarodowe traktaty, a jednocześnie nie wypowiadając oficjalnie wojny, zajęła ukraiński Krym i część Donbasu rozpoczynając tzw. dziwną wojnę. Jednak nie był to termin zupełnie nieznany w przeszłości.

Przed 2014 rokiem konflikt między Izraelem a Hezbollahem w 2006 roku był najczęściej przytaczanym przykładem wojny, która mieściła się we współczesnych definicjach wojny hybrydowej. Hezbollah, wyszkolony i wyposażony przez Iran, zaskoczył Izrael wyrafinowanym połączeniem działań partyzanckich i konwencjonalnej taktyki wojskowej oraz wykorzystaniem uzbrojenia i systemów łączności typowych dla sił zbrojnych państw rozwiniętych. Na poziomie strategicznym Hezbollah skutecznie wykorzystywał Internet i inne media do celów informacyjnych i propagandowych. Jego zarządzanie informacją okazało się znacznie skuteczniejsze niż izraelskie w oddziaływaniu na opinię światową od samego początku konfliktu (Wither, 2016).

Z faktu, że to Rosja rozpoczęła wojnę hybrydową z Ukrainą niekiedy niesłusznie formułuje się wniosek, że pojęcie to zrodziło się w rosyjskiej myśli wojskowej. Tymczasem według niektórych ekspertów koncepcja wojny hybrydowej zaistniała po raz pierwszy w amerykańskiej strategii wojskowej i była wykorzystywana przez amerykańskich analityków w operacjach wojskowych prowadzonych w Afganistanie i Iraku (Gruszczak, 2011).

Polska przynajmniej od 2022 roku stała się obiektem wojny hybrydowej ze strony Rosji i Białorusi. Przejawia się ona w intensywnej wojnie informacyjnej, która jest zdominowana przez agresywną dezinformację,

wzmacnianą kinetycznymi mikro atakami, jak akty sabotażu, naruszanie granic przez rakiety i drony, ataki informatyczne na infrastrukturę krytyczną. Na pierwszym plan wybija się tu jednak, co podkreślił w swoim raporcie Rządowy Zespół ds. Dezinformacji, „skoordynowane i zakrojone na szeroką skalę ofensywne działania informacyjne wymierzone w bezpieczeństwo (m.in.: informacyjne, informatyczne, ekonomiczne, energetyczne, zdrowotne) Rzeczypospolitej Polskiej, społeczeństwo polskie, instytucje i procesy demokratyczne, media, organizacje pozarządowe, instytucje naukowe oraz eksperckie i inne" (Raport Zespołu ds. Dezinformacji, 2025).

Pojęcie i istota wojny hybrydowej

W literaturze przedmiotu nie ma ustalonej jednolitej definicji wojny hybrydowej. Co więcej, znaczenie i użycie samego terminu uległy znacznym zmianom w okresie między 2002 a 2015 rokiem. Termin „hybryda" pochodzi od łacińskiego hybrida i oznacza twór, który składa się z różnych elementów, często niepasujących do siebie (PWN, b.d.). W biologii to pewien rodzaj skrzyżowania osobników należących do dwóch różnych odmian, ras, gatunków. Tak jest również z wojną hybrydową – są to działania skomponowane z wielu elementów, wielowarstwowe, wieloczłonowe. A więc mamy wojnę informacyjną, niekiedy wojnę czy presję ekonomiczną, do tego działania czysto militarne jawne i ukryte, ataki cybernetyczne – to wszytko tworzy nam ową hybrydę. Tu jednak wszystkie działania do siebie pasują.

Niektórzy autorzy wymieniają pięć powiązanych ze sobą, ale różnych pojęć wojny hybrydowej (Solmaz, 2022):

1. Zastosowanie synergicznego połączenia broni konwencjonalnej, taktyk nieregularnych, terroryzmu i działań przestępczych na tym samym polu walki.
2. Jednoczesne użycie sił regularnych i nieregularnych pod wspólnym dowództwem.
3. Stosowanie różnych środków militarnych i niemilitarnych w celu zastraszenia wroga.
4. Działania podprogowe obejmujące dowolną kombinację środków brutalnych i bezkrwawych.

5. Sposób osiągania celów politycznych poprzez stosowanie bezkrwawych działań wywrotowych.

Według definicji NATO wojna hybrydowa to „kreatywne wykorzystanie siły twardej, miękkiej i inteligentnej przez wrogie podmioty państwowe lub niepaństwowe w celu osiągnięcia celów wojennych i politycznych. Działania wrogie obejmują szerokie spektrum militarnych i niemilitarnych instrumentów przymusu wykraczających poza konwencjonalnie pojmowaną wielodomenową przestrzeń walki. Wojna hybrydowa obejmuje politykę, dyplomację, informację, gospodarkę, technologię, wojsko i społeczeństwo, a także wymiary takie jak kultura, psychologia, legitymizacja i morale. Skoordynowane przeprowadzanie tych wrogich działań odbywa się zarówno jawnie, jak i skrycie w niejednoznacznych, szarych strefach rozmytych powiązań: między wojną a pokojem, przyjaciółmi a wrogiem, stosunkami wewnętrznymi i zewnętrznymi, cywilnymi a wojskowymi oraz podmiotami państwowymi i niepaństwowymi, a także w obszarach odpowiedzialności zazwyczaj poniżej progu wojny lub jako element towarzyszący regularnym konfliktom zbrojnym" (NATO Headquarters, 2024).

W literaturze nader często sięga się po definicję zaprezentowana w wydaniu „Military Balance" z 2015 r., która kładzie nacisk na stasowane metody walki, a mianowicie „wykorzystanie narzędzi wojskowych i niemilitarnych w zintegrowanej kampanii, której celem jest zaskoczenie przeciwnika, przejęcie inicjatywy i uzyskanie przewagi psychologicznej i fizycznej przy użyciu środków dyplomatycznych, wyrafinowanych i szybkich operacji informacyjnych, elektronicznych i cybernetycznych, tajnych i okazjonalnie jawnych działań wojskowych i wywiadowczych oraz presji ekonomicznej" (The Military Balance, 2015).

Jak wspomniano, wojna hybrydowa to nie jest termin rosyjski, ale zachodni, natomiast rosyjskie podejście do tej kwestii jest nader istotne. Rosyjscy analitycy najczęściej używają terminów „wojna nowej generacji" lub „wojna nieliniowa". Ten pierwszy został upowszechniony w artykule generała Walerija Gierasimowa, szefa rosyjskiego Sztabu Generalnego opublikowanym w lutym 2013 roku. W związku z tym rosyjskie podejście do wojny hybrydowej jest czasami błędnie nazywane „doktryną Gierasimowa". Gierasimow opisuje wojnę nowej generacji jako „szerokie wykorzystanie środków politycznych, ekonomicznych, informacyjnych, humanitarnych i innych środków pozamilitarnych… wspomaganych przez niepokoje

społeczne wśród miejscowej ludności i ukryte siły zbrojne" (Galeotti, 2014). Gierasimow przyznaje, że wiele wskazanych przez niego metod tradycyjnie nie było częścią działań uznawanych za wojenne. Uważa jednak, że są one typowe dla działań wojennych XXI wieku i w rzeczywistości mają większe znaczenie dla osiągnięcia celów strategicznych niż środki militarne, ponieważ mogą zmniejszyć potencjał bojowy wroga poprzez wywoływanie niepokojów społecznych i promowanie klimatu załamania bez jawnego użycia przemocy. Niemniej jednak z artykułu Gierasimowa jasno wynika, że siły zbrojne odgrywają istotną rolę uzupełniającą w działaniach wojennych nowej generacji. Dotyczy to w szczególności sił operacji specjalnych, które mogą być wykorzystywane pod przykrywką „misji pokojowych i regulacji kryzysowych" do nawiązywania kontaktów z grupami opozycyjnymi w państwie docelowym (Galeotti, 2014).

Postrzeganie wojny hybrydowej przez Unię Europejską jest zbliżone do NATO z tym, że unijne gremia chętniej posługują się terminem „zagrożenia hybrydowe", których definicja jest dość złożona. Z perspektywy Unii Europejskiej zagrożenia hybrydowe „łączą w sobie działania konwencjonalne i niekonwencjonalne, militarne i niemilitarne, które mogą być wykorzystywane w skoordynowany sposób przez podmioty państwowe i niepaństwowe w celu osiągnięcia określonych celów politycznych. Kampanie hybrydowe są wielowymiarowe, łączą w sobie środki przymusu i wywrotowe, wykorzystując zarówno konwencjonalne, jak i niekonwencjonalne narzędzia i taktyki. Są one zaprojektowane tak, aby były trudne do wykrycia lub przypisania. Zagrożenia te atakują krytyczne luki w zabezpieczeniach i mają na celu wywołanie zamieszania, aby utrudnić szybkie i skuteczne podejmowanie decyzji" (EEAS, 2018).

W polskich dokumentach normatywnych, ściślej w „Strategii Bezpieczeństwa Narodowego 2020" wojna hybrydowa została opisana jako działania poniżej progu wojny, jakie prowadzi Federacja Rosyjska, „niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także (…) wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych" (Strategia Bezpieczeństwa Narodowego RP, 2020).

Cele wojny hybrydowej są zróżnicowane. Główny cel, jak każdej wojny, to zadawanie przeciwnikowi strat, wszelkich strat, szeroko rozumianych nie tylko materialnych. Zdobycie terytorium jest tu celem rzadkim, współcześnie ważniejszym celem jest ludzki umysł - innymi słowy zdobycie wpływu i kształtowanie rzeczywistości według swoich koncepcji. Ważne jest też osłabienie umowy społecznej, która wiąże państwo i jego członków, aktor hybrydowy próbuje podważyć zaufanie między instytucjami państwowymi a ludźmi. W rezultacie państwo traci swoją legitymację.

Łotewski analityk Jānis Bērziņš podsumowuje rosyjskie podejście do nowoczesnej wojny stwierdził: „Głównym polem bitwy jest umysł, a w rezultacie wojny nowej generacji mają być zdominowane przez wojnę informacyjną i psychologiczną (...) Głównym celem jest ograniczenie konieczności rozmieszczania twardej siły militarnej do niezbędnego minimum" (Bērziņš, 2014). Wydaje się, że jest to cel uniwersalny wojen hybrydowych.

Na podstawie dotychczasowych wojen hybrydowych, zwłaszcza rosyjskiej przeciw Ukrainie z lat 2014-2016, można wyodrębnić kilka charakterystycznych cech tych wojen. Po pierwsze, granica między wojną a czasem pokoju jest niejasna. Oznacza to, że trudno jest zidentyfikować lub dostrzec próg wojny, a więc wojna staje się w jakimś sensie nieuchwytna. Po drugie, taka wojna, pomimo braku jawnej przemocy, przynosi ogromne korzyści, mimo że jest łatwiejsza, tańsza i mniej ryzykowna niż operacje kinetyczne. Po trzecie, celuje w podatności (słabości) w społeczeństwach w sposób, o którym tradycyjnie nie myślimy. Największe sukcesy odnosi w społeczeństwach spolaryzowanych, pękniętych na pół. Po czwarte, synchronizuje swoje środki w nowy sposób. Po piąte, decydujące znaczenie nabierają długoterminowe działania psychologiczne i informacyjne, a kluczową rolę wojny dezinformacyjne (Bērziņš, 2014).

Pojęcie i istota dezinformacji

Dezinformacja jest relatywnie nowym pojęciem, jej teoretyczne fundamenty stworzył francuski autor rosyjskiego pochodzenia Vladimir Volkoff, który opisał ją jako „systematyczne przekazywanie fałszywych sygnałów politycznych, informacji i fabrykacji, celem wytworzenia wypaczonego obrazu powodującego wadliwą analizę sytuacji" (Volkoff, 1991).

Dezinformacja jest częścią szerszego zjawiska, które w literaturze określa się mianem zaburzenia informacyjnego – information disorder (Wardle, Derakhshan, 2017). W tej zaburzonej przestrzeni informacyjnej mieszczą się oprócz wymienionych pojęć również kłamstwa, teorie spiskowe, plotki, mistyfikacje, treści hiperpartyjne, zmanipulowane przekazy medialne itp. Natomiast z perspektywy wojny informacyjnej, jako części wojny hybrydowej, dezinformacja jest jednym z jej narzędzi obok operacji psychologicznych, propagandy, cyberataków społecznościowych oraz manipulacji informacją (Grabowski, 2016).

Pojęcie dezinformacji ma w literaturze wiele definicji. J. H. Fetzer opisuje ją jako rozpowszechnianie fałszywych, błędnych lub wprowadzających w błąd informacji w zamierzonym celu, którym jest oszukanie lub zmylenie odbiorcy (Fetzer, 2004). Tomasz R. Aleksandrowicz definiuje dezinformację jako „sposób przekazania informacji – prawdziwej lub fałszywej – aby wprowadzić w błąd przeciwnika/konkurenta i skłonić go do zachowania zgodnego z naszymi oczekiwaniami i korzystnymi dla nas. Dezinformacja nie jest prostym kłamstwem, czyli przekazaniem fałszywej informacji; jest podstępem" (Aleksandrowicz, 2016). W ten sposób autor powiela opinię chińskiego klasyka wojny informacyjnej Sun Tzu, że dezinformacja to w istocie podstęp. Z kolei D.E. Denning używa równoważnego terminu "manipulowanie percepcją", który odnosi do operacji informacyjnych oddziałujących na percepcję innych, aby wpłynąć na ich emocje, rozumowanie, decyzje i w rezultacie także na działanie. Manipulowanie percepcją może być ukierunkowane na jednostki, grupy lub całe społeczeństwa (Denning, 2002). M. J. Wachowicz zaproponował - jak się ocenia - wyczerpującą definicję dezinformacji jako: „świadome, umyślne i podstępne wprowadzanie w błąd przeciwnika przez ukrywający rzeczywiste zamierzenia dowolny podmiot państwowy lub pozapaństwowy, w przestrzeni fizycznej lub informacyjnej, za pomocą odpowiednio zniekształconych (dosłownie bądź kontekstowo) danych, informacji i dokumentów, w celu doprowadzenia dezinformowanego do podjęcia korzystnych dla dezinformatora decyzji (działań lub zaniechań), zmylenia dezinformowanego, odwrócenia jego uwagi, uzyskania efektu zaskoczenia, zniekształcenia realnego obrazu rzeczy i świata, jak również w celu ochrony godziwych i niegodziwych interesów dezinformatora" (Wachowicz, 2019).

Generalnie dezinformacja może być produktem podmiotów państwowych lub niepaństwowych, krajowych lub zagranicznych, a jej istota (podobnie jak propagandy) tkwi w tym, że informacje określane takim mianem są lub mogą:

- być w całości lub w części fałszywe, zmanipulowane lub wprowadzające w błąd albo wykorzystujące nieetyczne techniki perswazji,
- dotyczyć kwestii leżących w interesie publicznym,
- być obarczone intencją wywołania poczucia braku bezpieczeństwa, wrogości lub polaryzacji, bądź też podejmują próbę zakłócenia procesów demokratycznych,
- być rozpowszechniane i/lub wzmacniane za pomocą zautomatyzowanych i agresywnych technik, takich jak boty społecznościowe, sztuczna inteligencja (AI), mikrotargetowanie lub płatne ludzkie „trolle" (Bayer i in., 2019).

Zasadniczym celem dezinformacji, jest kształtowanie pożądanych postaw i zachowań dezinformowanych, aby w konsekwencji zaspokoić interesy dezinformatora. Podobnie ten cel formułuje T. R. Aleksandrowicz stwierdzając: „celem dezinformacji jest kształtowanie określonego typu postrzegania, którego efektem jest podejmowanie przez ofiarę dezinformacji działań korzystnych dla dezinformującego" (Aleksandrowicz, 2016). R. Nogacki i K. Surdyk określają go równie lapidarnie: „celem dezinformacji jest decydent lub grupa społeczna, który(a) w wyniku działań dezinformacyjnych ma zostać wprowadzony(a) w błąd" (Nogacki, Surdyk, 2020).

W istniejących badaniach na ogół przyjmuje się cztery zasadnicze cele (motywy) dezinformacji: polityczne, finansowe, reputacyjne, społeczno-psychologiczne. Kampanie dezinformacyjne mogą wynikać również wyłącznie z motywacji do poszukiwania rozrywki lub rozgłosu w Internecie. Metoda „trollingu" - znęcania się mającego na celu wywołanie gniewu, wściekłości albo poczucia bezradności atakowanego dla rozrywki sprawców - jest od dawna immanentną cechą kultury internetowej. Poza indywidualnym trollingiem kampanie trollingowe są koordynowane przez nieformalne, zwykle anonimowe grupy użytkowników online i mogą wykorzystywać szereg technik, od fabrykowania wprowadzających w błąd dokumentów i innych informacji po skoordynowane, bezpośrednie próby zaangażowania i wprowadzenia w błąd innych użytkowników w Internecie (Hwang, 2017).

W literaturze przedmiotu istnieje wiele podziałów i klasyfikacji metod (technik) dezinformacji, ale także samej dezinformacji. Ich charakterystykę m należałoby rozpocząć od taksonomii zaproponowanej przez klasyka V. Volkoffa, który wyróżnił następujące (Konieczny, 2021):

- negacja faktów – mamy z nią do czynienia w sytuacji, gdy pojawiające się w przestrzeni publicznej fałszywe informacje nie są możliwe do zweryfikowania z powodu braku osoby czy źródła, które mogłyby obnażyć nieprawdziwy przekaz,
- odwrócenie faktów – podobnie jak przy negacji faktów przedstawia się błędne informacje (tak zwane odwrócone fakty) wówczas, gdy ma się pewność, że nie istnieje możliwość ich weryfikacji,
- mieszanie prawdy i kłamstwa – sytuacja, w której odbiorca ma określony zasób informacji, ale otrzymuje następne, tym razem zafałszowane, które zakłócają właściwą percepcję i ocenę; polega na informowaniu opinii publicznej o wydarzeniach, które miały miejsce, ale odbiorcy posiadają tylko niepełny ich obraz,
- modyfikacja motywu i okoliczności – odbiorca otrzymuje informacje fałszywe, które nie pozwolą mu właściwie ocenić okoliczności i motyw określonego działania,
- rozmycie – podobnie jak kamuflaż, polega na umieszczeniu głównej informacji wraz z faktami nieistotnymi dla prezentowanej sytuacji i jej drobiazgowym opisie; odwraca się uwagę odbiorcy od istoty rzeczy,
- kamuflaż – polega na wytworzenie chaosu informacyjnego, mającego przykryć istotę problemu; nadmierne uszczegółowianie, które prowadzi do rozbicia przekazu na szereg informacji drobnych, nieistotnych,
- interpretacja – jest stosowana, gdy fakty są nie do podważenia, ale u odbiorcy chce się wyrobić pożądaną opinię na ich temat, na przykład skrajnie negatywną lub wywołać pozytywne skojarzenia opinii publicznej,
- generalizacja – w wyniku stosowania generalizacji łagodzi się wyjątkowość, spektakularność danego faktu lub wydarzenia, a jednocześnie nadaje mu się cechę powszechności, braku unikatowości, słowem - celowo obniża się jego rangę i znaczenie, które w istocie posiada,

- ilustracja – na przykładzie zdarzenia jednostkowego ilustruje się szerszy kontekst społeczny,
- nierówna reprezentacja – w sytuacji gdy są prezentowane dwa odmienne stanowiska, metodą tą utrudnia się adwersarzowi pełną wypowiedź, skraca i odpowiednio interpretuje, wchodzi w zdanie, przerywa itp.,
- równa reprezentacja – stosowana w sytuacji, gdy sączona wcześniej dezinformacja uprawdopodobniła się i odbiorca ma przekonanie, że dysponuje informacjami prawdziwymi, polega na zamknięciu dyskursu oraz podsumowaniu, które ma legitymizować nieprawdę przy wykorzystaniu analiz i poparciu ekspertów budzących zaufanie.

Przedstawione metody dezinformacji mogą być skuteczne jedynie w określonych sytuacjach, zwłaszcza niestabilności, zagrożeń, ograniczonym poczuciu bezpieczeństwa (Mazur, 2021).

Należy podkreślić, że stosowanie narzędzi i taktyk dezinformacji jest możliwe dzięki rozwojowi nowoczesnych technologii i postępującej cyfryzacji codziennego życia. Wprawdzie jakaś forma dezinformacji istniała zawsze, ale bez ewolucji technologicznej, bez prawdziwie sieciowego społeczeństwa miałaby znacznie większe trudności w rozprzestrzenianiu się i rozwoju. Amerykański naukowiec, Justin McBrayer usystematyzował i opisał sposoby, w jaki technologia pomogła w „epidemii" dezinformacji (McBrayer, 2021):

- poprzez zwiększanie ilość informacji, które odbieramy,
- poprzez selekcje i organizację (lub zezwalając na to innym) przesyłania podzbiorów fałszywych informacji, na które narażony jest każdy odbiorca,
- poprzez zwiększenie szybkości dystrybucji informacji i dezinformacji,
- poprzez ułatwienie tworzenia fake newsów.

Szeroki wachlarz metod i technik dezinformacji ma na celu konstruowanie takiego przekazu, który nie tylko wprowadza w błąd, ale wpływa na myśli, uczucia i zachowanie odbiorców. Niektóre z metod dezinformacji służą „zmiękczaniu faktów", zakłócaniu i podważaniu u nich wiary w prawdziwość informacji, natomiast kontrapunktem są dla nich inne metody i techniki, które „utwardzają" interpretacje mniej poparte empirycznie. Fakt, że obserwujemy

wiele technik dezinformacji, czasami nakładających się na siebie, a czasami pozostających ze sobą w sprzeczności, wskazuje na złożony charakter komunikacji dezinformacyjnej jako poważnego problemu publicznego.

Dezinformację napędza populizm, który systematycznie zyskuje na popularności. Z populizmem wiąże się pośrednio zjawisko zacierania granic między polityką i rozrywką. Polityka skolonizowana przez media wywiera wpływ na sposób jej przetwarzania; politycy dają niejako przyzwolenie na to, że media stosują narrację lekką, humorystyczną, a nawet satyryczną opisując ważne problemy społeczno-polityczne. Rosnąca popularność humorystycznych opisów dotyczących kwestii politycznych jest symptomem wypierania poważnego debatowania o polityce na rzecz narracji popowych. Ma to krytyczny wpływ na szerokie grono mniej upolitycznionych odbiorców, którzy mają trudności z dokonaniem „krytycznych interpretacji procesu humorystycznej dekonstrukcji" (Dias, Reis, Lopes, 2022).

Chociaż główną areną dezinformacji są media społecznościowe, to jednak potężni aktorzy instrumentalnie wykorzystują obawy związane z fałszywymi wiadomościami, aby zwalczać także rzetelne media informacyjne. Są one niekiedy ofiarami rygorystycznych przepisów, które bezkrytycznie ograniczają wszystkie platformy i działania komunikacyjne. Ich skutkiem, choć nie zawsze zamierzeniem, jest poddanie mediów informacyjnych ograniczeniom, mających na celu cenzurowanie informacji z powodów czysto politycznych.

Niemniej jednak również w tym przypadku niektórzy specjaliści widzą miejsce na optymizm, ponieważ informacyjne „ekscesy" powodują zmęczenie społeczeństwa, co skłania poważniejsze media do wzmacniania norm dziennikarskich i doceniania dziennikarstwa śledczego, które produkuje artykuły dłuższe i bardziej złożone (Dias, Reis, Lopes, 2022).

Dezinformacja istniała zawsze, ale uległa przyspieszeniu dzięki trzem innowacjom technicznym: drukowi, środkom masowego przekazu i Internetowi. W szczególności Internet nabrał jeszcze większego przyspieszenia rozwojowego w ostatniej dekadzie w związku z popularnością mediów społecznościowych. Wraz ze spadkiem zaufania do mediów głównego nurtu rozkwitły alternatywne ekosystemy informacyjne. Rewolucja cyfrowa – w szczególności dostępność łączy szerokopasmowych w ciągu ostatnich piętnastu lat – i późniejszy rozwój mediów społecznościowych zmieniły pole działania. Media społecznościowe stały się wszechobecne w życiu miliardów ludzi. Platformy te opanowały sieć jednocześnie generując ogromne

przychody z reklam. Model biznesowy platform internetowych promuje treści generujące kliknięcia, co zwiększa polaryzację. Sprzyja to tworzeniu bardziej jednorodnych odbiorców, podważa tolerancję dla alternatywnych poglądów (Colomina, Margalef, Youngs, 2021).

Gwałtowny rozwój platform cyfrowych znacznie zwiększył ryzyko dezinformacji na kilka sposobów:

- zalew informacji, o którym wspominano wcześniej, sprzyja dezinformacji, gdyż prowadzi do spadku koncentracji odbiorców, rodzi niechęć do pracochłonnej selekcji i obniża umiejętność rozpatrywania kontrargumentów; prawda znana z psychologii pasuje do sfery cyfrowej: zbyt dużo informacji szkodzi podejmowaniu decyzji (Information Manipulation, 2018),
- wzrasta liczba dostępnych wektorów rozpowszechniania dezinformacji (potencjalnie tyle, ile jest użytkowników tych sieci, czyli miliardy),
- rośnie precyzja segmentacji odbiorców na małe populacje i docierania z określoną informacją; określa się to mianem „mikrotargetowania", na które najbardziej są narażeni młodzi ludzie,
- niski koszt rozpowszechnienia dezinformacji (kilka kliknięć, kilka minut) i łatwość, z jaką można stworzyć pozornie renomowaną stronę internetową; blogowi, stronie internetowej lub witrynie internetowej łatwo można nadać profesjonalny wygląd,
- horyzontalna natura mediów społecznościowych, która umożliwia każdemu udostępnianie treści innym osobom bez konieczności przechodzenia przez organ kontroli redakcyjnej,
- Internet, a szerzej cyberprzestrzeń, nie mają granic, w związku z czym obcy aktorzy państwowi mogą łatwo infiltrować społeczności i rozpowszechniać fałszywe wiadomości,
- następuje postęp techniczny w dostosowywaniu treści fotograficznych, wideo i audio tak, aby coraz bardziej przypominały rzeczywistość, co z kolei utrudnia wykrycie modyfikacji i dezinformacji (Information Manipulation, 2018).

Jedną z popularnych teorii wyjaśniających, dlaczego niektórzy odbiorcy „ulegają" dezinformacji, którą napotykają w Internecie, jest brak umiejętności korzystania z technologii cyfrowych. Uważa się, że ktoś, kto

nie posiada umiejętności korzystania z technologii cyfrowych, może być bardziej podatny na fałszywe informacje i dzielenie się nimi. W rezultacie osoby o niski poziomie wiedzy cyfrowej mogą odegrać znaczącą rolę w rozpowszechnianiu dezinformacji. Argument ten ma intuicyjny sens, jednak w bardzo niewielu badaniach faktycznie przeanalizowano związek między umiejętnością korzystania z technologii cyfrowych, a podatnością na wiarę w fałszywe informacje. Jednak badania przeprowadzone przez Nathaniela Sirlina i Davida Randa wykazały, że umiejętność korzystania z technologii cyfrowych jest istotnie dobrym prognostykiem umiejętności odróżniania prawdziwych informacji od fałszu (Rand, Sirlin, 2022). Natomiast nie ma tak oczywistego związku między umiejętnością korzystania z technologii cyfrowych a chęcią dzielenia się z innymi fałszywymi informacjami za pośrednictwem mediów społecznościowych. Osoby posiadające większą wiedzę cyfrową równie często deklarowały, że udostępniają fałszywe artykuły, jak osoby pozbawione umiejętności cyfrowych. Co najbardziej zaskakujące, nawet osoby o wysokim poziomie umiejętności cyfrowych nie były odporne na kliknięcie „udostępnij" w przypadku fałszywych wiadomości. Według autorów badania, chociaż większość ludzi nie chce rozpowszechniać dezinformacji, to media społecznościowe rozpraszają, odbiorcy zbyt szybko przewijają oglądane strony, a ich uwagę przyciągają oceny społeczne i inne informacje zwrotne, takie jak liczba polubień ich postów, w efekcie „zapominają nawet zadać sobie pytanie, czy dana historia jest prawdziwa, czy fałszywa, zastanawiając się, czy i jak szybko ją udostępnić" (Rand, Sirlin, 2022). Konkluzja jest taka, że umiejętność korzystania z technologii cyfrowych zapewne ułatwia ocenę informacji, ale może nie być kluczowym czynnikiem pozwalającym przewidzieć, kto rozpowszechnia dezinformację w mediach społecznościowych, bowiem nikt nie jest całkowicie odporny na ryzyko rozpowszechniania dezinformacji.

Z kolei R. Janke i B. Cooper stwierdzają, że głównym czynnikiem ułatwiającym szerzenie dezinformacji jest niska umiejętność czytania i pisania odbiorców. Konsekwencje takiego stanu rzeczy przejawiają się m.in. w: trudności w znalezieniu właściwych informacji, niskich kompetencjach w zakresie oceny jakości wiadomości uprzedzeniach do selekcjonowania informacji; braku zaangażowania w czytaniu tekstów dłuższych, tematycznie złożonych, analitycznych (Janke, Cooper, 2017).

Reasumując, oddziaływanie dezinformacji i jej wpływ na kształtowanie opinii publicznej nie jest podważany. Podkreśla się, że dezinformacja jest skuteczna a więc podatna na konsumpcję, przetwarzanie i szerokie udostępnianie, bowiem charakteryzuje się czterema cechami (Wardle, Derakhshan, 2017):

- prowokuje reakcję emocjonalną,
- posiada potężny komponent wizualny,
- ma silną narrację,
- jest powtarzana.

Twórcy kampanii informacyjnych, prawdziwych lub fałszywych, rozumieją siłę tej formuły. Zidentyfikowanie tych cech pomaga rozpoznać kampanie dezinformacyjne, które mają szanse powodzenia oraz ułatwia podejmowanie prób jej przeciwdziałania, aby chronić opinię publiczną.

Dezinformacja zdecydowanie negatywnie oddziałuje na opinię publiczną: osłabia wolność słowa, podmywa fundamenty demokracji, podkopuje zaufanie obywateli do instytucji i mediów. Ten destrukcyjny wpływ jest szczególnie niepokojący w przypadku wyborów i kampanii politycznych. Celem dezinformacji, szczególnie podczas wyborów, nie jest pełne przekonanie opinii publicznej, że jej treść jest prawdziwa, ale wywarcie wpływu na kształtowanie programów politycznych (na to, co ludzie uważają za ważne) i wprowadzenie takiego szumu informacyjnego, który osłabi czynnik racjonalności w decyzjach wyborczych ludzi. Podobnie, niepewność wynikająca z dezinformacji, może w dużym stopniu wpływać na stanowisko opinii publicznej w kwestiach migracji, zmiany klimatu i innych.

Pomiar efektywności dezinformacji jest trudny lub prawie niemożliwy, ponieważ związek między fałszywym komunikatem a późniejszym zachowaniem odbiorców obejmuje zbyt wiele innych zmiennych. Można jednak odróżnić wpływ w środowisku cyfrowym, który jest stosunkowo mierzalny i wymierny (to znaczy, jeśli uda się oddzielić realne konta od coraz bardziej wyrafinowanych botów) od szerszego efektu dezinformacji. Można wyróżnić kilka przejawów oddziaływania dezinformacji na opinię publiczną.

Z jednej strony istnieje skutek bezpośredni. Wiąże się on z pytaniem, czy dezinformacja może owocować powstaniem nowych opinii, czy jedynie wzmocnieniem istniejących. Z dostępnych badań wynika, że dezinformacja nie generuje nowych opinii, lecz zasiewa wątpliwości i zamęt, a czasami ułatwia działanie (Information Manipulation, 2018). Innymi słowy,

czasami dezinformacja przekształca bierne przekonanie w aktywne działanie – w sposób podobny do procesu radykalizacji. Taką sytuacją może być np. głosowanie.

Z drugiej strony istnieje efekt pośredni. Dezinformacja jest pokusą dla elit rządzących, aby naruszać swobody obywatelskie. W ten sposób, paradoksalnie, mogłyby realizować cele obcych państw stających za dezinformacją: nie tyle przekonanie obywateli do tej czy innej narracji, ile nakłonienie rządów do podjęcia działań sprzecznych z ich demokratycznymi, liberalnymi wartościami, które z kolei, wywołałyby reakcję opozycji czy społeczeństwa obywatelskiego. W rezultacie dezinformacja przyczynia się do pogłębienia podziałów w społeczeństwie. Stąd ważne jest, aby państwo właściwie monitorowało działania dezinformacyjne i konsolidowało swoje wysiłki w jej zwalczaniu.

Kwestie bezpośredniego i pośredniego efektu dezinformacji winny znajdować się w polu zainteresowania naukowców, specjalistów zakresu nauki o informacji i komunikacji, które pozwolą na ocenę wpływu kampanii dezinformacyjnych na kształtowanie opinii publicznej. Informacja coraz częściej postrzegana jest jako dobro wspólne, którego ochrona winna być powinnością wszystkich obywateli dbających o jakość debaty publicznej. Przede wszystkim obowiązkiem społeczeństwa obywatelskiego jest rozwijanie własnej odporności na dezinformację, natomiast rządy mogą i powinny przyjść z pomocą tam, gdzie występują oczywiste zagrożenia podważające podstawy demokracji i bezpieczeństwa.

Dezinformacja w wojnie hybrydowej. Wojna kognitywna

Dezinformacja rosyjska będąca częścią wojny pełnoskalowej przeciwko Ukrainie oraz hybrydowej wymierzonej w takie państwa, jak m.in. Polska, Mołdawia, Rumunia czy Gruzja, weszła w zaawansowane stadium, które coraz częściej określa się wojną kognitywną. Rządowy Zespół ds. Dezinformacji określa ją w odniesieniu do Polski jako „rodzaj agresji niemilitarnej i mającej na celu nie tylko wprowadzanie w błąd, ale także, a może przede wszystkim, wpływanie na opinie i postawy Polaków" (Raport Zespołu ds. Dezinformacji, 2025).

Wojna kognitywna wkracza na obszar, który określamy „poznaniem", a więc to ono jest istotną areną wrogich działań, mających na celu przejęcie

kontroli nad umysłem decydenta i grupy docelowej. Jest to wymiar, w którym ludzie myślą, postrzegają, wizualizują i podejmują decyzje. Obejmuje między innymi: przekonania kulturowe, normy, motywację, emocje, podatności, tożsamość, ideologię, percepcję, wolę, świadomość, postawę, zrozumienie, opinie, doświadczenie, wiedzę, założenia i zachowanie (Gergelewicz, 2024).

W literaturze funkcjonuje wiele określeń wojny kognitywnej. Francuscy autorzy określają ja jako „niekonwencjonalną formą działań wojennych, która wykorzystuje narzędzia cybernetyczne do modyfikowania procesów poznawczych wroga, wykorzystywania uprzedzeń mentalnych lub myślenia refleksyjnego, a także prowokowania zniekształceń myślowych, wpływania na podejmowanie decyzji i utrudniania działań, co ma negatywne skutki zarówno na poziomie indywidualnym, jak i zbiorowym" (Claverie, du Cluzel, 2023). W tym ujęciu wojna kognitywna daleko wykracza poza „zwykłe" zniekształcanie informacji, ale ukierunkowuje informacje na oddziaływanie na myślenie poszczególnych osób. Wykracza zatem poza ludzkie konsekwencje cyberwojny, obejmującej inżynierię komputerową, robotykę i programy komputerowe; efekt poznawczy nie jest produktem ubocznym działania, lecz jego celem samym w sobie.

W ujęciu NATO wojna kognitywna „integruje możliwości cybernetyczne, informacyjne, psychologiczne i socjotechniczne. Działania te, prowadzone w synchronizacji z innymi instrumentami władzy, mogą wpływać na postawy i zachowania poprzez wpływanie, ochronę lub zakłócanie procesów poznawczych jednostek i grup w celu uzyskania przewagi nad przeciwnikiem" (NATO ACT, 2023).

Wojna kognitywna prowadzona jest za pomocą różnych narzędzi, a jednym z najistotniejszych jest dezinformacja. W tym kontekście T. Greglewicz wymienia trzy elementy dezinformacji: manipulacja faktami, tworzenie fake newsów oraz szum w sferze informacyjnej (Gergelewicz, 2024).

Przywoływany wcześniej rządowy Zespół ds. Dezinformacji uwypuklił kilka cech charakterystycznych i technik wojny kognitywnej (Raport Zespołu ds. Dezinformacji, 2025):

- podstawowy ciężar działań przenosi się na wpływanie na percepcję wydarzeń oraz na procesy decyzyjne,
- przywiązywanie większej wagi do dewaluacji faktów niż o ukrycie kłamstwa,

- operowanie tzw. wielkim kłamstwem – absurdalnym oskarżeniem drugiej strony, możliwie szokującym i wywołującym sensację. Absurdalność „wielkiego kłamstwa" paradoksalnie buduje jego wiarygodność na zasadzie: „przecież by tego sobie nie wymyślili",
- wykorzystanie języka łatwego do zrozumienia – język skomplikowany i wyszukany może być odrzucany przez wyborców przyzwyczajonych do coraz krótszych komunikatów w mediach społecznościowych. Prymitywizm języka, jako starannie dobraną metoda,
- prowadzenie operacji kognitywnych polegające na wprowadzeniu do środowiska naukowego i eksperckiego fałszywych teorii naukowych, paradygmatów, koncepcji oraz strategii wywierających wpływ na zarządzanie państwem w celu osłabienia jego potencjału naukowego i obronnego,
- wprowadzanie narracji, które odrzucają jako naiwne i lekkomyślne argumenty dotyczące praw człowieka, wolności słowa czy demokracji,
- wprowadzanie do obiegu publicznego narracji spiskowych.

Autorzy podkreślają, że pochodną operacji kognitywnych jest zarządzanie refleksyjne. Według nich to „techniki i sposoby manipulacji emocjami, percepcją i świadomością kierownictwa wojskowego, elit przywódczych, grup społecznych państwa przeciwnika. To zestaw metod sterowania społecznego, metod psychofizycznych (siła, przymus, presja i strach) oraz intelektualnych (propaganda, dezinformacja), których dobór opiera się na kognitywnym modelu zachowań rywala. Łączy umiejętności zarządzania, psychologii oraz manipulacji i jest nastawione na deformację interpretowanej przez odbiorców rzeczywistości" (Raport Zespołu ds. Dezinformacji, 2025).

Rosyjska wojna kognitywna przeciwko Polsce prowadzona jest za pomocą tzw. narracji pośrednich i bezpośrednich. Narracje pośrednie mają na celu podważenie sensu polityki otwarcia na Zachód prowadzonej przez kolejne rządy, a więc atak skierowany jest na zachodnie wartości i cywilizację. Zachód jest przedstawiany jako źródło „upadku i zepsucia": traci tożsamość (narodową, religijną, rasową), odcina się od „chrześcijańskich korzeni" oraz „obiektywnych i uniwersalnych" wzorców społecznych (pod tym terminem zwykle rozumie się wzorce chrześcijańskie i bardzo konserwatywne). Państwa i społeczeństwa zachodnie stały się zakładnikami elit - mediów, instytucji, polityków, wielkiego biznesu, a co jeszcze gorsze

ulegają kolejnym ideologiom, np. gender, LGBT, ateizm, ekologizm, polityczna poprawność (Raport Zespołu ds. Dezinformacji, 2025).

Narracje bezpośrednie odnoszą się do konkretnych (rzekomych) działań władz, o których „zwykły" Polak nie jest nawet informowany. Tu najczęściej podnoszony jest wątek imigrantów, m.in. takie „sensacje", jakoby rząd polski zamykał szkoły podstawowe, aby przeznaczyć ich budynki na zakwaterowanie dla imigrantów i planuje sprowadzać do Polski „400 tysięcy murzynów rocznie" (Raport Zespołu ds. Dezinformacji, 2025). Ponadto niemal codziennymi są zarzuty ze strony rosyjskich i prorosyjskich mediów, jakoby Polska: chciała podzielić Ukrainę terytorialnie, wchłonąć zachodnią Ukrainę; chciała sprowokować nuklearną wojnę z Rosją czy bezmyślnie niszczyła swoją gospodarkę, kupując amerykańską broń (Raport Zespołu ds. Dezinformacji, 2025).

Praktycznie dopiero od 2014 roku Polska, podobnie jak wiele innych krajów Europy Środkowo-Wschodniej zaczęła obserwować, identyfikować i analizować zagrożenia związane z dezinformacją i wpływami obcego państwa, zwłaszcza Rosji w kontekście jej agresji na Ukrainę. Dla potrzeb analizy przyjęto zachodni termin FIMI (Foreign Information Manipulation and Interference), czyli Zagraniczna Manipulacja i Zakłócanie Informacji - używany do opisania działań podejmowanych przez wrogie podmioty zagraniczne, które mają na celu wpływanie na opinię publiczną, procesy polityczne (procesy decyzyjne), czy bezpieczeństwo narodowe poprzez manipulację informacją lub zakłócenia przepływu informacji.

Z polskiego raportu opartego na danych Europejskie Służby Działań Zewnętrznych (European External Action Service – EEAS), badającej zagrożenia wynikające z manipulacji informacjami zagranicznymi i ingerencją w sprawy międzynarodowe (FIMI) wynika, że do najważniejszych narracji, jakie Rosja stosowała przeciwko Polsce w latach 2014-2024 należały (Sijer, Pokora, 2024):

- manipulowanie obrazem rosyjskiej agresji na Ukrainę i przedstawianie go jako rzekomej wojny obronnej Rosji przeciwko Zachodowi/NATO,
- presja psychologiczna przez zastraszanie – szantaż bronią nuklearną,
- szantaż kryzysem energetycznym,
- kampanie propagandowe uderzające w wizerunek Wojska Polskiego i polskiej polityki obronnej,

- manipulowanie historią II wojny światowej,
- propaganda antynatowska i antyamerykańska,
- dezinformacja związana z COVID-19,
- podsycanie napięć społecznych i politycznych,
- kampanie dezinformacyjne wymierzone w Ukrainę,
- ataki na polskie media i dziennikarzy,
- wykorzystywanie kryzysu migracyjnego (mechanizm przymusowej migracji zastosowany przez Rosję i Białoruś przeciwko Polsce i krajom bałtyckim),
- ataki na polski wizerunek międzynarodowy,
- wspieranie skrajnej prawicy i lewicy (polaryzacja),
- podsycanie anty-imigranckich nastrojów,
- wspieranie ruchów antysystemowych.

Generalnie celem tych działań była destabilizacja społeczeństwa, osłabienie zaufania do instytucji demokratycznych, podważenie wyników wyborów, wywołanie niepokojów społecznych lub wpłynięcie na decyzje polityczne. Odbiorca tych narracji, według założeń, miał stracić zaufanie do państwa, nauki czy mediów, a także do współobywateli.

Polskie władze i odpowiedzialne instytucje na ogół prawidłowo reagowały na zagrożenia wynikające z prowadzonej wojny kognitywnej. Wprowadzono wiele nowych regulacji prawnych, np. w zakresie cyberbezpieczeństwa. Instytucje takie jak ABW, MON, MSWiA oraz NASK odgrywają kluczową rolę w przeciwdziałaniu dezinformacji, a niedawno powołano nowe instytucje odpowiedzialne za monitorowanie i przeciwdziałanie zagrożeniom informacyjnym.

Wciąż istnieje wiele luk i słabości, które wrogie podmioty mogą wykorzystać. Głównymi wyzwaniami są m.in. polaryzacja polityczna, słabości systemu medialnego, brak edukacji medialnej oraz niedostateczna współpraca instytucji i organizacji pozarządowych w zakresie zwalczania dezinformacji.

Podsumowanie

Dezinformacja to współcześnie ważny oręż wojen hybrydowych. Jest skuteczna, bo przede wszystkim nie wymaga wysokich nakładów i kierowana

jest głównie tam, gdzie znajduje podatny grunt, a więc w spolaryzowanych politycznie społeczeństwach.

Psychologicznie istnieje wiele wyjaśnień na czym polega skuteczność dezinformacji, m.in. jest to wynik selektywnego przyjmowanie informacji i całkowity opór wobec faktów u odbiorców, zwłaszcza jeśli są sprzeczne z wcześniejszymi ich przekonaniami i wartościami. Są też badania wskazujące na to, że głównym czynnikiem ułatwiającym szerzenie dezinformacji jest niska umiejętność czytania i pisania odbiorców. Konsekwencje takiego stanu rzeczy przejawiają się m.in. w: trudności w znalezieniu właściwych informacji, niskich kompetencjach w zakresie oceny jakości wiadomości, uprzedzeniach do selekcjonowania informacji. braku zaangażowania w czytaniu tekstów dłuższych, tematycznie złożonych, analitycznych.

Dezinformacja to kluczowy czynnik wspomagający działania w szarej strefie i integralna część obecnego zestawu narzędzi wojny hybrydowej. Dezinformacja, w połączeniu z operacjami wpływu, odgrywa istotną rolę w koncepcji wojny hybrydowej, zarówno z perspektywy zagrożenia, jak i własnej odporności strony atakowanej.

Wojna kognitywna to nie tylko wyrafinowane posłużenie się dezinformacją, ale koncepcja tej wojny uwypukla znaczącą zmianę charakteru współczesnego konfliktu, umieszczając ludzki umysł w centrum działań strategicznych. W ramach działań wojny kognitywnej atakuje się jednostki i podważa zaufanie społeczne, spójność i stabilność instytucjonalną, najczęściej bez użycia siły kinetycznej.

Rosyjskie i białoruskie oddziaływanie na polskie społeczeństwo celuje w pogłębianie podziałów społecznych i tworzenie nowych, ma się przyczynić do dalszego spadku zaufania wobec instytucji demokratycznych, ale i naukowych, eksperckich oraz mediów oraz ma na celu dyskredytację wartości europejskich i praw człowieka – wreszcie ma cynicznie je wykorzystywać do realizacji swoich interesów.

Wojna kognitywna stanowi poważne wyzwanie ze względu na jej długofalowy, systemowy wpływ oraz zdolność do wykorzystywania nowych technologii, takich jak sztuczna inteligencja i neuronauka. Dla bezpieczeństwa narodowego oznacza to priorytetowe traktowanie inicjatyw budujących odporność, które wzmacniają zaufanie społeczne i krytyczne myślenie, wzmacniają kompetencje cyfrowe oraz wspierają inkluzyjność w celu minimalizowania podatności na zagrożenia.

Celem wojny kognitywnej jest wpływanie na sposób postrzegania rzeczywistości przez określone społeczeństwo lub jego grupy. Im większa polaryzacja społeczeństw, im mniej wykształceni są ludzie i im mniej krytycznego myślenia angażuje się w przyswajanie wiedzy z infosfery, tym łatwiej ulega się wpływom i podejmuje określone działania. Społeczeństwa winny być wyposażone w narzędzia do obrony i być wspierane przez państwo w walce z zagrożeniami informacyjnymi. Wszelkie koncepcje przeciwdziałania dezinformacji powinny stanowić holistyczne podejście obronne wobec wrogich operacji wpływu, wrogich narracji i być oparte na trzech filarach: skutecznej komunikacji, edukacji antydezinformacyjnej i zwalczaniu dezinformacji.

Literatura

1. Aleksandrowicz, T. R. (2016). *Podstawy walki informacyjnej*. Warszawa: Editions Spotkania.
2. Bayer, J., Bitiukova, N., Bárd, P., Szakács, J., Alemanno, A., Uszkiewicz, E. (2019). *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. Strasbourg: Directorate General for Internal Policies of the Union (IPOL), European Parliament.
3. Bērziņš, J. (2014). Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy. *Policy Paper No 2*. National Defence Academy of Latvia, Center for Security and Strategic Research.
4. Claverie, B., du Cluzel, F. (2023). *The Cognitive Warfare Concept*. NATO Innovation Hub. Pobrano z: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (dostęp: 20.03.2026).
5. Colomina, C., Margalef, H. S., Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world*. Strasbourg: Directorate General for External Policies of the Union, European Parliament.
6. Denning, D. (2002). *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa: Wydawnictwo Naukowo-Techniczne.
7. Dias, C. P., Reis, B., Lopes, P. (2022). Post-Truth and Democracy: a Reflection on Disinformation Mechanisms. *Revista de Investigaciones Políticas y Sociológicas, 21*(1).

8. European External Action Service (EEAS). (2018). *A Europe that Protects: Countering Hybrid Threats*. Pobrano z: https://www.eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf (dostęp: 20.03.2026).
9. Fetzer, J. H. (2004). Disinformation: The Use of False Information. *Minds and Machines, 14*.
10. Galeotti, M. (2014). *The 'Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows*. Pobrano z: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (dostęp: 20.03.2026).
11. Gergelewicz, T. (2024). Countering Disinformation Concept for building social resilience in times of cognitive warfare. *Defence Science Review, 20*, 31-44.
12. Grabowski, T. (2016). Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016). *Horyzonty Polityki, 7*(20).
13. Gruszczak, A. (2011). *Hybrydowość współczesnych wojen – analiza krytyczna*. W: W. Sokala, B. Zapała (red.), *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*. Warszawa: Biuro Bezpieczeństwa Narodowego.
14. Hwang, T. (2017). *Digital Disinformation*. A Primer. Washington, DC: The Atlantic Council, Eurasia Center.
15. Information Manipulation, A Challenge for Our Democracies. (2018). *Paris: A Report by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces)*.
16. Janke, R., Cooper, B. (2017). *News Literacy: Helping Students and Teachers Decode Fake News*. Lanham: Rowman & Littlefield.
17. Komisja do spraw badania wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004-2024. (2025). *Raport Zespołu ds. Dezinformacji*. Warszawa.
18. Konieczny, M. (2021). Wokół pojęcia dezinformacji w aspekcie prawno-kryminalistycznym. De Securitate et Defensione. *O Bezpieczeństwie i Obronności, 2*(7).
19. Mazur, J. (2021). Informacja i dezinformacja w przestrzeni publicznej. Wprowadzenie do problematyki. *Przestrzeń Społeczna, 1*(21).

20. McBrayer, J. P. (2021). *Beyond Fake News: Finding the Truth in a World of Misinformation*. New York: Routledge.
21. NATO Allied Command Transformation (ACT). (2023). *Cognitive Warfare: Strengthening and Defending the Mind*. Pobrano z: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind (dostęp: 20.03.2026).
22. NATO Headquarters. (2024). *Hybrid Threats and Hybrid Warfare. Reference Curriculum*. Brussels: NATO Headquarters.
23. Nogacki, R., Surdyk, K. (2020). *Teoria i praktyka działań dezinformacyjnych*. PWG Skarbiec. Pobrano z: https://www.wywiad-gospodarczy.pl/teoria-i-praktyka-dzialan-dezinformacyjnych.html (dostęp: 20.03.2026).
24. PWN. (b.d.). *Hybryda*. Słownik języka polskiego PWN. Pobrano z: https://sjp.pwn.pl/sjp/hybryda;2560929.html (dostęp: 20.03.2026).
25. Rand, D., Sirlin, N. (2022). *Digital Literacy Doesn't Stop the Spread of Misinformation*. Scientific American. Pobrano z: https://www.scientificamerican.com/article/digital-literacy-doesnt-stop-the-spread-of-misinformation/ (dostęp: 20.03.2026).
26. Sijer, M., Pokora, W. (2024). *Obce manipulacje informacyjne i ingerencja zewnętrzna (FIMI). Zagrożenia i przeciwdziałania w Polsce za okres od 2014 do 2024 r. Raport 09*. Info OPS Polska, International Republican Institute.
27. Solmaz, T. (2022). *Hybrid Warfare: One Term, Many Meanings*. Small Wars Journal.
28. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. (2020). Warszawa.
29. The Military Balance. (2015). *Complex Crises Call for Adaptable and Durable Capabilities, 115*(1).
30. Volkoff, V. (1991). *Psychosocjotechnika, dezinformacja – oręż wojny*. Warszawa: Wydawnictwo Delikon.
31. Wachowicz, M. J. (2019). Ujęcia teoretyczne pojęcia dezinformacji. Kwartalnik Wiedzy Obronnej, *1-2*, 226-253. https://doi.org/10.34752/x40y-nc78
32. Wardle, C., Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policymaking*. Strasbourg: Council of Europe.
33. Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal, 15*(2).

Mateusz Rudaś[1]

Akademia Leona Koźmińskiego w Warszawie

https://doi.org/10.29316/9788368103359_16

CYFROWE PLATFORMY E-COMMERCE A BEZPIECZEŃSTWO FINANSÓW PUBLICZNYCH – WYBRANE PROBLEMY SYSTEMOWE

DIGITAL E-COMMERCE PLATFORMS AND PUBLIC FINANCIAL SECURITY – SELECTED SYSTEMIC PROBLEMS

Streszczenie

Celem rozdziału jest analiza roli cyfrowych platform e-commerce w systemie bezpieczeństwa finansów publicznych, ze szczególnym uwzględnieniem identyfikacji ryzyk fiskalnych wynikających z platformowego modelu handlu oraz oceny skuteczności instrumentów prawnych ograniczających te zagrożenia, zwłaszcza w obszarze podatku VAT oraz należności celnych. Problem badawczy sformułowano: w jakim stopniu rozwój cyfrowych platform e-commerce wpływa na poziom bezpieczeństwa finansów publicznych? W rozdziale przyjęto hipotezę, że cyfrowe platformy

[1] https://orcid.org/0009-0008-8140-9719, e-mail: mateusz.rudas@jrd.pl

e-commerce, ze względu na skalę działalności, transgraniczny charakter obrotu oraz centralizację danych transakcyjnych, stały się kluczowym elementem systemu ochrony bezpieczeństwa finansów publicznych, jednak obowiązujące regulacje prawne jedynie częściowo odpowiadają na rzeczywiste przesunięcie ryzyk fiskalnych z poziomu podatników na poziom architektury platform cyfrowych. W opracowaniu zastosowano metodę dogmatyczno-prawną, uzupełnioną analizą funkcjonalną oraz odniesieniami do praktyki stosowania prawa i regulacji unijnych w zakresie opodatkowania transakcji e-commerce i poboru należności publicznoprawnych. Przeprowadzona analiza pozwala stwierdzić, że rozwój handlu elektronicznego prowadzi do systemowego przekształcenia mechanizmów poboru danin publicznych, w którym kluczową rolę zaczynają odgrywać platformy e-commerce jako podmioty gromadzące dane i pośredniczące w transakcjach, natomiast skuteczna ochrona bezpieczeństwa finansów publicznych wymaga dalszego rozwoju regulacji prawnych, zwiększenia obowiązków informacyjnych i raportowych platform oraz zapewnienia rzetelności danych transakcyjnych przy jednoczesnym zachowaniu równowagi między efektywnością fiskalną a zasadą proporcjonalności regulacji.

Słowa kluczowe: cyfrowe platformy e-commerce, bezpieczeństwo finansów publicznych, VAT, ryzyka fiskalne, handel elektroniczny

Abstract

The aim of the chapter is to analyze the role of digital e-commerce platforms in the system of public finance security, with particular emphasis on the identification of fiscal risks resulting from the platform trading model and the assessment of the effectiveness of legal instruments to mitigate these threats, especially in the area of VAT and customs duties. The research problem was formulated: to what extent does the development of digital e-commerce platforms affect the level of security of public finances? The chapter hypothesizes that digital e-commerce platforms, due to the scale of their operations, cross-border nature of trade and centralization of transaction data, have become a key element of the system of protection of public finances, but the current legal regulations only partially respond to the actual shift of fiscal risks from the level of taxpayers to the level of digital platform architecture. The study uses the dogmatic and legal method, supplemented by a functional analysis and references to the practice of applying EU law and regulations in the field of taxation of e-commerce transactions and collection of public law receivables. The analysis allows us to conclude that the development of e-commerce leads to a systemic transformation of the mechanisms for collecting public levies, in which e-commerce platforms as entities collecting data and intermediating in transactions

are beginning to play a key role, while effective protection of the security of public finances requires further development of legal regulations, increased information and reporting obligations of platforms and ensuring the reliability of transaction data while maintaining a balance between fiscal efficiency and the principle of proportionality of regulation.

Keywords: digital e-commerce platforms, security of public finances, VAT, fiscal risks, e-commerce

Wstęp

Bezpieczeństwo finansów publicznych stanowi jedno z fundamentalnych zagadnień współczesnego państwa, warunkując jego zdolność do realizacji konstytucyjnych zadań oraz zapewnienia stabilności gospodarczej i społecznej. Wśród kluczowych wyznaczników bezpieczeństwa finansów publicznych w literaturze wskazuje się zasadę równowagi budżetowej (Hanusz, 2019). Sprowadza się ona do dostosowania globalnej kwoty wydatków budżetowych do globalnej kwoty dochodów budżetowych. Bezpieczeństwo finansów publicznych pozostaje przy tym w ścisłym związku z efektywnością systemu poboru danin publicznych oraz zaufaniem obywateli do państwa i stanowionego przez nie prawa podatkowego. W kontekście bezpieczeństwa finansowego państwa wskazuje się na ryzyko wynikające z niewystarczającej ściągalności dochodów budżetowych, przejawiające się m.in. narastaniem zaległości podatkowych. Zjawisko to może istotnie ograniczać zdolność państwa do finansowania i wykonywania zadań publicznych (Grześkiewicz, 2018).

Współczesne zagrożenia dla bezpieczeństwa finansów publicznych mają w coraz większym stopniu charakter systemowy. Nie wynikają one wyłącznie z działań o charakterze incydentalnym lub jednostkowych naruszeń prawa podatkowego, lecz są konsekwencją głębokich zmian strukturalnych zachodzących w gospodarce. Do najważniejszych z nich należy postępująca cyfryzacja obrotu gospodarczego, która prowadzi do transformacji tradycyjnych modeli biznesowych oraz zmiany sposobu funkcjonowania rynków. Cyfryzacja ta wpływa bezpośrednio na relacje pomiędzy podatnikami a administracją publiczną, stawiając przed systemem finansów

publicznych nowe wyzwania o charakterze organizacyjnym, prawnym i technologicznym.

Jednym z najbardziej dynamicznie rozwijających się obszarów gospodarki cyfrowej jest handel typu e-commerce. Zgodnie z danymi Głównego Urzędu Statystycznego w listopadzie 2025 r. sprzedaż detaliczna realizowana za pośrednictwem Internetu, liczona w cenach bieżących, wzrosła o 6,6% w porównaniu z analogicznym okresem roku poprzedniego. Jednocześnie udział handlu internetowego w całkowitej sprzedaży detalicznej zwiększył się z poziomu 10,7% do 11,0% (Główny Urząd Statystyczny, 2025). Transakcje e-commerce coraz częściej realizowane są za pośrednictwem cyfrowych platform, które pełnią funkcję pośredników pomiędzy sprzedawcami a nabywcami, organizując jednocześnie płatności, logistykę oraz przetwarzanie danych transakcyjnych. Platformy e-commerce nie tylko ułatwiają zawieranie umów, lecz w istotny sposób kształtują warunki obrotu, wpływając na transparentność transakcji, sposób ustalania cen oraz przepływ środków finansowych.

Z perspektywy finansów publicznych szczególne znaczenie ma fakt, że działalność platform e-commerce cechuje się wysokim stopniem automatyzacji oraz masowością transakcji o niskiej jednostkowej wartości. Model ten prowadzi do rozproszenia obrotu oraz utrudnia identyfikację rzeczywistych uczestników transakcji, co w praktyce ogranicza skuteczność tradycyjnych instrumentów kontroli podatkowej i celnej. Administracja publiczna nie posiada bezpośredniego dostępu do danych niezbędnych do prawidłowej oceny obowiązków podatkowych, gdyż informacje te są agregowane i kontrolowane przez prywatne podmioty prowadzące platformy cyfrowe. Powstaje w ten sposób asymetria informacyjna, która sprzyja powstawaniu luk podatkowych oraz zwiększa ryzyko uszczupleń dochodów publicznych.

Cyfrowe platformy e-commerce nie są przy tym jedynie neutralnymi technicznie pośrednikami. Ich rola w obrocie gospodarczym powoduje, że stają się one kluczowymi punktami koncentracji danych i przepływów finansowych. Z tego względu coraz częściej postrzegane są jako podmioty pełniące funkcję swoistych „węzłów fiskalnych", od których w znacznym stopniu zależy skuteczność poboru podatków i ceł. Przesunięcie ciężaru odpowiedzialności fiskalnej z poziomu indywidualnych podatników na poziom architektury platform prowadzi do konieczności redefinicji roli tych podmiotów w systemie finansów publicznych.

Szczególnie wyraźnie opisane ryzyka ujawniają się w obszarze handlu transgranicznego, gdzie złożoność łańcuchów dostaw oraz różnice pomiędzy krajowymi systemami podatkowymi sprzyjają błędom lub nadużyciom. Dotyczy to w szczególności opodatkowania podatkiem od towarów i usług oraz poboru należności celnych od towarów importowanych. Masowość przesyłek o niskiej jednostkowej wartości, charakterystyczna dla sprzedaży internetowej, sprzyja zaniżaniu wartości towarów, błędnej kwalifikacji transakcji oraz wykorzystywaniu luk regulacyjnych, co może prowadzić do istotnych uszczupleń dochodów publicznych.

W odpowiedzi na powyższe wyzwania ustawodawca krajowy oraz unijny podejmuje działania zmierzające do wzmocnienia ochrony bezpieczeństwa finansów publicznych w środowisku cyfrowym. Działania te obejmują stopniowe włączanie platform e-commerce w system poboru danin publicznych poprzez nakładanie na nie obowiązków informacyjnych, raportowych oraz – w określonych przypadkach – materialnej odpowiedzialności podatkowej. Rozwiązania te stanowią element szerszego procesu polegającego na wykorzystaniu potencjału informacyjnego i organizacyjnego platform e-commerce do realizacji celów fiskalnych państwa.

Celem niniejszego rozdziału jest analiza roli cyfrowych platform e-commerce w kontekście bezpieczeństwa finansów publicznych, ze szczególnym uwzględnieniem wybranych problemów systemowych związanych z opodatkowaniem transakcji realizowanych w środowisku cyfrowym. Przedmiotem analizy jest identyfikacja ryzyk fiskalnych wynikających z platformowego modelu obrotu oraz ocena skuteczności instrumentów prawnych mających na celu ich ograniczenie, w szczególności w kontekście zwolnienia z należności celnych dla przesyłek o niskiej wartości oraz opodatkowania podatkiem od towarów i usług transakcji realizowanych za pośrednictwem platform e-commerce. Przedmiotem analizy jest również rola danych, kontroli i odpowiedzialności platform w ochronie dochodów publicznych.

Postawiona w rozdziale teza zakłada, że cyfrowe platformy e-commerce, ze względu na skalę działalności, transgraniczny charakter obrotu oraz centralizację danych transakcyjnych, stały się kluczowym elementem systemu ochrony bezpieczeństwa finansów publicznych, przy czym obowiązujące regulacje prawne jedynie częściowo odpowiadają na rzeczywiste przesunięcie ryzyk fiskalnych z poziomu podatników na poziom architektury

platform. W rozdziale zastosowano metodę dogmatyczno-prawną, uzupełnioną o analizę funkcjonalną oraz odniesienia do praktyki stosowania prawa, co pozwala na ocenę efektywności obowiązujących rozwiązań oraz sformułowanie wniosków o charakterze systemowym.

Rola platform cyfrowych w systemie finansów publicznych

Rozwój cyfrowych platform e-commerce doprowadził do istotnej zmiany struktury obrotu gospodarczego, w ramach której tradycyjny, dwustronny model relacji pomiędzy sprzedawcą a nabywcą został zastąpiony przez model platformowy, obejmujący co najmniej trzech uczestników: sprzedawcę, nabywcę oraz operatora platformy. Platforma e-commerce nie ogranicza się przy tym do biernego udostępniania infrastruktury technicznej, lecz aktywnie organizuje proces zawierania transakcji, wpływając na warunki obrotu, przepływ informacji oraz realizację płatności. Z punktu widzenia systemu finansów publicznych oznacza to pojawienie się nowego podmiotu, który – mimo formalnego braku statusu podatnika w odniesieniu do większości transakcji – posiada realny wpływ na wykonanie obowiązków podatkowych i celnych przez pozostałych uczestników obrotu (OECD, 2019).

Specyfika działalności platform e-commerce polega na centralizacji kluczowych funkcji związanych z obrotem gospodarczym. Platformy te gromadzą dane dotyczące stron transakcji, przedmiotu dostawy, ceny, miejsca przeznaczenia towaru oraz momentu dokonania transakcji, a często również pośredniczą w płatnościach i organizują proces logistyczny. Zakres informacji pozostających w dyspozycji platform znacząco przewyższa zakres danych, jakimi dysponuje administracja publiczna w ramach tradycyjnych mechanizmów poboru danin publicznych. W rezultacie operatorzy platform uzyskują faktyczną kontrolę nad strumieniami informacyjnymi i finansowymi, które mają bezpośrednie znaczenie fiskalne.

Powyższe uwarunkowania prowadzą do stopniowego przesunięcia ciężaru ryzyk fiskalnych z poziomu indywidualnych podatników na poziom architektury platformy. O ile w klasycznym modelu obrotu gospodarczego odpowiedzialność za prawidłowe rozliczenie podatków i ceł spoczywała przede wszystkim na sprzedawcy lub importerze, o tyle w modelu platformowym skuteczność poboru danin publicznych w coraz większym stopniu

zależy od jakości danych oraz procedur stosowanych przez operatora platformy. Platforma staje się zatem kluczowym ogniwem systemu ochrony bezpieczeństwa finansów publicznych, niezależnie od formalnej konstrukcji obowiązków podatkowych.

W literaturze przedmiotu zjawisko to opisywane jest jako przejście od podejścia opartego wyłącznie na indywidualnej odpowiedzialności podatnika do modelu uwzględniającego rolę pośredników cyfrowych w realizacji funkcji fiskalnych państwa (Dmoch i in., 2022). Platformy e-commerce, ze względu na swoją pozycję rynkową oraz dostęp do danych, są predestynowane do pełnienia funkcji wspierających pobór danin publicznych, w szczególności w obszarach charakteryzujących się wysokim poziomem transgraniczności i masowości transakcji. Jednocześnie rodzi to pytania o granice odpowiedzialności platform oraz o zgodność tego modelu z zasadami prawa podatkowego, w tym zasadą pewności prawa i proporcjonalności obciążeń.

Z perspektywy bezpieczeństwa finansów publicznych istotne znaczenie ma również fakt, że platformy e-commerce działają w skali międzynarodowej, często poza bezpośrednim zasięgiem jurysdykcji pojedynczego państwa. Transgraniczny charakter ich działalności utrudnia skuteczne egzekwowanie obowiązków publicznoprawnych oraz sprzyja wykorzystywaniu różnic pomiędzy krajowymi systemami prawnymi. W takich warunkach państwo traci możliwość pełnej kontroli nad procesem poboru danin publicznych, co może prowadzić do erozji bazy podatkowej oraz osłabienia stabilności dochodów publicznych.

W odpowiedzi na powyższe wyzwania obserwuje się stopniową zmianę podejścia regulacyjnego, polegającą na włączaniu platform e-commerce w realizację funkcji tradycyjnie zastrzeżonych dla administracji publicznej. Zmiana ta znajduje wyraz w nakładaniu na platformy obowiązków informacyjnych, raportowych oraz – w określonych przypadkach – materialnych obowiązków podatkowych. Warto tutaj zwrócić w szczególności uwagę przepisy Dyrektywy 2006/112/WE Rady z dnia 28 listopada 2006 r. w sprawie wspólnego systemu podatku od wartości dodanej (Dz. U. UE. L. 2006 nr 347, str. 1 z późn. zm.), która przewiduje odpowiedzialność platform elektronicznych za pobór podatku VAT od określonych dostaw. Tendencja ta wpisuje się w szerszy proces, w ramach którego architektura systemów cyfrowych ma sprzyjać automatycznemu wykonywaniu obowiązków publicznoprawnych, będąc jednocześnie odpowiedzią na potrzebę

dostosowania regulacji prawnych do gwałtownie rosnącej cyfryzacji światowego handlu (Bełdzikowski i in., 2024).

Na tle powyższych rozważań cyfrowe platformy e-commerce należy postrzegać nie tylko jako uczestników obrotu gospodarczego, lecz również jako istotny element w infrastrukturze systemu finansów publicznych. Ich rola w zakresie gromadzenia i przetwarzania danych, organizacji transakcji oraz pośrednictwa w płatnościach sprawia, że od sposobu funkcjonowania platform w znacznym stopniu zależy skuteczność ochrony bezpieczeństwa finansów publicznych. Okoliczność ta uzasadnia potrzebę pogłębionej analizy prawnej pozycji platform e-commerce w systemie poboru danin publicznych, która stanowi punkt wyjścia do dalszych rozważań zawartych w niniejszym rozdziale.

Cyfryzacja handlu a nowe ryzyka dla bezpieczeństwa finansów publicznych

Postępująca cyfryzacja handlu prowadzi do zasadniczej zmiany warunków funkcjonowania systemu finansów publicznych. Zmiana ta nie polega wyłącznie na zastąpieniu tradycyjnych kanałów sprzedaży kanałami elektronicznymi, lecz ma charakter strukturalny i systemowy. Cyfryzacja wpływa bowiem na sposób organizacji obrotu gospodarczego, role poszczególnych uczestników rynku oraz mechanizmy przepływu informacji i środków finansowych. W konsekwencji powstają nowe kategorie ryzyk fiskalnych, które nie mogą być skutecznie adresowane przy wykorzystaniu wyłącznie klasycznych instrumentów prawa podatkowego i celnego.

Jednym z kluczowych czynników generujących ryzyka dla bezpieczeństwa finansów publicznych w środowisku cyfrowym jest masowość transakcji realizowanych w ramach handlu elektronicznego. Platformy e-commerce umożliwiają zawieranie ogromnej liczby transakcji o relatywnie niskiej jednostkowej wartości, które z perspektywy administracji publicznej są trudne do indywidualnej weryfikacji. Model ten znacząco utrudnia stosowanie tradycyjnych metod kontroli podatkowej opartych na analizie pojedynczych zdarzeń gospodarczych, prowadząc do konieczności zarządzania ryzykiem na poziomie systemowym, a nie jednostkowym.

Szczególnym przykładem systemowego ryzyka fiskalnego związanego z masowością transakcji w handlu elektronicznym było funkcjonujące

przez wiele lat w państwach członkowskich Unii Europejskiej zwolnienie z podatku od towarów i usług dla przesyłek o niskiej wartości, nieprzekraczającej 22 euro. Mechanizm ten sprzyjał powstawaniu zjawiska faktycznego nieopodatkowania towarów wysyłanych w ramach transgranicznego handlu elektronicznego, polegającego na braku opodatkowania zarówno w państwie pochodzenia, jak i w państwie konsumpcji. W konsekwencji regulacja ta stała się istotnym źródłem luki w podatku od towarów i usług. Jak wskazywał Europejski Trybunał Obrachunkowy, nadużycia związane z tym zwolnieniem przybierały w praktyce różnorodne formy, w szczególności polegały na zaniżaniu deklarowanej wartości towarów w celu spełnienia kryteriów zwolnienia, sztucznym dzieleniu przesyłek na mniejsze partie, a także na błędnym kwalifikowaniu przesyłek handlowych jako podarunków. Praktyki te, trudne do wykrycia w warunkach masowego i zautomatyzowanego obrotu, dodatkowo potęgowały skalę ryzyk fiskalnych oraz ograniczały skuteczność kontroli podatkowej (Europejski Trybunał Obrachunkowy, 2019).

Kolejnym istotnym źródłem ryzyk fiskalnych jest transgraniczny charakter handlu elektronicznego. Cyfrowe platformy e-commerce umożliwiają łatwy dostęp do rynków zagranicznych zarówno sprzedawcom, jak i nabywcom, często bez fizycznej obecności przedsiębiorcy w państwie konsumpcji. Prowadzi to do rozmycia tradycyjnych kryteriów jurysdykcji podatkowej oraz utrudnia ustalenie miejsca opodatkowania poszczególnych transakcji. W rezultacie państwa napotykają trudności w egzekwowaniu obowiązków podatkowych od podmiotów działających poza ich terytorium, co może prowadzić do erozji bazy podatkowej (Małecka-Ziembińska, 2023).

Transgraniczność e-commerce wiąże się również z problemem fragmentaryzacji łańcuchów dostaw. W praktyce proces sprzedaży, płatności, wysyłki towaru oraz obsługi posprzedażowej może być realizowany przez różne podmioty zlokalizowane w odmiennych jurysdykcjach. Taki model utrudnia przypisanie odpowiedzialności podatkowej oraz identyfikację podmiotu zobowiązanego do rozliczenia danin publicznych. Z punktu widzenia bezpieczeństwa finansów publicznych prowadzi to do zwiększenia ryzyka sporów kompetencyjnych pomiędzy państwami oraz wykorzystywania rozbieżności regulacyjnych przez uczestników obrotu.

Istotnym elementem ryzyka fiskalnego w środowisku cyfrowym jest asymetria informacyjna pomiędzy administracją publiczną a podmiotami prywatnymi. Platformy e-commerce dysponują szczegółowymi danymi

dotyczącymi transakcji, które z punktu widzenia państwa mają kluczowe znaczenie dla prawidłowego ustalenia zobowiązań podatkowych. Jednocześnie dostęp administracji do tych danych jest ograniczony lub pośredni, co utrudnia skuteczne wykrywanie nieprawidłowości. Asymetria ta osłabia zdolność państwa do bieżącej ochrony dochodów publicznych i sprzyja przenoszeniu ryzyk fiskalnych na etap kontroli ex post.

Automatyzacja procesów handlowych i podatkowych, charakterystyczna dla środowiska platformowego, stanowi jednocześnie źródło szans i zagrożeń dla bezpieczeństwa finansów publicznych. Z jednej strony umożliwia ona usprawnienie poboru danin publicznych poprzez integrację systemów informatycznych oraz automatyczne przekazywanie danych do administracji publicznej. Z drugiej strony automatyzacja może sprzyjać skalowaniu nieprawidłowości, gdyż błędy w algorytmach lub świadome manipulacje danymi mogą oddziaływać na ogromną liczbę transakcji jednocześnie.

Opisane ryzyka mają charakter strukturalny i nie mogą być skutecznie eliminowane wyłącznie poprzez zwiększenie intensywności kontroli podatkowych. Wymagają one bowiem zmiany podejścia do ochrony bezpieczeństwa finansów publicznych, polegającej na przesunięciu akcentu z kontroli jednostkowych transakcji na zarządzanie ryzykiem systemowym. W tym kontekście kluczowego znaczenia nabiera współpraca z operatorami platform e-commerce oraz wykorzystanie ich potencjału informacyjnego w procesie poboru danin publicznych.

Podsumowując, cyfryzacja handlu prowadzi do powstania nowych, złożonych ryzyk dla bezpieczeństwa finansów publicznych, które wynikają z masowości transakcji, transgraniczności obrotu, asymetrii informacyjnej oraz automatyzacji procesów gospodarczych. Zjawiska te uzasadniają potrzebę dalszej analizy szczególnych instrumentów prawnych mających na celu ograniczenie ryzyk fiskalnych, w tym rozwiązań dotyczących zwolnień celnych dla przesyłek o niskiej wartości oraz mechanizmów opodatkowania VAT transakcji realizowanych za pośrednictwem platform e-commerce, które zostaną omówione w kolejnych częściach rozdziału.

Zwolnienie z cła dla przesyłek o niskiej wartości jako przykład ryzyka systemowego

Zwolnienie z należności celnych dla przesyłek o niskiej wartości stanowi jeden z kluczowych elementów konstrukcji prawnej importowego e-commerce w Unii Europejskiej. Zgodnie z obowiązującymi przepisami prawa celnego towary importowane w przesyłkach o wartości nieprzekraczającej 150 euro korzystają ze zwolnienia z cła, przy jednoczesnym objęciu ich obowiązkiem rozliczenia podatku od towarów i usług. Rozwiązanie to zostało wprowadzone jako instrument upraszczający obsługę drobnych przesyłek oraz ograniczający koszty administracyjne poboru należności celnych.

W realiach współczesnego handlu elektronicznego zwolnienie to utraciło jednak swój marginalny charakter i stało się elementem masowego modelu obrotu towarowego. Jak wskazuje Komisja Europejska, w 2024 r. do Unii Europejskiej importowano bezpośrednio do konsumentów około 4,6 mld przesyłek o niskiej wartości, co odpowiada nawet 12 mln paczek dziennie. Skala ta powoduje, że mechanizm zwolnienia z cła przestaje pełnić funkcję czysto technicznego uproszczenia, a zaczyna generować ryzyka o charakterze systemowym, istotne z punktu widzenia bezpieczeństwa finansów publicznych (Komisja Europejska, 2025).

Podstawowym źródłem ryzyka fiskalnego związanego ze zwolnieniem celnym dla przesyłek o niskiej wartości jest możliwość zaniżania deklarowanej wartości towarów importowanych. W praktyce polega to na deklarowaniu wartości przesyłki na poziomie nieprzekraczającym progu 150 euro, mimo że rzeczywista wartość ekonomiczna towaru jest wyższa. Zjawisko to jest szczególnie trudne do wykrycia w warunkach masowego importu drobnych przesyłek, gdzie indywidualna weryfikacja każdej deklaracji celnej jest organizacyjnie i ekonomicznie nieuzasadniona.

Drugim istotnym mechanizmem nadużyć jest sztuczne dzielenie przesyłek, polegające na rozbijaniu jednego zamówienia na kilka odrębnych paczek, z których każda formalnie spełnia kryteria zwolnienia celnego. Mechanizm ten jest szczególnie łatwy do zastosowania w środowisku platformowym, gdzie proces logistyczny jest zautomatyzowany, a konsument końcowy często nie posiada wiedzy o faktycznej strukturze wysyłki towarów. Z punktu widzenia administracji publicznej prowadzi to do trudności w ustaleniu rzeczywistej wartości transakcji i przypisaniu odpowiedzialności fiskalnej.

Ryzyka systemowe potęguje również brak pełnej spójności pomiędzy danymi wykorzystywanymi do celów celnych, podatkowych oraz logistycznych. W praktyce informacje dotyczące wartości towaru, kosztów transportu oraz podstawy opodatkowania VAT pochodzą z różnych systemów informatycznych, co sprzyja powstawaniu rozbieżności i utrudnia skuteczną kontrolę prawidłowości rozliczeń. Brak integracji danych prowadzi do sytuacji, w której administracja publiczna nie dysponuje kompletnym obrazem transakcji, co zwiększa ryzyko uszczupleń dochodów publicznych.

Szczególną rolę w funkcjonowaniu mechanizmu zwolnienia celnego odgrywają cyfrowe platformy e-commerce. Platformy te w praktyce wpływają na sposób prezentowania ceny towaru, kosztów transportu oraz innych elementów składających się na deklarowaną wartość przesyłki. Jednocześnie co do zasady nie ponoszą one bezpośredniej odpowiedzialności za prawidłowość zgłoszeń celnych, które składane są przez sprzedawców lub operatorów logistycznych. Taka konstrukcja sprzyja przerzucaniu ryzyka fiskalnego na administrację publiczną i osłabia efektywność ochrony dochodów publicznych.

Skala wskazanych problemów doprowadziła do podjęcia na poziomie Unii Europejskiej prób przeciwdziałania ryzykom systemowym generowanym przez masowy import przesyłek e-commerce. Komisja Europejska wprost wskazuje, że dotychczasowy model oparty na zwolnieniu z cła dla przesyłek o niskiej wartości oraz selektywnej kontroli nie odpowiada już realiom współczesnego handlu elektronicznego. W konsekwencji zaproponowano wprowadzenie stałej, niedyskryminującej opłaty manipulacyjnej pobieranej od każdej przesyłki e-commerce importowanej spoza Unii Europejskiej (Rada Unii Europejskiej i Komisja Europejska, 2025).

Projektowana opłata nie ma charakteru należności celnej ani podatku sensu stricto, lecz stanowi instrument o charakterze parafiskalnym, którego celem jest pokrycie kosztów obsługi celnej oraz wzmocnienie zdolności administracji publicznej do skutecznej kontroli masowych przesyłek. Z punktu widzenia bezpieczeństwa finansów publicznych istotne znaczenie ma fakt, że opłata ta ma być pobierana niezależnie od wartości towaru, co ogranicza bodźce do zaniżania wartości przesyłek w celu uniknięcia obciążeń publicznoprawnych.

Wprowadzenie jednolitej opłaty od każdej przesyłki należy postrzegać jako próbę przesunięcia akcentu z reaktywnej kontroli nadużyć na

instrument prewencyjny, który ogranicza ryzyka systemowe już na etapie masowego importu towarów. Rozwiązanie to potwierdza tezę, że zwolnienie z cła dla przesyłek o niskiej wartości w obecnym kształcie przestało odpowiadać realiom cyfrowego handlu i wymaga uzupełnienia o nowe narzędzia ochrony bezpieczeństwa finansów publicznych. Jednocześnie należy podkreślić, że skuteczność projektowanych rozwiązań będzie zależeć od ich integracji z mechanizmami opodatkowania VAT oraz od stopnia zaangażowania platform e-commerce w realizację funkcji fiskalnych.

Opodatkowanie VAT transakcji realizowanych za pośrednictwem platform e-commerce jako instrument ochrony bezpieczeństwa finansów publicznych

Podatek od towarów i usług stanowi jedno z podstawowych źródeł dochodów publicznych państw członkowskich Unii Europejskiej, a jego stabilność ma kluczowe znaczenie dla bezpieczeństwa finansów publicznych. W przeciwieństwie do podatków bezpośrednich VAT charakteryzuje się wysoką wrażliwością na zmiany modeli biznesowych oraz sposobu organizacji obrotu gospodarczego. Rozwój handlu elektronicznego i platform cyfrowych ujawnił istotne ograniczenia tradycyjnych mechanizmów poboru VAT, opartych na indywidualnej odpowiedzialności podatnika i terytorialnym powiązaniu działalności gospodarczej.

W środowisku platformowym klasyczny model rozliczania VAT, w którym obowiązek podatkowy realizowany jest przez sprzedawcę towarów lub usług, okazał się niewystarczający. Transgraniczny charakter e-commerce, rozproszenie sprzedawców oraz masowość mikrotransakcji prowadziły do istotnych uszczupleń dochodów publicznych oraz wzrostu luki VAT. W odpowiedzi na te zjawiska ustawodawca unijny podjął działania zmierzające do przeniesienia ciężaru odpowiedzialności podatkowej na podmioty, które faktycznie kontrolują przepływ informacji i środków finansowych, czyli na operatorów platform e-commerce.

Kluczowym instrumentem tej zmiany stała się konstrukcja tzw. deemed supplier, polegająca na uznaniu platformy e-commerce za podmiot dokonujący dostawy towarów na potrzeby VAT, mimo że faktycznym sprzedawcą pozostaje podmiot trzeci. Mechanizm ten prowadzi do przesunięcia obowiązku rozliczenia VAT z poziomu często anonimowego lub

zagranicznego sprzedawcy na platformę, która posiada realne możliwości organizacyjne i techniczne do prawidłowego wykonania obowiązków podatkowych. Z punktu widzenia bezpieczeństwa finansów publicznych rozwiązanie to ma charakter systemowy, gdyż ogranicza ryzyko niewywiązywania się z obowiązków podatkowych w skali masowej (Merkx, 2022).

Uzupełnieniem mechanizmu deemed supplier są procedury szczególne rozliczania VAT, w tym One Stop Shop (OSS) oraz Import One Stop Shop (IOSS). Procedury te mają na celu uproszczenie rozliczeń podatkowych w transgranicznym e-commerce oraz zwiększenie poziomu dobrowolnej zgodności podatkowej. Z perspektywy administracji publicznej OSS i IOSS umożliwiają centralizację rozliczeń VAT oraz ograniczenie liczby podmiotów zobowiązanych do bezpośredniego kontaktu z organami podatkowymi, co sprzyja efektywniejszemu zarządzaniu ryzykiem fiskalnym.

W szczególności procedura IOSS została zaprojektowana jako narzędzie ograniczające ryzyka związane z importem towarów o niskiej wartości. Umożliwia ona pobór VAT już na etapie sprzedaży towaru, przed jego wprowadzeniem na obszar celny Unii Europejskiej, co w założeniu eliminuje potrzebę poboru podatku na etapie odprawy celnej. Mechanizm ten ma istotne znaczenie dla bezpieczeństwa finansów publicznych, gdyż zmniejsza ryzyko niepobrania VAT w warunkach masowego importu przesyłek e-commerce.

Praktyka stosowania procedur OSS i IOSS ujawnia jednak szereg ograniczeń. Skuteczność tych mechanizmów uzależniona jest w dużej mierze od jakości danych przekazywanych przez platformy oraz od poziomu współpracy pomiędzy administracjami podatkowymi państw członkowskich. W przypadku braku rzetelnych informacji dotyczących wartości towarów, miejsca konsumpcji lub statusu sprzedawcy ryzyka fiskalne nie zostają wyeliminowane, lecz jedynie przesunięte na inny etap obrotu.

Z punktu widzenia bezpieczeństwa finansów publicznych istotne znaczenie ma również kwestia zakresu odpowiedzialności platform e-commerce za prawidłowość rozliczeń VAT. Obowiązujące regulacje koncentrują się przede wszystkim na funkcji poboru podatku, pozostawiając w ograniczonym zakresie odpowiedzialność za prawdziwość danych źródłowych. W rezultacie platformy pełnią rolę pośredników fiskalnych, jednak nie zawsze ponoszą konsekwencje systemowe w przypadku wystąpienia nadużyć lub błędów o charakterze masowym.

Analiza roli VAT w środowisku platformowym prowadzi do wniosku, że podatek ten przestaje pełnić wyłącznie funkcję rozliczeniową, a staje się instrumentem prewencyjnym ochrony bezpieczeństwa finansów publicznych. Mechanizmy takie jak deemed supplier, OSS czy IOSS mają na celu nie tylko pobór podatku, lecz również wymuszenie określonych standardów organizacyjnych i informacyjnych po stronie platform e-commerce. Skuteczność tych instrumentów zależy jednak od ich dalszego rozwoju oraz integracji z innymi narzędziami prawnymi, w tym regulacjami dotyczącymi odpowiedzialności platform i dostępu administracji publicznej do danych transakcyjnych.

Platformy e-commerce a administracja publiczna – dane, kontrola i odpowiedzialność

Cyfryzacja handlu elektronicznego prowadzi do zasadniczej zmiany relacji pomiędzy administracją publiczną a uczestnikami obrotu gospodarczego. W modelu platformowym kluczowym zasobem determinującym skuteczność poboru danin publicznych stają się dane transakcyjne, obejmujące informacje o stronach transakcji, przedmiocie dostawy, wartości towarów oraz przepływach finansowych. Dostęp do tych danych pozostaje w przeważającej mierze w rękach operatorów platform e-commerce, co powoduje przesunięcie ciężaru ochrony bezpieczeństwa finansów publicznych z poziomu bezpośredniej kontroli podatników na poziom kontroli architektury systemu cyfrowego.

Znaczenie danych transakcyjnych dla administracji publicznej znajduje również potwierdzenie w orzecznictwie sądów administracyjnych. W wyroku z dnia 10 marca 2022 r., sygn. III SA/Wa 1806/21, Wojewódzki Sąd Administracyjny w Warszawie jednoznacznie uznał, że raport generowany przez platformę Amazon może stanowić pełnoprawny dowód dla celów podatku od towarów i usług. Sąd wskazał, że raport ten należy traktować jako dokument przewozowy w rozumieniu art. 42 ust. 3 pkt 1 ustawy o podatku od towarów i usług, tj. dokument otrzymany od przewoźnika lub spedytora odpowiedzialnego za wywóz towarów z terytorium kraju, w sytuacji gdy przewóz jest zlecany podmiotowi trzeciemu. Orzeczenie to potwierdza, że dane gromadzone i przetwarzane przez platformy e-commerce mogą posiadać walor dowodowy równoważny tradycyjnym dokumentom

wykorzystywanym w kontroli podatkowej, a jednocześnie uwydatnia kluczowe znaczenie jakości tych danych oraz istnienia odpowiedniej struktury organizacyjno-technicznej zapewniającej ich prawidłowość, kompletność i rzetelność.

W warunkach masowego e-commerce tradycyjne instrumenty kontroli podatkowej, oparte na analizie pojedynczych zdarzeń gospodarczych, tracą na skuteczności. Administracja publiczna zmuszona jest do stosowania narzędzi analitycznych oraz selektywnego podejścia do kontroli, opartego na profilowaniu ryzyka. W takich realiach jakość, kompletność i terminowość danych przekazywanych przez platformy e-commerce stają się kluczowym czynnikiem determinującym efektywność ochrony dochodów publicznych.

W odpowiedzi na te wyzwania ustawodawca unijny konsekwentnie zmierza do wzmacniania obowiązków informacyjnych i raportowych nakładanych na operatorów platform cyfrowych. Szczególnym przykładem tego podejścia jest Dyrektywa Rady (UE) 2021/514 z dnia 22 marca 2021 r. zmieniająca dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opodatkowania (Dz.U. UE. L. 2021 r. nr 104 str. 1, tzw. dyrektywa DAC7), która ustanawia obowiązek raportowania przez platformy cyfrowe danych dotyczących sprzedawców. Zakres raportowania obejmuje w szczególności dane identyfikacyjne sprzedawcy (imię i nazwisko lub nazwę, adres, numer identyfikacji podatkowej, numer VAT, datę urodzenia – w przypadku osób fizycznych), informacje o liczbie transakcji dokonanych za pośrednictwem platformy, a także o łącznej kwocie wynagrodzenia wypłaconego lub uznanego w danym okresie. Raportowanie danych na podstawie dyrektywy DAC7 odbywa się w ujęciu rocznym i obejmuje okres roku kalendarzowego, przy czym operatorzy platform są zobowiązani do przekazania informacji właściwym organom podatkowym do końca stycznia roku następującego po roku raportowanym. Dane te następnie podlegają automatycznej wymianie pomiędzy administracjami podatkowymi państw członkowskich, co umożliwia identyfikację ewentualnych rozbieżności w zakresie obrotu wynikającego z danych platform i deklaracji podatników. Należy jednak podkreślić, że mechanizm raportowania przewidziany w dyrektywie DAC7 ma w przeważającej mierze charakter następczy. Kontrola prawidłowości rozliczeń podatkowych dokonywana jest bowiem po zakończeniu roku kalendarzowego, już po zrealizowaniu transakcji i często po rozliczeniu należnych danin publicznych przez podatników. Oznacza to,

że choć raportowanie danych umożliwia wykrycie nieprawidłowości ex post, to nie w każdym przypadku pozwala na skuteczne zapobieżenie powstaniu uszczupleń dochodów publicznych, zwłaszcza w sytuacjach, gdy podatnik zaprzestał działalności, zmienił jurysdykcję lub gdy egzekucja zaległości napotyka istotne trudności praktyczne.

Z perspektywy bezpieczeństwa finansów publicznych szczególne znaczenie ma zatem przesunięcie akcentu z wyłącznie następczej kontroli ex post na mechanizmy o charakterze prewencyjnym i bieżącym. Obowiązki raportowe oraz automatyczna wymiana danych stanowią istotny element systemu identyfikacji ryzyk fiskalnych, jednak ich skuteczność w ochronie dochodów publicznych wzrasta dopiero w połączeniu z rozwiązaniami umożliwiającymi wcześniejszy dostęp administracji publicznej do danych transakcyjnych. Jednocześnie model ten prowadzi do zwiększenia roli platform e-commerce jako podmiotów współodpowiedzialnych za prawidłowe funkcjonowanie systemu poboru danin publicznych.

Kwestia odpowiedzialności platform e-commerce stanowi jeden z najbardziej kontrowersyjnych elementów współczesnej debaty regulacyjnej. Z jednej strony platformy nie są formalnie stroną większości transakcji handlowych, z drugiej jednak dysponują realnym wpływem na sposób dokumentowania, raportowania i wykonywania obowiązków publicznoprawnych przez sprzedawców. Ograniczenie ich roli wyłącznie do funkcji neutralnych pośredników coraz częściej okazuje się niewystarczające z punktu widzenia ochrony bezpieczeństwa finansów publicznych.

Analiza obowiązujących i projektowanych regulacji prowadzi do wniosku, że ustawodawca unijny dostrzega pojawiające się ryzyka i zmierza do stopniowego rozszerzania odpowiedzialności platform e-commerce. Platformy coraz częściej traktowane są jako element infrastruktury systemu finansów publicznych, a nie wyłącznie jako prywatni uczestnicy obrotu gospodarczego. Kierunek ten należy ocenić jako konsekwencję strukturalnych zmian w gospodarce cyfrowej oraz próbę dostosowania instrumentów prawnych do rzeczywistego rozkładu ryzyk fiskalnych.

Podsumowanie

Przeprowadzona analiza pozwala stwierdzić, że cyfrowe platformy e-commerce odgrywają coraz istotniejszą rolę w systemie ochrony

bezpieczeństwa finansów publicznych. Skala ich działalności, transgraniczny charakter obrotu oraz centralizacja danych transakcyjnych powodują, że tradycyjne modele poboru danin publicznych, oparte na indywidualnej odpowiedzialności podatników, stają się niewystarczające.

Zwolnienie z cła dla przesyłek o niskiej wartości, mechanizmy opodatkowania VAT w środowisku platformowym oraz rosnące znaczenie danych transakcyjnych stanowią przykłady obszarów, w których ryzyka fiskalne mają charakter systemowy. Reakcja ustawodawcy unijnego, polegająca na stopniowej fiskalizacji platform e-commerce oraz wprowadzaniu instrumentów prewencyjnych, takich jak rozszerzone obowiązki raportowe czy projektowana stała opłata od przesyłek e-commerce, stanowi próbę zmiany podejścia do ochrony dochodu publicznego w kontekście zmieniającej się dynamicznie specyfiki handlu.

W świetle powyższych rozważań należy uznać, że skuteczna ochrona bezpieczeństwa finansów publicznych w warunkach cyfryzacji handlu wymaga dalszego rozwoju regulacji uwzględniających rzeczywistą rolę platform e-commerce jako istotnych uczestników systemu finansów publicznych. Kluczowe znaczenie ma przy tym nie tylko zakres obowiązków informacyjnych i raportowych nakładanych na te podmioty, lecz również możliwość weryfikacji mechanizmów gromadzenia i przetwarzania danych transakcyjnych, w tym oceny szczelności systemów informatycznych platform oraz ich odporności na nadużycia i manipulacje. Bez zapewnienia rzetelności i integralności danych źródłowych nawet najbardziej rozbudowane obowiązki raportowe mogą okazać się niewystarczające z punktu widzenia ochrony dochodów publicznych. Jednocześnie kierunek ten powinien uwzględniać potrzebę zachowania równowagi pomiędzy efektywnością fiskalną a zasadami pewności prawa i proporcjonalności obciążeń, tak aby nowe rozwiązania regulacyjne nie prowadziły do nadmiernego obciążenia legalnej działalności gospodarczej ani do nieuzasadnionego przenoszenia kosztów systemowych na konsumentów końcowych.

Literatura

1. Bełdzikowski, M., Mioduszewski, M., Mudrecki, A., Wiatrowski, R. (red.). (2024). *VAT w erze cyfryzacji.* Wydawnictwo Akademii Leona Koźmińskiego w Warszawie.

2. Dmoch, W., Kołodziej, B., Mioduszewski, M., Mudrecki, A. (red.). (2022). *Harmonisation of VAT in the European Union: Present and Future*. Wydawnictwo Akademii Leona Koźmińskiego w Warszawie.
3. Europejski Trybunał Obrachunkowy. (2019). *Sprawozdanie specjalne 12/2019. Handel elektroniczny – wiele problemów związanych z poborem podatku VAT i należności celnych czeka na rozwiązanie*. Pobrano z: https://op.europa.eu/webpub/eca/special-reports/e-commerce-12-2019/pl/ (dostęp: 20.03.2026).
4. Główny Urząd Statystyczny. (2025). *Dynamika sprzedaży detalicznej w listopadzie 2025 r.* Pobrano z: https://stat.gov.pl/obszary-tematyczne/ceny-handel/handel/dynamika-sprzedazy-detalicznej-w-listopadzie-2025-r-,14,132.html (dostęp: 20.03.2026).
5. Grześkiewicz, W. (2018). Wpływ zaległości budżetowych na bezpieczeństwo finansowe budżetu państwa, *Prawo Budżetowe Państwa i Samorządu, 6*(3), 45-67. https://doi.org/10.12775/PBPS.2018.016
6. Hanusz, A. (red.). (2019). *Prawo finansowe. Wybrane zagadnienia*. Warszawa: Wydawnictwo Sejmowe.
7. Komisja Europejska. (2025). *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2025) 37 final*. Pobrano z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0037 (dostęp: 20.03.2026).
8. Małecka-Ziembińska, E. (red.). (2023). *Oszustwa związane z VAT w dobie pandemii i cyfryzacji gospodarki.* Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.
9. Merkx, M. (2022). Platform liability: an efficient and fair collection model for VAT? *VAT Challenges and opportunities in the new digital economy*. EUR Research Information Portal.
10. OECD. (2019). *The Role of Digital Platforms in the Collection of VAT/GST on Online Sales*. Pobrano z: https://www.oecd.org/en/publications/the-role-of-digital-platforms-in-the-collection-of-vat-gst-on-online-sales_e0e2dd2d-en.html (dostęp: 20.03.2026).

11. Rada Unii Europejskiej i Komisja Europejska. (2025). *E-commerce: 150 EUR customs duty exemption threshold to be removed as of 2026*. Pobrano z: https://taxation-customs.ec.europa.eu/news/e-commerce-150-eur-customs-duty-exemption-threshold-be-removed-2026-2025-11-13_en (dostęp: 20.03.2026).

Łukasz Stelmaszczyk[1]

Menedżerska Akademia Nauk Stosowanych w Warszawie

https://doi.org/10.29316/9788368103359_17

WIRTUALNY PIENIĄDZ – NOWE MOŻLIWOŚCI I ZAGROŻENIA

VIRTUAL CURRENCY – NEW OPPORTUNITIES AND THREATS

Streszczenie

Wirtualny pieniądz jest ważnym zagadnieniem we współczesnej gospodarce, powiązanym z bezpieczeństwem państwa. Rozwój nowych technologii informatycznych zmienia oblicze finansów, na poziomie gospodarstw domowych, przedsiębiorstw i struktur państwowych. W niniejszym opracowaniu uwagę skupiono na kwestiach takich, jak systemy bankowości elektronicznej, wirtualny pieniądz, nowe sposoby zdalnego przesyłania pieniędzy, jak również ich znaczenie dla nowoczesnej gospodarki. Następnie scharakteryzowano pojęcie pieniądza oraz przedstawiono wpływ powyższych na współczesną ochronę przepływu i przechowywania pieniędzy. Celem rozdziału jest przedstawienie wagi zapewnienia ochrony wirtualnego pieniądza jako kluczowego czynnika gospodarczego bezpieczeństwa państwa, dotyczącego sfery prywatnej i publicznej. Głównym problemem badawczym jest pytanie: jaka jest rola wirtualnego pieniądza w bezpieczeństwie państw i organizacji?

[1] https://orcid.org/0009-0004-4149-6820, e-mail: l.a.stelmaszczyk@wp.pl

Niniejsze opracowanie powstało w oparciu o teoretyczne metody badawcze takie, jak analiza, synteza, wnioskowanie oraz abstrahowanie. Dla pełnego zobrazowania prezentowanych kwestii wykorzystano literaturę przedmiotu.

Słowa kluczowe: cyberbezpieczeństwo, wirtualny pieniądz, bankowość internetowa, Internet, współczesne zagrożenia, bezpieczeństwo państwa

Abstract

Virtual money is a significant issue in the contemporary economy, linked to national security. The development of new information technologies is transforming finance at the level of households, enterprises, and state structures. This study focuses on issues such as electronic banking systems, virtual money, new methods of remote money transfer, and their importance for the modern economy. The concept of money is then characterized and its impact on the contemporary protection of money flow and storage is presented. The aim of this chapter is to demonstrate the importance of ensuring the protection of virtual money as a key factor in the economic security of the state, affecting both the private and public spheres. The main research problem is: what is the role of virtual money in the security of states and organizations? This study is based on theoretical research methods such as analysis, synthesis, inference, and abstraction. The literature on the subject was used to fully illustrate the issues presented.

Keywords: cybersecurity, virtual money, online banking, Internet, modern threats, state security

Wstęp

Przechodzenie do świata wirtualnego kolejnych aspektów działalności człowieka nie ominęło również pieniędzy. Środki płatnicze towarzyszyły ludzkiej cywilizacji od najdawniejszych czasów. Plemienne społeczności bazowały na handlu wymiennym, jednak, z biegiem lat pojawiły się środki płatnicze stanowiące poprzednik obecnego pieniądza. Poprzez futra zwierząt (np. sobole), muszle, metale (miedź, srebro, złoto), środki płatnicze miały zawsze kilka wspólnych cech (Dylewski, 2011, s. 11). Jedną z nich jest możliwość w miarę swobodnego przesyłania pieniądza, często na duże odległości. Złote i srebrne monety, futra niedźwiedzi i muszle cauri, można było przewozić konno, zaprzęgiem, saniami, łodzią i przenosić pieszo. Kolejną

cecha pieniądza jest jego wartość, najlepiej, jeśli dany środek płatniczy jest jak powszechnie uznawany przez wszystkie kraje, w których obowiązuje dana waluta. Bizantyjskie, arabskie, francuskie, węgierskie, hiszpańskie czy nawet brytyjskie monety były uznawane zarówno w kraju wybicia jak i na terenie innych państw o różnym stopniu rozwoju cywilizacyjnego i rozmaitym stosunku do kraju emitenta (Harrison, 2022).

Wirtualny pieniądz spełnia powyższe cechy, co jednak nie wyklucza istnienia szeregu zagrożeń od jakich wolne były tradycyjne nośniki wartości w rodzaju srebrnych groszy, złotych dukatów czy pęków skór sobolich lub kłów słonia. Stary pieniądz w wymiarze materialnym potrzebuje odpowiednich warunków do przechowywania, by zachować swoja wartość. Banknoty papierowe muszą być złożone w miejscu suchym, ciepłym i być zabezpieczone przed ogniem, czy też przed promieniami słonecznymi. Monety są bardziej odporne na wilgoć, jednak ich waga wymaga większych nakładów przy ich przewożeniu. W obecnych czasach największe nominały pięćset, dwieście, sto, pięćdziesiąt, dwadzieścia i dziesięć złotych występują na obszarze Polski w postaci papierowych banknotów. Powyższy układ sprawia, że monety obiegowe Narodowego Banku Polskiego mają niskie wartości jednostkowe, kolejno: pięć złotych, dwa złote, jeden złoty oraz wartości wynoszące od pięćdziesięciu do jednego grosza. Zważywszy na nadmienione, większość transakcji pieniężnych w postaci gotówkowej odbywa się przy użyciu banknotów papierowych (Dylewski, 2011, s. 310). W celu zabezpieczenia wirtualnego pieniądza należy odpowiednio chronić sieci informacyjne, które są podstawą dla przesyłania zapisów księgowych internetowych transakcji (Aleksandrowicz, 2016, s. 5).

Powstanie wirtualnego pieniądza

Wirtualny pieniądz pojawił się na świecie dzięki rozpowszechnieniu się komputerów osobistych PC (personal computer) na przełomie lat siedemdziesiątych i osiemdziesiątych dwudziestego wieku. W roku 1977 spółka Apple wprowadziła do masowej sprzedaży komputery stacjonarne. 12 sierpnia 1981 w Nowym Jorku w hotelu Astoria kolejna amerykańska firma IBM zaprezentowała komputer osobisty, zmieniając technologiczne oblicze milionów gospodarstw domowych. W tym samym czasie, czyli na początku lat osiemdziesiątych dwudziestego wieku, cztery banki działające

na obszarze USA wprowadziły bankowość elektroniczną poprzez instalowanie oprogramowania na komputerach domowych swych klientów. Użytkownicy bankowości elektronicznej uzyskali dostęp do swych kont bankowych, mogli sprawdzać stan konta, dokonywać przelewów i płacić w około 17 tysięcy sklepów.

W Europie w 1983 roku bankowość elektroniczna pojawiła się dzięki Nottingham Building Society, która we współpracy z Bank of Scotland wprowadziła usługę Homelink w Wielkiej Brytanii. W następnych latach bankowość elektroniczna pojawiła się w Finlandii i całej Skandynawii. W pierwszym okresie bankowość elektroniczna odbywała się poprzez sieć telefoniczna i telewizję handlową. Rozwój Internetu przyczynił się do zwiększenia rzesz użytkowników bankowości elektronicznej. Z początkiem lat dziewięćdziesiątych dwudziestego wieku wraz z pojawieniem się przeglądarek internetowych pozwalających na dostęp do stron internetowych. Graficzny interfejs pozwalał na czytelne odkrywanie zasobów internetowych. W tym czasie (lata dziewięćdziesiąte dwudziestego wieku) władze państwowe pozwoliły na wykorzystanie z Internetu do celów biznesowych. Pierwszy bank, który umożliwił swoim klientom (dzięki Internetowi), wirtualny dostęp do rachunku to kalifornijski bank La Jolla, a było to w 1994 roku. Pierwszy na świecie, całkowicie internetowy bank powstał w 1995 roku, w Nowym Jorku w USA. Był to Security First Network Bank. Mając na uwadze bogacenie się społeczeństwa i rozwój światowego biznesu można stwierdzić, że od końca dwudziestego wieku, do czasów współczesnych bankowość elektroniczna wpłynęła korzystnie na przepływ kapitału, transfer technologiczny, wymianę towarową i handel międzynarodowy (Krzysztoszek, 2017, s. 6).

W procesie globalizacji oprócz handlu i technologii ważny jest też przepływ ludzi. Globalne przelewy internetowe i możliwość zakupu biletu lotniczego on-line zachęcają do podróżowania. Osoba z Europy podróżując po Azji może korzystać ze swojej karty płatniczej czy karty kredytowej. Analogicznie, podróżnik z kraju azjatyckiego, jeśli korzysta z powszechnie uznawanej karty kredytowej, może płacić za restauracje, hotele, przejazdy i wejścia do muzeów. Budowa biznesu na skale globalną jest łatwiejsza za pomocą bankowości internetowej (Borcuch, 2007, s. 10). Przesyłanie pieniędzy do centrali przedsiębiorstwa z oddziałów zagranicznych pozwala zminimalizować ryzyko perturbacji w prowadzeniu biznesu. W przypadku

zawirowań politycznych, wojen, epidemii, kataklizmów naturalnych w rodzaju powodzi, czy chociażby wybuchu wulkanu, można błyskawicznie przenieść środki pieniężne z zagrożonego obszaru do innego oddziału, lub kraju macierzystego korporacji. W razie potrzeby doinwestowania przedsiębiorstwa można uzyskać pomoc od innych firm, banków zagranicznych lub od centrali korporacyjnej, z zaznaczeniem, że wszystkie te podmioty mogą być fizycznie zlokalizowane poza granicami państwa, w którym znajduje się firma potrzebująca dodatkowych środków pieniężnych. W obszarze handlu istnienie bankowości elektronicznej działającej cała dobę jest wielkim ułatwieniem zarówno dla przedsiębiorstw jak i dla pojedynczych kupców czy klientów indywidualnych.

Szybkie rozpowszechnienie wirtualnego pieniądza w Polsce

Na polskim rynku bankowym 14 października 1998 roku Powszechny Bank Gospodarczy z siedzibą w Łodzi uruchomił pierwszy wirtualny oddział dla klientów indywidualnych i małych firm. W 1999 roku Powszechny Bank Gospodarczy został przejęty przez Bank Pekao. Dzięki temu przekształceniu pojawił się internetowy rachunek Eurokonto WWW. W tym samym roku, działalność w Internecie rozpoczęły dwa inne banki: Wielkopolski Bank Kredytowy i Bank Przemysłowo-Handlowy (Bank BPH). Sławomir Lachowski piastując stanowisko wiceprezesa Powszechnego Banku Gospodarczego w Łodzi (PBG S.A.), wprowadził w 2000 roku bankowość elektroniczną do użytku, udostępniając ją dla swoich klientów. W wyniku prac zespołu Sławomira Lachowskiego powstał mBank s.a. – pierwszy polski detaliczny bank internetowy. Wspomniany bank, zainicjował swoją działalność z dniem 26 listopada 2000 roku.

Przykład sukcesu rynkowego mBanku zapoczątkował lawinowy wzrost klientów bankowości internetowej. Na początku XXI wieku z e-bankowości w Polsce korzystało około 50 tysięcy użytkowników (Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych, Dz.U. Nr 169, poz. 1385 ze zm.). W następnych latach klienci wirtualnej bankowości przekroczyli liczbę pół miliona, zachowując tendencję wzrostową. MBank dzięki stałemu rozwojowi oraz podążaniu za duchem czasu a przede wszystkim, inwestowani w nowoczesne technologie, stał się trzecim bankiem internetowym w Europie i piątym na świecie. Bank PKO BP S.A. od 2002

roku przejął bank Inteligo, dzięki temu bankowość internetowa zaczęła być obecna w strukturach jednego z największych banków w Polsce. W 2007 roku, firma Apple przedstawiła swój sztandarowy projekt - smartfon iPhone. To urządzenie łączyło w sobie funkcje telefonu i przenośnego komputera. W rok później, bankowość internetowa stała się dostępna przy użyciu smartfonów dla klientów banku PKO BP który, jak wzmiankowano przejął aktywa banku Inteligo. W celu technicznego połączenia telefonów komórkowych z wirtualną bankowością zastosowano system Android stworzony przez amerykańskiego globalnego potentata Google (Gawrychowski, 2016, s. 105). W obecnych czasach, każdego dnia zarówno starsze, jak i młodsze pokolenie powszechnie posługuje się telefonami komórkowymi z dostępem do Internetu. Możliwość wysyłania przelewów przez całą dobę, za pomocą telefonu dodatkowo otwiera łatwą ścieżkę dla dokonywania zakupów, płacenia za bilety komunikacji miejskiej, wizyty w restauracjach, punktach usługowych (salony fryzjerskie, solaria), bez posiadania przy sobie fizycznej gotówki. Powyższy wachlarz możliwości zachęca do aktywności turystycznej, towarzyskiej i gospodarczej. Zwiększenie mobilności społecznej jest impulsem do tworzenia coraz nowocześniejszych technologii. Wyzwaniem nie jest obecnie poziom technologii, lecz poziom rozwoju technologicznego społeczeństwa, ponieważ zwiększona mobilność wywołuje mieszanie się ludzi pochodzących z odmiennych kręgów kulturowych różniących się religią, obyczajowością, zamożnością, tradycją, stosunkiem do kobiet i rodziny, językiem i planami na przyszłość.

Zagrożenia jakie niesie z sobą wirtualny pieniądz

Społeczeństwo można łatwo kontrolować poprzez śledzenie wirtualnych transakcji bankowych. Łatwość płatności internetowych wykonywanych za pomocą telefonów komórkowych jest wielką pokusą by ograniczyć transakcje gotówkowe. Wiele banków i rządów krajowych sprzyja i dąży do ograniczenia obiegu gotówkowego na rzecz zwiększenia roli bankowości internetowej. Wywiady mogą śledzić miejsce przebywania każdej osoby wykonującej płatności za pomocą telefonu komórkowego na całym świecie. Nawet najmniejsze zakupy paliwa na stacji benzynowej czy zakup chleba w sklepie osiedlowym zostaną zarejestrowane i zapisane w historii konta internetowego.

Każde zatrzymanie dostawy prądu elektrycznego może wywołać blokadę w handlu i ograniczenia w dostępie do swych wirtualnych kont bankowych przez miliony użytkowników. Awarie serwerowni mogą zniszczyć historie transakcji giełdowych i bankowych i zaburzyć handel w Internecie. Od lat siedemdziesiątych dwudziestego wieku zaczynają się pojawiać kradzieże pieniędzy z banku przy wykorzystaniu nowoczesnej techniki. W 1973 roku w Nowym Jorku, Dime Savings Bank stracił dwa miliony dolarów w związku kradzieżą jaka został przeprowadzona przy użyciu systemu teleinformatycznego. Od tej chwili przestępcy nie musieli przeprowadzać napadów na bank wedle starego wzoru, w myśl którego przestępcy wchodzą do budynku banku i poprzez włamanie lub zastraszenie obsługi przejmują gotówkę lub papiery wartościowe. Rozwój technologii zapoczątkował przestępstwa bankowe które nie wymagały obecności kryminalistów w siedzibie instytucji finansowej. Zwiększyło się bezpieczeństwo osobiste pracowników banku, podobnie zmniejszyło się ryzyko uszczerbku dla zdrowia wśród złodziei, gdyż wcześniej ochrona banku lub wezwany oddział Policji mógł podczas walki zranić lub zabić przestępców. Jednocześnie w związku z pojawieniem się nowych sposobów na kradzież pieniędzy, środki zgromadzone na rachunkach bankowych stały się bardziej zagrożone. Władze banków w odpowiedzi na powstanie nowych zagrożeń, wprowadziły nowe procedury bezpieczeństwa informatycznego, skupiając się na uszczelnieniu systemu dostępu do kont elektronicznych.

First National Bank of Chicago stracił siedemdziesiąt milionów dolarów w 1988 roku w wyniku działania zorganizowanej grupy kryminalistów działającej w cyber przestrzeni. Narzędziem przestępstwa nie był już pistolet ani łom lub wytrych. Przestępcy posłużyli się telefonem, za którego pomocą potwierdzili przelewy bankowe z rachunków paru spółek np. przedsiębiorstw lotniczych (United Airlines) i finansowych (Merrill Lynch). Autoryzowanie przelewów odbywało się przez połączenie telefoniczne. Złodzieje znając procedury bankowe za sprawą pracowników banku podszyli się pod osoby uprawnione do telefonicznego potwierdzania przelewów. Skradzione pieniądze odnalazły się na kontach Citibanku i Chase Manhattan Banku. Pieniądze zostały odnalezione, zanim zostały przesłane do Austrii. Następnym krokiem był pełnoprawny atak hackerski przeprowadzony przez organizację kierowana przez Władimira Lewina. W 1994 roku członkowie tej kryminalnej grupy włamali się do zasobów komputerowych Citibanku skąd

ukradli dane klientów wraz z hasłami do kont. Złodzieje ukradli łącznie 3,7 miliardów dolarów w ciągu kilku tygodni. Przejęte środki pieniężne trafiły na rachunki w bankach zlokalizowane w USA, Holandii, Finlandii, Izraelu i Niemczech. Władze Citibanku zawiadomiły o kradzieży FBI (Federalna Agencja Bezpieczeństwa).

W wyniku intensywnego śledztwa udało się aresztować członków szajki, kiedy przychodzili do banków celem wypłacania pieniędzy. Po serii ataków hackerskich instytucje finansowe i duże przedsiębiorstwa wzmocniły swoja ochronę cybernetyczną, co sprawiło, że przestępcy nie skupiają się na dużych instytucjach. Kluczem do powodzenia oszustwa w przestrzeni wirtualnej jest pozyskanie danych wrażliwych. Phishing to metoda kradzieży stosowana w cyberprzestrzeni, polegająca na pozyskaniu danych klientów banków poprzez podszywanie się pod osobę godną zaufania lub organizację. Wiadomości wysyłane rzekomo przez pracowników banków lub urzędy państwowe w rodzaju Zakładu Ubezpieczeń Społecznych lub Urzędu Skarbowego stanowią poważne zagrożenie. Posiadając login i hasło do konta bankowego przestępcy są w stanie wejść na konto ofiary a dodatkowo mając dostęp do jednorazowego hasła uwierzytelnianego są w stanie dokonywać przelewów i nawet zaciągać pożyczki (Bednarczyk, 2020, s. 6). Ważnym aspektem działalności cyberprzestępców jest współpraca z pracownikami banków, dzięki którym kryminaliści mogą dokładnie wybierając cel kradzieży typując osoby majętne, posiadające znaczne kwoty pieniędzy na kontach bankowych. Dodatkowy kryterium wyboru może być wiek potencjalnej ofiary. Osoby starsze zazwyczaj mają mniej biegłe w obsłudze nowoczesnych urządzeń technicznych, stając się bardziej podatnymi na zabiegi internetowych oszustów. Tworzenie wirusów komputerowych i złośliwego oprogramowania jest kolejnym sposobem na dokonanie kradzieży w Internecie.

Przejmując kontrolę nad kontem ofiary, hackerzy mogą dowolnie dysponować środkami pieniężnymi, zaciągać pożyczki i zmieniać hasła dostępowe. W przypadku kont przedsiębiorstw próba przejęcia konta może odbywać się za pomocą podawania się oszustów za wysoko postawionych przedstawicieli kontrahentów lub klientów. Zdarza się, że pracownik chcący zaradzić pojawiającemu się kłopotowi, w rzeczywistości wchodząc w rolę nieświadomego pomocnika złodziei, chcących poznać loginy i hasła firmowe by dokonać kradzieży. W przypadku osób chcących wykazywać się w pracy ponad przeciętną efektywnością, istnieje ryzyko zlekceważenia

zasad bezpieczeństwa i poufności danych na rzecz zwiększenia wydajności przedsiębiorstwa (Kubiak, Lizińska, 2025, s. 5). Chęć otrzymania awansu i podwyżki jest bardzo kuszącą perspektywą, by nie stanowiła szansy na osiągniecie powodzenia w oszustwach internetowych, co skrzętnie wykorzystują hackerzy atakując banki i przedsiębiorstwa (Szelągowska, Iwanicz-Drozdowska, Zawadzka, Jaworski, 2017, s 104).

Pełna transparentność operacji bankowych poprzez zapis każdego przelewu, wszystkich zakupów, nawet takich opiewających na niskie kwoty i dotyczące trywialnych spraw w rodzaju kupna chleba, gazety czy paliwa na stacji benzynowej czyni z bankowości wirtualnej sprawne narzędzie wywiadowcze. Rządy państw i właściciele banków mogą dokładnie prześledzić powiązania zawodowe i towarzyskie, trasę podróży, ulubione miejsca i preferencje zakupowe każdego człowieka korzystającego z bankowości wirtualnej. Sprawny profiler, śledczy czy wywiadowca analizując bilingi rachunku bankowego jest w stanie poznać wiele szczegółów z życia danej osoby. Oczywistym i obrazowym przykładem jest posłużenie się kryterium zakupu alkoholu w sklepach i lokalach gastronomicznych.

W celu osiągniecia powodzenia w akcji szpiegowskiej lub działaniu terrorystycznym ważne jest wybranie informatora lub współpracownika. Osoby często kupujące alkohol z dużą dozą prawdopodobieństwa wykazują się ponad przeciętną towarzyskością lub cierpią na chorobę alkoholową, pozostając pod wpływem nałogu. Pozyskanie takiego człowieka do własnych celów jest dużo łatwiejszym zadaniem dla wywiadu wrogiego państwa czy grupy terrorystycznej niż w przypadku człowieka zdrowego posiadającego silniejsze mechanizmy samokontroli własnego zachowania. Skrupulatne śledzenie wydatków obserwowanej osoby może przynieść wiele innych cennych wywiadowczo spostrzeżeń. Wydatki na restauracje, drogie hotele, biżuterię, spa, salony masażu, wycieczki zagraniczne mogą sugerować istnienie romansu w jakim znajduje się obserwowana postać. Jeśli dodatkowo jest to nieformalny związek, współistniejący z oficjalnym stadłem małżeńskim lub inną stałą relacją to dana informacją jest wysoko uplasowana na drabinie możliwego szantażu.

Kolejnym faktem mogącym wyniknąć z właściwej segregacji przelewów i wpłat oraz płatności jest przyjmowanie korzyści majątkowych będących przekupstwem lub wręcz dokonywanie samodzielnie kradzieży. Jeżeli wydatki nie odpowiadają osiąganym poborom w zestawieniu miesięcznym

lub rocznym, jest to ważna wskazówka dla zbadania prawdziwych źródeł środków finansowych obserwowanego człowieka. W ujęciu rocznym przy dodatkowych danych przeczących otrzymaniu podwyżki lub spadku przez obserwowaną postać lub osobę z jej najbliższego kręgu rodzinno- towarzyskiego nagłe zwiększenie wydatków powinno obudzić uzasadnione podejrzenie. Samo wzięcie kredytu i pozostawanie zadłużonym przez dłuższy czas bez wyraźnych powodów może prowadzić do uznania danego człowieka za utracjusza lubiącego rekompensować własne braki lub porażki życiem ponad własny stan majątkowy. Często dla pozyskania wpływu na ustosunkowanego człowieka będącego pracownikiem służb mundurowych, wymiaru sprawiedliwości, instytucji finansowych, firmy energetycznej czy ważnego urzędu wystarczy sama groźba ujawnienia wstydliwych szczegółów życiorysu, wykrytych poprzez sprawdzenie transakcji bankowych wykonanych w systemie informatycznych, tworzących świat wirtualnego pieniądza. Ukrywany nałóg czy choroba mogą być wykryte poprzez odczytanie przelewu skierowanego do ośrodka leczenia uzależnień lub prywatnej kliniki. Dla ludzi piastujących ważne stanowiska w prywatnych przedsiębiorstwach lub administracji rządowej ochrona własnego dobrego imienia może być cenniejsza od wierności krajowi czy lojalności korporacji (Kubik, 2024). Ujawnienie zdrady małżeńskiej lub kradzieży środków publicznych czy należących do przedsiębiorstwa załamało by karierę wielu wpływowych ludzi. Nawet jeśli nie ponieśliby konsekwencji karnych to zła sława jak otoczyłaby ich osoby w przestrzeni publicznej spowodował a by konieczność ustąpienia ze stanowiska za sprawą zakulisowych nacisków przełożonych zaniepokojonych szarganiem dobrego imienia instytucji. Obawa przed społecznym linczem w przypadku celowego przecieku hańbiących wiadomości do mediów, może stanowić decydujący czynnik stanowiący przyczynę, dla której wiele ważnych urzędów państwowych i międzynarodowych instytucji (Kunica, 2025) i przedsiębiorstw jest ciągle infiltrowana przez wrogie wywiady innych państw i grupy terrorystyczne. Jeśli przestępcy, szpiedzy obcych państw, terroryści wejdą w posiadanie danych bankowych mogą mieć dostęp do wiedzy zarezerwowanej dla służb państwowych. W celu przeciwdziałania przestępczości zorganizowanej i globalnemu terroryzmowi wszelkie przelewy środków pieniężnych powyżej kwoty piętnastu tysięcy euro są rejestrowane przez polski sektor bankowy z jednoczesnym powiadamianiu służb skarbowych i Policji oraz służb wywiadowczych (Czowalla, 2025).

Świat przestępczy nieustannie poszukuje nowych dróg obejścia prawa i działalności poza oficjalnymi normami. Tak zależność występuje również w przypadku systemu bankowego obracającego wirtualnymi pieniędzmi. W sytuacji, kiedy nie przestępcy nie mogą korzystać z oficjalnego systemu bankowego, pozostają im do dyspozycji alternatywne systemy obrotu pieniężnego. Przykładem takiego nieformalnego układu finansowego jest arabski system hawala, będący skupiskiem „niewidzialnych banków" (Nadolny, 2021). W powyższym systemie w jednym miejscu na świecie człowiek przekazuje gotówkę pośrednikowi, który to pośrednik za pomocą wiadomości e mail, rozmowy telefonicznej, wpisu na portalu społecznościowym lub komunikatorze internetowym zleca wypłatę środków w innym, niejednokrotnie odległym miejscu na świecie. Wypłata pieniędzy odbywa się za pomocą hasła. Nie ma potrzeby podawania imienia i nazwiska żadnej ze stron transakcji. Bez podpisywania przelewów nie można zidentyfikowania ilości przekazywanych kwot, podobnie jak nadawców i odbiorców pieniędzy. Przelew nie jest rejestrowany w żadnym systemie bankowym, nie podlega nadzorowi urzędów skarbowych, jest wolny od opodatkowania i nie podlega nadzorowi służb państwowych. Wszystkie powyższe cechy sprawiają, że z hawali korzystają organizacje przestępcze i terrorystyczne. Ten nieformalny system bankowy jest bardzo popularny w Indiach, Pakistanie i Afganistanie. W krajach, w których nie ma rozwiniętego rynku bankowego Somalia, Jemen z uwagi na niski poziom gospodarczy i długotrwałe wojny domowe i zewnętrzne hawala jest podstawą wirtualnego obiegu pieniężnego. W Ameryce Północnej i Europie ten alternatywny system został wprowadzony przez przybyszy z obszarów Azji stanowiących emigrację zarobkową i socjalną. System hawala stanowi platformę finansową z której korzystają często przestępcy i terroryści. We Wrocławiu w 2020 roku zatrzymano dwóch obywateli Iraku podejrzewanych o finansowanie bojowników Państwa Islamskiego działających na terenie Iraku i Syrii. Finansowanie odbywało się przy pomocy nieoficjalnego systemu hawala (Żaryn, 2020).

Niestosowanie się przybyszy z Afryki lub Azji (głownie Bliski Wschód, Indie, Pakistan) do standardów zachowania przyjętych w Europie lub Ameryce Północnej jest powszechnie znanym zjawiskiem. Powyższe alternatywne systemy finansowe w rodzaju hawali doskonale odzwierciedlają znaczne różnice kulturowe wśród przybyszy z globalnego południa. Osoby nie przyjmujące zwyczajów panujących w krajach rozwiniętych,

opierają się procesom integracji oraz pozostają przy własnych obyczajach często wchodząc w konflikt z miejscowymi władzami i miejscową społecznością (Warzecha, 2024).

Przyszłość wirtualnego pieniądza

Ważnym aspektem wirtualnego pieniądza jest świat gier komputerowych, które w związku z rozwojem technologii w coraz doskonalszy sposób imitują prawdziwą rzeczywistość tworząc atrakcyjne, cyfrowe, alternatywne światy równoległe. W społeczności graczy komputerowych podłączonych do całodobowej sieci internetowej waluta jest informacja, znakomicie utworzona fikcyjna postać czy budynek. Wiele osób szczególnie w społeczeństwach krajów rozwiniętych i zamożnych w USA, Europie, Japonii czy Singapurze przykłada dużą wagę do spędzania wolnego czasu w wirtualnej przestrzeni. Przepracowanie, brak więzi rodzinnych, ograniczenie relacji towarzyskich, braki wystarczającego czasu wolnego sprzyjają ucieczkom ludzi do świata wirtualnego. W społeczności graczy, twórców internetowych zamieszczających wpisy i filmy na platformach streamingowych, portalach społecznościowych i medialnych odpowiednikiem pieniądza będzie ciekawa informacja pozwalająca zwiększyć zasięgi oglądalności a tym samym zwielokrotnić zyski poprzez wzmożone zainteresowanie reklamodawców. Wiele osób jest bardzo mocno pochłoniętych przez wirtualną rzeczywistość, dlatego są gotowi na zapłatę, często wysokich kwot za dostęp do platform graczy, rozmaite benefity i rozszerzenie możliwości korzystania z wirtualnej rzeczywistości (Solarz, 2008).

W Indiach wiele gospodarstw domowych korzysta ze złota jako trwałego środka płatniczego, służącego jako zabezpieczenie rodziny poprzez oszczędności w danym metalu szlachetnym. W tradycji Indii posag kobiety wychodzącej za mąż jest wypłacany w złotych przedmiotach (np. biżuterii), ma to wpływ na duże, niesłabnące zapotrzebowanie na posiadanie fizycznego złota przez Hindusów. 8 listopada 2016 roku rząd Indii pod przewodnictwem premiera Narendra Modiego ogłosił wycofanie z obiegu banknotów o nominałach 500 i 1000 rupii, przy jednoczesnym terminie zwrotu wyżej wymienionych banknotów do końca grudnia 2016 roku. Jeśli obywatel Indii zwrócił w banku kwotę większą niż 250 000 rupii (około równowartości 15 tys. złotych w nieaktualnych banknotach wtedy grozi sankcja karna ze

strony urzędu skarbowego w postaci podatku wynoszącego 200% domiaru od hipotetycznie, niezapłaconych podatków. Banknoty, kttóre straciły ważność można było wymienić na nowe jednak w tym przypadku najwyższa kwota wymiany wynosiła 4500 rupii, po uprzednim okazaniu dowodu tożsamości. Podobną reformę walutową przeprowadziły komunistyczne władze w PRL w 1950 kradnąc oszczędności Polaków. Zakazano wtedy posiadania obcych walut, złota i platyny. Wprowadzono denominację według przelicznika 100:1 w przypadku gotówki. Depozyty bankowe, ceny i płace zdenominowano w proporcji 100:3. Wprowadzone zmiany dotknęły przede wszystkim przedsiębiorców i rolników indywidualnych.

Zagrożenie denominacją i niepewność co do polityki monetarnej rządu skłania wielu ludzi do szukania alternatywnych sposobów oszczędzania. Moim zdaniem w następnych latach i dziesięcioleciach złoto, opierając się na wcześniej przytoczonym przykładzie Indii będzie w dalszym ciągu jednym z ważniejszych zamienników pieniądza, również tego wirtualnego. Mając w pamięci denominacje i wymianę banknotów przez banki centralne można mieć uzasadnione obawy o dostępność pieniędzy ulokowanych na kontach internetowych. Podczas światowego kryzysu gospodarczego w 2008 roku wielu klientów banków nie mogło wypłacić pieniędzy z bankomatu lub w oddziale banku ani dokonać przelewu wirtualnego, choć mieli zgromadzone środki na swych wirtualnych rachunkach. Takie ograniczenie dotknęło między innymi klientów banku Icesave (Wypijewska, Kuk, 2008). Wprawdzie obywatele Islandii otrzymali pieniądze od rządu w Reykjaviku, lecz już zagraniczni klienci upadłego, islandzkiego banku pochodzący głównie z Wielkiej Brytanii i Holandii nie mogli liczyć na podobną pomoc. Wedle orzeczenia trybunału Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) rząd islandzki mógł wypłacić pieniądze jedynie własnym obywatelom jacy ucierpieli w wyniku upadku islandzkich banków. Banki stały się niewypłacalne i ogłosiły bankructwo, które przyczyniło się do nacjonalizacji wielu instytucji finansowych. Upadły trzy największe banki Kaupthing, Landsbanki i Glitnir. Wielu ludzi traciło oszczędności przez denominację, zwiększyło się bezrobocie.

Kryzys finansowy był jedną z przyczyn braku zaufania do pieniądza i przeniesienie uwagi inwestorów na nieruchomości. W latach 2015-2027 ceny nieruchomości na Islandii wzrosły o ponad 30%. Wprowadzono bardziej restrykcyjne zasady przyznawania pożyczek, gdyż wielu klientów

banku nie było w stanie spłacić swych zobowiązań kredytowych. Te wydarzenia podważyły zaufanie do banków i do długotrwałej wartości pieniądza, również tego wirtualnego. Uważam, że w przyszłości klienci dalej będą skłonni zakupić nieruchomość jako lokatę kapitału pamiętając o kryzysach finansowych jakie uniemożliwiały podjęcie pieniędzy z wirtualnych kont. W obecnej dobie rozwoju technologii, zwiększenia mobilności i przepływów kapitału można zakupić ziemię, domy lub mieszkania w odległych krajach takich jak Hiszpania (Hass, 2024) .

Kryptowaluty pojawiły się w obiegu w niedawnym czasie, lecz wywarły znaczący wpływ na światowy rynek finansowy, stając się jednym z najlepiej rozpoznawalnych wirtualnych wartości pieniężnych. 3 stycznia 2009 roku powstał blok Genesis zapoczątkowując powstanie kryptowaluty Bitcoin. Kryzys finansowy z 2008 roku objawiający się między innymi upadkiem banków, inflacja i denominacją oraz utratą dostępu do pieniędzy ulokowanych na wirtualnych kontach spowodował powstanie powszechnego zapotrzebowania na nową walutę, dostępną na całym świecie, a przy tym odporną na zawirowania polityczne i gospodarcze (Piotrowska, 2018). Za twórcę całego projektu uważa się anonimowa postać Satoshi Nakamoto, która równie dobrze może być całym zespołem ukrywającym swoje tożsamości pod zbiorczym pseudonimem. W celu pozyskania Bitcoina czyli inaczej wirtualnej monety należy dokonać na komputerze skomplikowanych obliczeń matematycznych, aby potwierdzić transakcję. Następnie transakcja jest oznaczana na liście dotychczasowych obrotów kryptowalutą nazywaną łańcuchem bloków (blockchain). Pierwszy zakup przy pomocy Bitcoina został przeprowadzony 22 maja 2010 roku. W tamtych czasach jeden Bitcoin kosztował około 20 dolaróww, obecnie jeden Bitcoin ma wartość 380 tysięcy złotych (Misztal, 2023). Bitcoin z racji braku nadzoru ze strony banków centralnych i urzędów może być wykorzystywany do płatności w świecie przestępczym. Wszelkie nielegalne towary w rodzaju narkotyków, broni, ukradzionych dzieł sztuki mogą być kupowane za pośrednictwem kryptowalut. Ponadto opłacanie dokonanych przestępstw lub aktów terrorystycznych, również może być dokonywane dzięki kryptowalutom. W tym przypadku unikanie podatków jest tylko jednym z wykroczeń przeciwko prawu. Kradzieże, sabotaż, zamachy terrorystyczne zabójstwa, przemyt to tylko jedne z wielu przestępstw jakie mogą być zlecane i opłacane przez Bitcoina lub inne podobne, alternatywne środki płatnicze (Opitek, Butor-Keller, Kanclerz,

2022). Nawet polska prokuratura zgadza się przyjąć poręczenie majątkowe w Bitcoinach (Rycerski, 2025).

Sposoby na ograniczenie strat w przypadku zatrzymania dostępu do wirtualnego pieniądza

W przypadku braku dostępu do wirtualnego pieniądza może dojść do wielu przestępstw i zaburzeń w funkcjonowaniu społeczeństw. W chwili braku dostępu do wirtualnych przelewów może dość do próby oszustw i spekulacji obliczonych na osiągnięcie znacznych zysków poprzez pośrednictwo w wymianie towarowej (np. poprzez listy zastawne w oparciu o trwałe wartości w rodzaju paliw, drewna, żywności, ziemi, złota itp.).

Przeciwdziałanie spekulacji i oszustwom artykułów pierwszej potrzeby (żywność, leki, paliwo) może odbywać się poprzez korzystanie z rządowych rezerw materiałowych i zastosowanie zakupów kredytowych w odniesieniu do hurtowni, sklepów wielkopowierzchniowych i stacji paliw. W chwili, kiedy nie można dokonywać płatności kartami kredytowymi i dokonywać przelewów internetowych artykuły pierwszej potrzeby powinny być zapewniane przez koordynowaną akcję rządową przy pomocy Wojska Polskiego, Policji i Wojsk Obrony Terytorialnej. Mając na uwadze napięcia społeczne, ryzyko wystąpienia paniki i wzmożenie przestępczości należy wprowadzić zwiększone środki bezpieczeństwa w postaci ochrony sklepów (zwłaszcza wielkopowierzchniowych), banków i punktów wydawania żywności i leków. Największa firma paliwowa w Polsce to Orlen S.A., jest zarządzana przez polski rząd, co jest szczególnie ważne w sytuacjach kryzysowych. Państwo poprzez swoje agendy (NBP, Bank PKO) powinno ułatwić pozyskiwanie gotówki przez obywateli w przypadku awarii systemów bankowości internetowej.

Na wypadek ataku hackerskiego w wyniku, którego klienci banków tracą swoje oszczędności, powinien zadziałać mechanizm Bankowego Funduszu Gwarancyjnego zabezpieczającego depozyty bankowe. Równie istotne są mechanizmy wyśledzenia ukradzionych pieniędzy jakie zostały wysłane z kont klientów do innych banków, często znajdujących się za granicą. Jeśli pieniądze zostały przelane przez hackerów do banków umiejscowionych w krajach, które honorują praworządność i są otwarte na współpracę z organami ścigania (policją, prokuraturą) i władzami banku, który stał się celem

kradzieży. Jeśli działania śledcze zostaną przeprowadzone szybko i sprawnie oraz spotkają się z pomocą zagranicznych banków i wymiaru sprawiedliwości krajów, gdzie złodzieje przelali zagrabione pieniądze jest duża nadzieja na odzyskanie strat. Szybkie działanie sądów sprawia, że środki pieniężne co do których zachodzi uzasadnione podejrzenie, iż pochodzą z przestępstwa zostaną zablokowane. Następnym krokiem jest przeprowadzenie śledztwa w wyniku, którego zostaje wydany wyrok nakładający na bank, do którego trafiły ukradzione pieniądze obowiązek dokonania przelewu zwrotnego. Ważne jest szczegółowe doprecyzowanie z jakiego banku hackerzy ukradli pieniądze by środki zostały przelane na właściwe konta, jeśli mamy do czynienia z wieloma bankami jakie stanowiły stacje pośrednie w zatarciu śladów przestępstwa. Oprócz szybkości działania kluczem do odzyskania pieniędzy skradzionych przez atak hackerski jest umiejętność pracowników banku, którzy są biegli w poruszaniu się w wirtualnym świecie. Mamy tu do czynienia z dwiema stronami konfliktu: hackerami dokonującymi kradzieży oraz informatykami zatrudnionymi przez banki i policję.

Podsumowanie

Wirtualny pieniądz niesie ze sobą zarówno nowe możliwości i zagrożenia. Oprócz łatwości dokonywania zakupów, prowadzenia przedsiębiorstw i podróżowania wirtualny pieniądz wpisuje się w nowoczesny świat przesiąknięty nowymi technologiami. Kontekst społeczny łączy się tutaj z rozwojem technologii. Telefony komórkowe są powszechnie użytkowane przez wszystkie grupy społeczne, a złożoność nowoczesnych telefonów pozwala dokonywać zakupów i przelewów przez całą dobę.

Ataki hackerskie na pieniądze zgromadzone na wirtualnych kontach istnieją od chwili powstania wirtualnej bankowości. W odpowiedzi na zagrożenie przestępstwami internetowymi banki zaczęły wzmacniać zabezpieczenia swych systemów internetowych. Mając na uwadze bezpieczeństwo depozytów bankowych, klienci indywidualni zostali wyposażeni w dodatkowe progi dostępowe, obejmujące zarówno hasła dostępowe jak i dodatkowe hasła wysyłane za pomocą wiadomości SMS. Polska jest w awangardzie wirtualnej bankowości, gdyż zarówno polskie banki jak ich klienci, działaj sprawnie w przestrzeniach Internetu. Pomimo zagrożeń jakie są stale obecnie w przestrzeni internetowej, bankowość wirtualna ciągle się rozwija,

zyskując nowych klientów. Od chwili powstania wirtualnej bankowości zwiększają się zastępy jej użytkowników.

Należy zaznaczyć, że istnieją też alternatywne instrumenty finansowe działające w wirtualnym świecie. Bitcoin i inne kryptowaluty stały się odpowiedzią na potrzebę anonimowości w wirtualnych finansach bez nadzoru państwa i ingerencji władz banków. Pomimo ryzyka niespodziewanej zmiany wartości i oszustw istnieje społeczność mająca zaufanie do kryptowalut. Dokonywanie nielegalnych zakupów i użytkowanie danych instrumentów finansowych przez świat przestępczy to ciemna strona kryptowalut. Alternatywna bankowość w postaci systemu Hawala często służy finansowaniu terroryzmu i unikaniu opodatkowania. Dany system Hawala, podobnie jak kryptowaluty nie podlega nadzorowi urzędów państwowych i banków. Pomimo rozwoju wirtualnego pieniądza, wiele osób na całym świecie wybiera tradycyjne formy oszczędzania. Niesłabnąca popularność złota sprawia, że stare sposoby zachowania swego majątku nie tracą na znaczeniu, pomimo gwałtownego rozwoju cywilizacyjnego. W celu ochrony wirtualnego pieniądza banki wprowadzają szereg zabezpieczeń informatycznych, aby uniemożliwić lub zminimalizować próby kradzieży środków pieniężnych poprzez ataki hackerów.

Władze państwowe są zobowiązane w jak największym stopniu chronić swoich obywateli przed cyberprzestępczością. W razie kryzysu bankowości elektronicznej i ograniczonego dostępu do wirtualnych pieniędzy w wyniku awarii technologicznej, zorganizowanej akcji hackerskiej władze państwowe muszą być gotowe do zapewnienia ładu społecznego i ciągłości zaopatrzenia ludności w artykuły pierwszej potrzeby jak leki, paliwo i żywność oraz szybkiego dostępu do gotówki. Szybkie działania podjęte po ataku hackerskim pozwalają na odzyskanie skradzionych pieniędzy z wirtualnych kont bankowych.

Literatura

1. Aleksandrowicz, T. (2016). *Podstawy walki informacyjnej*. Warszawa: CeDeWu.

2. Harrison, M. (2022). *Niemcy zapłaciły ostatnią ratę odszkodowań za I wojnę światową po 92 latach.* Pobrano z: https://www.bankier.pl/wiadomosc/Niemcy-zaplacily-ostatnia-rate-odszkodowan-za-I-wojne-swiatowa-po-92-latach-8386364.html (dostęp: 20.03.2026).
3. Bednarczyk, P. (2020). Bankowość Internetowa w Polsce. *Zeszyty Naukowe Wydziału Ekonomii i Finansów Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu Studia Ekonomiczne, Prawne i Administracyjne.* Rocznik *2020* (Zeszyt 2), 6-20.
4. Borcuch, A. (2007). *Pieniądz elektroniczny – Pieniądz przyszłości - analiza ekonomiczno-prawna*. Warszawa: CeDeWu.
5. Kunica, M. (2025). *Korupcja w Parlamencie Europejskim. Osiem osób oskarżonych.* Pobrano z: https://businessinsider.com.pl/wiadomosci/korupcja-w-parlamencie-europejskim-huawei-pod-lupa-sledczych/5hyywp2 (dostęp: 20.03.2026).
6. Czowalla, A. (2025). *Od tej kwoty bank powiadomi skarbówkę. Sumują przelewy.* Pobrano z: https://biznes.interia.pl/finanse/news-od-tej-kwoty-bank-powiadomi-skarbowke-sumuja-przelewy,nId,7910612 (dostęp: 20.03.2026).
7. Dylewski, A. (2011). *Historia Pieniądza na Ziemiach Polskich*. Warszawa: Carta Blanca.
8. Gawrychowski, M. (2026). *Banki w sieci*. Pobrano z: https://mowiawieki.pl/templates/site_pic/files/Pewne_jak_w_banku_Historia_zabezpieczen_bankowych_odcinek_8(sierpien_2016).pdf (dostęp: 20.03.2026).
9. Hass, W. (2024). *Coraz chętniej kupujemy domy w Hiszpanii. Padł rekord udziału Polaków w hiszpańskim rynku nieruchomości*. Pobrano z: https://strefainwestorow.pl/artykuly/nieruchomosci/20240904/polacy-hiszpanski-rynek-nieruchomosci-2q24 (dostęp: 20.03.2026).
10. Krzysztoszek, M. (2017). *Bankowość elektroniczna w teorii i praktyce.* Pobrano z: https://www.knf.gov.pl/knf/pl/komponenty/img/Bankow%C5%9B%C4%87%20elektroniczna%20w%20teorii%20i%20praktyce_60154.%20Materia%C5%82y%20dla%20%C5%9Brodowiska%20szkolnego_60154.pdf (dostęp: 20.03.2026).
11. Kubiak, J., Lizińska, J. (2025). *Finanse Przedsiębiorstw*. Warszawa: CeDeWu.

12. Kubik, W. (2024). *Tomasz Szmydt nie planował ucieczki? Sensacyjne doniesienia z Białorusi*. Pobrano z: https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9508675,tomasz-szmydt-nie-planowal-ucieczki-sensacyjne-doniesienia-z-bialorus.html (dostęp: 20.03.2026).
13. Misztal, J. (2023). *14 lat minęło jak jeden dzień. Bitcoin świętuje urodziny*. Pobrano z: https://www.bankier.pl/wiadomosc/Bitcoin-ma-14-lat-8466320.html.
14. Nadolny, D. (2021). *Akt oskarżenia za finansowanie działalności tzw. „państwa islamskiego"*. Pobrano z: https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-za-finansowanie-dzialalnosci-tzw-panstwa-islamskiego (dostęp: 20.03.2026).
15. Opitek, P., Butor-Keller, A., Kanclerz, K. (2022). *Terroryzm, studia, analizy, prewencja.* Pobrano z: https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr4/8_-_artykul8_-_artykul_-_P__Opitek_i_inni.pdf(dostęp: 20.03.2026).
16. Piotrowska, A. I. (2018). *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*. Warszawa: CeDuWu.
17. Rycerski, A. (2025). *Sprawa Red is Bad i poręczenie majątkowe w formie bitcoina. Czy to dopuszczalne?*. Pobrano z: https://www.rp.pl/opinie-prawne/art41841381-adrian-rycerski-poreczenie-w-formie-bitcoina-prokuratura-moze-miec-problem (dostęp: 20.03.2026).
18. Solarz, M. (2008). *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2004-2007*. Pobrano z: https://stat.gov.pl/banki-i-bazy-danych (dostęp: 20.03.2026).
19. Szelągowska, A., Iwanicz-Drozdowska, M., Zawadzka, Z., Jaworski, W. L. (2017). *Bankowość. Instytucje, operacje, zarządzanie*. Warszawa: Poltext.
20. Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych, Dz.U. nr 169, poz. 1385 ze zm.
21. Warzecha, Ł. (2024). *Europoseł PO sprawdził przestępczość wśród imigrantów. I wyraził zaskoczenie*. Pobrano z: https://www.salon24.pl/newsroom/1369095,europosel-po-sprawdzil-przestepczosc-wsrod-imigrantow-i-wyrazil-ogromne-zaskoczenie (dostęp: 20.03.2026).
22. Wypijewska, M., Kuk, M. (2008). *Islandia kolejną ofiarą kryzysu*. Pobrano z: https://www.rp.pl/banki/art16001161-islandia-kolejna-ofiara-kryzysu (dostęp: 20.03.2026).

23. Żaryn, S. (2020). *Zatrzymani przez ABW obywatele Iraku oskarżeni o finansowanie ISIS.* Pobrano z: https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/zatrzymani-przez-abw-obywatele-iraku-oskarzeni-o-finansowanie-isis (dostęp: 20.03.2026).

Ewelina Melaniuk[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103359_18

ROLA WIRTUALNEGO PIENIĄDZA W ROZWOJU GOSPODARKI CYFROWEJ

THE ROLE OF VIRTUAL CURRENCY IN THE DEVELOPMENT OF THE DIGITAL ECONOMY

Streszczenie

Wirtualny pieniądz stanowi istotny komponent infrastruktury gospodarki cyfrowej, jednocześnie generując nowe wyzwania w obszarze cyberbezpieczeństwa. Celem rozdziału jest analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy bezpieczeństwa systemów informatycznych, ochrony transakcji oraz zarządzania ryzykiem cybernetycznym. Badanie oparto na analizie literatury naukowej, raportów zespołów CERT, instytucji nadzorczych oraz dokumentów branżowych. W rozdziale dokonano klasyfikacji form wirtualnego pieniądza, obejmującej kryptowaluty, stablecoiny, waluty wirtualne platform cyfrowych oraz cyfrowe waluty banków centralnych (CBDC), z uwzględnieniem ich podatności na zagrożenia takie jak phishing, malware, ransomware, ataki na giełdy kryptowalut oraz nadużycia

[1] https://orcid.org/0009-0002-9434-6258, e-mail: e.melaniuk@dyd.akademiabialska.pl

związane z kradzieżą kluczy kryptograficznych. Wyniki analizy wskazują, że wirtualny pieniądz przyczynia się do rozwoju gospodarki cyfrowej, lecz równocześnie zwiększa powierzchnię ataku oraz złożoność architektury bezpieczeństwa. Wnioski podkreślają konieczność integracji mechanizmów cyberochrony, w tym kryptografii, monitorowania transakcji, edukacji użytkowników oraz ram regulacyjnych, jako warunku bezpiecznego rozwoju ekosystemów finansów cyfrowych.

Słowa kluczowe: wirtualny pieniądz, cyberbezpieczeństwo, zagrożenia cyfrowe, kryptografia, bezpieczeństwo transakcji, gospodarka cyfrowa

Abstract

Virtual money constitutes a critical component of the digital economy infrastructure while simultaneously introducing new challenges in the field of cybersecurity. The aim of this chapter is to examine the role of virtual money in the development of the digital economy from the perspective of information system security, transaction protection, and cyber risk management. The study is based on a review of academic literature, CERT reports, supervisory authority publications, and industry documents. The chapter provides a classification of virtual money forms, including cryptocurrencies, stablecoins, virtual currencies of digital platforms, and central bank digital currencies (CBDCs), with particular attention to their exposure to threats such as phishing, malware, ransomware, attacks on cryptocurrency exchanges, and abuses related to the theft of cryptographic keys. The findings indicate that while virtual money supports the growth of the digital economy, it also expands the attack surface and increases the complexity of security architectures. The conclusions emphasize the necessity of integrating cybersecurity mechanisms, including cryptography, transaction monitoring, user awareness, and regulatory frameworks, as a prerequisite for the secure development of digital finance ecosystems.

Keywords: virtual money, cybersecurity, digital threats, cryptography, transaction security, digital economy

Wstęp

Wraz z dynamicznym rozwojem technologii informacyjno-komunikacyjnych i cyfryzacją gospodarki tradycyjne formy pieniądza ulegają zasadniczym przemianom. Coraz większe znaczenie zyskują formy pieniądza wirtualnego, obejmujące kryptowaluty, waluty wirtualne w ekosystemach

cyfrowych oraz cyfrowe waluty banków centralnych (Central Bank Digital Currencies, CBDC). Te instrumenty finansowe stają się nie tylko medium wymiany, ale również kluczowym elementem infrastruktury gospodarki cyfrowej, w której transakcje finansowe, handel elektroniczny i usługi finansowe są realizowane głównie w środowisku cyfrowym. Kryptowaluty takie jak Bitcoin czy Ethereum zrewolucjonizowały postrzeganie pieniądza, oddzielając go od formy fizycznej i podkreślając jego cyfrową naturę jako środka wymiany i przechowywania wartości (Ryś, 2023).

Wirtualny pieniądz, zwłaszcza w postaci CBDC, staje się przedmiotem rosnącego zainteresowania banków centralnych i regulatorów na całym świecie. Banki centralne podejmują prace nad cyfrowymi wersjami pieniądza fiducjarnego, które mają potencjał usprawnienia płatności detalicznych i transgranicznych, zwiększenia efektywności systemów płatniczych oraz poprawy inkluzji finansowej. Jednak równocześnie pojawiają się istotne wyzwania w obszarze cyberbezpieczeństwa, integralności systemów, ochrony prywatności oraz ryzyka technicznego (Gasz, Smalara, 2025).

Bezpieczeństwo cyfrowych systemów pieniężnych jest kluczowe dla ich stabilności i zaufania społecznego. Badania wskazują, że wprowadzenie CBDC oraz innych form pieniądza cyfrowego wiąże się z szeregiem zagrożeń cybernetycznych, takich jak kradzież lub przejęcie danych uwierzytelniających, podatności na ataki typu „double spending", denials-of-service oraz naruszenia integralności systemu transakcyjnego (WEF, 2021; IMF, 2024). Jednocześnie infrastrukturę tych systemów mogą stanowić atrakcyjne cele dla cyberprzestępców, co wpływa na konieczność wdrożenia kompleksowych mechanizmów ochronnych, w tym zaawansowanej kryptografii, monitorowania anomalii w czasie rzeczywistym oraz odporności na incydenty (Fed, 2022).

W literaturze podkreśla się również kwestie prawne i regulacyjne związane z emisją i wdrażaniem CBDC oraz kryptowalut, których brak harmonizacji w skali globalnej stanowi barierę dla ich powszechnego przyjęcia oraz efektywnego nadzoru ryzyka (Karpiuk-Wawryszuk, 2023). Ponadto intensywna cyfryzacja systemów finansowych zwiększa powierzchnię ataku, co wymaga od instytucji finansowych i regulatorów sprostania zarówno tradycyjnym, jak i nowym zagrożeniom w cyberprzestrzeni.

Celem niniejszego rozdziału jest analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy cyberbezpieczeństwa

i zarządzania ryzykiem. Podjęto próbę kompleksowego ujęcia tego zjawiska poprzez klasyfikację form wirtualnego pieniądza oraz wskazanie, w jaki sposób ich adopcja wpływa na funkcjonowanie cyfrowych systemów finansowych, a także jakie ryzyka cybernetyczne i organizacyjne są z tym związane. Przyjęte podejście opiera się na przeglądzie literatury naukowej, analizie raportów instytucjonalnych oraz przeglądzie istotnych badań w obszarze finansów cyfrowych i bezpieczeństwa informatycznego.

Znaczenie wirtualnego pieniądza w rozwoju gospodarki cyfrowej

Wirtualny pieniądz, obejmujący kryptowaluty, stablecoiny i cyfrowe waluty banków centralnych (CBDC), odgrywa coraz istotniejszą rolę w transformacji cyfrowej gospodarki. Umożliwia szybkie i bezpośrednie transakcje finansowe, rozwój innowacyjnych modeli biznesowych, zwiększa płynność rynków i wspiera ekspansję globalną przedsiębiorstw (IMF, 2024; Schär, 2021). Poniżej przedstawiono cztery kluczowe obszary wpływu wirtualnego pieniądza na gospodarkę cyfrową: wspieranie zdecentralizowanych finansów (DeFi), tokenizacja aktywów, integracja z płatnościami cyfrowymi i e-commerce oraz wyzwania cyberbezpieczeństwa i zaufania.

Zdecentralizowane finanse (DeFi) stanowią jedno z najważniejszych zastosowań wirtualnego pieniądza. Umożliwiają bezpośrednie transakcje peer-to-peer, bez potrzeby angażowania pośredników bankowych. Eliminuje to koszty pośrednictwa, skraca czas realizacji transakcji oraz zwiększa efektywność systemów finansowych (Schär, 2021).

Platformy takie jak Ethereum i Binance Smart Chain pozwalają tworzyć smart kontrakty – samowykonujące się umowy kodowane w blockchainie – które mogą obsługiwać pożyczki, ubezpieczenia czy wymianę tokenów. Smart kontrakty automatyzują procesy, minimalizując ryzyko błędów ludzkich oraz opóźnień w transakcjach. Przykładem jest protokół Aave, który umożliwia użytkownikom zdeponowanie środków i udzielanie pożyczek bez pośrednictwa banku, z pełną kontrolą nad własnym kapitałem i transparentnym systemem odsetek (Schär, 2021).

W kontekście cyberbezpieczeństwa, DeFi stawia przed uczestnikami rynku wyzwania związane z lukami w smart kontraktach i ryzykiem ataków typu flash loan, które mogą prowadzić do strat finansowych w krótkim

czasie. Dlatego istotna jest integracja mechanizmów audytu kodu, monitoring transakcji i edukacja użytkowników (Raz i in., 2025).

Tokenizacja aktywów realnych stanowi kolejny istotny obszar wpływu wirtualnego pieniądza na gospodarkę cyfrową. Poprzez reprezentowanie fizycznych aktywów, takich jak nieruchomości, dzieła sztuki, obligacje czy papiery wartościowe, w postaci tokenów cyfrowych, możliwe staje się frakcjonowanie własności i zwiększenie płynności rynkowej (OECD, 2024). Przykładem jest projekt tokenizacji nieruchomości w Singapurze (2024), który umożliwił globalnym inwestorom zakup udziałów w lokalnych obiektach komercyjnych. Dzięki tokenizacji inwestorzy mogą nabywać ułamkowe udziały, co znacznie obniża barierę wejścia na rynek nieruchomości i umożliwia łatwiejszą dywersyfikację portfela inwestycyjnego (OECD, 2024).

Tokenizacja wspiera także rozwój cyfrowych rynków kapitałowych, w tym emisji tokenów reprezentujących akcje lub obligacje. Umożliwia przyspieszenie procesu pozyskiwania kapitału, automatyzację rozliczeń i zwiększenie przejrzystości transakcji. Z punktu widzenia bezpieczeństwa cybernetycznego, niezbędne są mechanizmy kryptograficzne chroniące przed manipulacją danymi, zabezpieczanie portfeli cyfrowych i audyt smart kontraktów (ENISA, 2023).

Stablecoiny i CBDC odgrywają kluczową rolę w usprawnianiu płatności cyfrowych, szczególnie w handlu transgranicznym. Pozwalają na szybkie, niskokosztowe i bezpieczne transakcje, co zwiększa efektywność przedsiębiorstw i poprawia doświadczenie klienta (IMF, 2024). Przykładem praktycznego zastosowania jest projekt CBDC w Bahrajnie (Project Dinar), który umożliwił przeprowadzanie transgranicznych płatności w czasie rzeczywistym, skracając czas rozliczenia z kilku dni do kilku minut. Integracja wirtualnego pieniądza z systemami e-commerce pozwala również na wdrażanie nowych modeli biznesowych, takich jak mikropłatności w usługach cyfrowych, subskrypcje w grach online czy tokenizacja lojalności klientów.

W kontekście cyberbezpieczeństwa, systemy płatnicze muszą zapewniać integralność i poufność transakcji, odporność na ataki typu man-in-the-middle oraz skuteczny monitoring sieci w czasie rzeczywistym. CBDC i stablecoiny wprowadzają też nowe wyzwania regulacyjne, wymagając współpracy międzynarodowej w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (FATF, 2022).

W miarę jak wirtualny pieniądz staje się powszechny, rośnie także ryzyko ataków cybernetycznych, błędów w systemach oraz utraty zaufania społecznego (ENISA, 2023). Zagrożenia obejmują kradzież kluczy prywatnych, manipulacje smart kontraktami, ransomware na giełdach kryptowalut oraz ataki typu 51% w zdecentralizowanych sieciach blockchain.

Bezpieczeństwo systemów wirtualnego pieniądza wymaga:

- integracji zaawansowanych technologii kryptograficznych,
- monitoringu transakcji w czasie rzeczywistym i wykrywania anomalii,
- audytów smart kontraktów i zabezpieczeń portfeli cyfrowych,
- edukacji użytkowników w zakresie bezpiecznego korzystania z cyfrowych aktywów,
- regulacji minimalizujących ryzyko oszustw i cyberprzestępczości (Gasz, Smalara, 2025; Raz i in., 2025).

Zaufanie uczestników rynku jest warunkiem rozwoju wirtualnego pieniądza w gospodarce cyfrowej. Bezpieczeństwo, przejrzystość i zgodność regulacyjna są kluczowe, aby wirtualny pieniądz mógł wspierać innowacje, inwestycje i ekspansję cyfrowych usług finansowych.

Zagrożenia cyberbezpieczeństwa w systemach wirtualnego pieniądza

Wprowadzenie wirtualnego pieniądza do gospodarki cyfrowej wiąże się z istotnymi ryzykami w obszarze cyberbezpieczeństwa. Systemy oparte na kryptowalutach, CBDC i platformach cyfrowych zwiększają powierzchnię ataku, stwarzając nowe wyzwania dla instytucji finansowych i użytkowników końcowych.

Podstawowym zagrożeniem są ataki skierowane na infrastrukturę systemów płatniczych i giełd kryptowalutowych. Przykłady obejmują kradzież środków z portfeli cyfrowych w wyniku błędów w smart kontraktach lub luk w zabezpieczeniach giełd (np. atak na platformę Binance w 2022 r., gdzie skradziono kryptowaluty o wartości ok. 6,5 mln USD) (Binance, 2022). Ataki te mogą prowadzić do strat finansowych oraz do utraty zaufania do całego systemu cyfrowych płatności (Kshetri, Bhushal, Pandey, 2022).

Kolejnym istotnym zagrożeniem jest przejęcie kluczy prywatnych użytkowników oraz ataki phishingowe. W cyberprzestrzeni powstają

wyspecjalizowane kampanie malware, które wyłudzają dane uwierzytelniające do portfeli cyfrowych. Przykładem jest kampania „CryptoStealer" z 2023 r., w której zainfekowano setki komputerów i przejęto dostęp do portfeli kryptowalutowych użytkowników (ENISA, 2023).

Wirtualne pieniądze, szczególnie kryptowaluty w sieciach zdecentralizowanych, narażone są na double-spending, czyli próbę wielokrotnego wydania tej samej jednostki cyfrowej. Takie ataki mogą być przeprowadzane przez podmioty kontrolujące znaczną część mocy obliczeniowej sieci (atak 51%), jak miało to miejsce w przypadku kryptowaluty Ethereum Classic (Sayeed, Marco-Gisbert, 2019).

Cyfrowe waluty banków centralnych (CBDC) wprowadzają nowe ryzyka, związane z integracją systemów bankowych z infrastrukturą cyfrową. Problemy techniczne, awarie serwerów oraz błędy w protokołach bezpieczeństwa mogą powodować przerwy w świadczeniu usług płatniczych i ograniczać zaufanie użytkowników. IMF (2024) podkreśla, że wdrażanie CBDC wymaga rygorystycznych testów odpornościowych i ciągłego monitorowania zagrożeń cybernetycznych.

Platformy handlu kryptowalutami i giełdy cyfrowe stają się celem ransomware, które może wymuszać okup w kryptowalutach. Przykład ataku na giełdę w Korei Południowej w 2022 r. pokazał, że złośliwe oprogramowanie może sparaliżować systemy płatnicze i wymusić znaczące straty finansowe (ESET, 2022).

Brak ujednoliconych ram regulacyjnych na poziomie międzynarodowym zwiększa ryzyko wykorzystywania wirtualnego pieniądza do prania pieniędzy, finansowania terroryzmu i działań przestępczych (FATF, 2022). Integracja mechanizmów cyberbezpieczeństwa z polityką regulacyjną jest więc niezbędna, aby zminimalizować ryzyka i zwiększyć odporność systemów (Gasz, Smalara, 2025).

Zagrożenia cyberbezpieczeństwa w systemach wirtualnego pieniądza mają charakter wielowymiarowy: obejmują aspekty techniczne (ataki na infrastrukturę, kradzieże kluczy), operacyjne (błędy integracyjne, niewłaściwe zarządzanie ryzykiem) oraz regulacyjne (niewystarczająca ochrona prawna i brak globalnych standardów). Efektywna adaptacja wirtualnego pieniądza w gospodarce cyfrowej wymaga więc integracji mechanizmów kryptograficznych, monitoringu transakcji, edukacji użytkowników oraz spójnych ram regulacyjnych.

Mechanizmy ochrony i rekomendacje dla cyberbezpieczeństwa w systemach wirtualnego pieniądza

W obliczu rosnących zagrożeń cybernetycznych związanych z wirtualnym pieniądzem konieczne jest opracowanie i wdrożenie kompleksowych mechanizmów ochrony, obejmujących aspekty techniczne i regulacyjne oraz edukacyjne.

Podstawowym elementem ochrony w systemach wirtualnego pieniądza jest wykorzystanie silnych mechanizmów kryptograficznych, takich jak algorytmy szyfrowania klucza publicznego, podpisy cyfrowe i wielopoziomowa weryfikacja transakcji (multi-signature). Systemy CBDC i kryptowaluty powinny również korzystać z protokołów odporności na ataki typu man-in-the-middle, a infrastruktura giełd i portfeli cyfrowych – z zaawansowanych firewalli, systemów wykrywania włamań (IDS/IPS) oraz segmentacji sieci (IMF, 2024; EBA, 2022).

Ważnym mechanizmem ochrony jest ciągłe monitorowanie transakcji w czasie rzeczywistym w celu wykrywania działań nietypowych lub podejrzanych. Systemy oparte na analizie zachowań użytkowników (UBA – User Behavior Analytics) oraz algorytmach sztucznej inteligencji mogą identyfikować próby nieautoryzowanych transferów, ataki phishingowe lub ransomware skierowane na portfele cyfrowe (ENISA, 2023). Przykładem skutecznej implementacji takich rozwiązań jest monitorowanie giełdy Coinbase, która w 2022 r. wykorzystała algorytmy AI do wczesnego wykrycia próby kradzieży środków i zatrzymania ataku.

Ochrona systemów wirtualnego pieniądza wymaga również odporności infrastruktury IT, osiąganej poprzez redundancję serwerów, segmentację sieci i stosowanie technologii chmurowych z geograficznym rozproszeniem danych. Dzięki temu w przypadku awarii lub incydentu cybernetycznego, dostęp do kluczowych funkcji systemu pozostaje zachowany, a ryzyko całkowitej utraty środków minimalizowane (Fed, 2022).

Najczęstszym wektorem ataków są błędy ludzkie, takie jak kliknięcie w złośliwy link w phishingu lub przechowywanie kluczy prywatnych w niechronionych lokalizacjach. Dlatego edukacja użytkowników i personelu instytucji finansowych jest kluczowa. Szkolenia powinny obejmować rozpoznawanie zagrożeń, bezpieczne korzystanie z portfeli cyfrowych, praktyki silnych haseł i uwierzytelniania dwuskładnikowego (2FA) (ESET, 2022).

Skuteczna ochrona cybernetyczna wymaga również spójnych ram regulacyjnych, które narzucają obowiązki w zakresie bezpieczeństwa, raportowania incydentów oraz przeciwdziałania praniu pieniędzy (AML) i finansowaniu terroryzmu (CFT). W Europie ramy MiCA (Markets in Crypto-Assets Regulation) oraz wytyczne FATF stanowią podstawę regulacyjną dla systemów wirtualnego pieniądza, zapewniając równowagę między innowacyjnością a bezpieczeństwem (KarpiukWawryszuk, 2023; FATF, 2022).

Rekomendacje strategiczne dla instytucji:

- integracja rozwiązań bezpieczeństwa w architekturze systemów transakcyjnych i giełd kryptowalut,
- stałe testy penetracyjne i audyty bezpieczeństwa w celu wykrycia luk w systemach,
- współpraca z zespołami CERT i organami nadzoru w celu szybkiego reagowania na incydenty,
- wdrożenie mechanizmów szybkiego backupu i odzyskiwania danych w razie ataku ransomware,
- monitorowanie nowych zagrożeń, w tym ataków wykorzystujących sztuczną inteligencję i automatyzację transakcji.

Bezpieczeństwo wirtualnego pieniądza wymaga wielowarstwowego podejścia, obejmującego kryptografię, monitorowanie transakcji, odporność infrastruktury, edukację użytkowników oraz spójne regulacje. Skuteczna implementacja tych mechanizmów pozwala ograniczyć ryzyko cyberzagrożeń oraz zwiększa zaufanie do systemów cyfrowych i wspiera rozwój gospodarki cyfrowej w sposób bezpieczny i stabilny.

Wnioski

Analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy cyberbezpieczeństwa wskazuje na następujące kluczowe wnioski:

1. Wirtualny pieniądz jako katalizator gospodarki cyfrowej: kryptowaluty, stablecoiny oraz CBDC znacząco wspierają rozwój cyfrowych systemów płatniczych, zwiększają efektywność transakcji oraz

umożliwiają wdrażanie innowacyjnych modeli biznesowych, takich jak DeFi czy tokenizacja aktywów.

2. Wieloaspektowe zagrożenia cyberbezpieczeństwa: systemy wirtualnego pieniądza są narażone na ataki typu phishing, ransomware, kradzież kluczy kryptograficznych oraz manipulację transakcji (np. double-spending). Zagrożenia te podkreślają konieczność integracji mechanizmów ochrony z architekturą systemów finansowych.
3. Znaczenie technologii ochronnych: skuteczna obrona wymaga stosowania zaawansowanej kryptografii, monitorowania transakcji w czasie rzeczywistym, segmentacji infrastruktury i redundancji systemów, a także ciągłego testowania odporności systemów na ataki cybernetyczne.
4. Edukacja i świadomość użytkowników: czynniki ludzkie pozostają jednym z najsłabszych ogniw systemów bezpieczeństwa. Szkolenia, świadomość zagrożeń i praktyki bezpieczeństwa, takie jak uwierzytelnianie dwuskładnikowe i bezpieczne przechowywanie kluczy prywatnych, mają kluczowe znaczenie dla ograniczenia ryzyka.
5. Ramy regulacyjne i nadzór: globalne zróżnicowanie przepisów prawnych stwarza wyzwania dla bezpieczeństwa i stabilności systemów wirtualnego pieniądza. Spójne regulacje, takie jak MiCA w UE czy wytyczne FATF, stanowią podstawę zrównoważonego rozwoju i ochrony uczestników rynku.
6. Zintegrowane podejście do cyberbezpieczeństwa: aby wirtualny pieniądz mógł efektywnie wspierać rozwój gospodarki cyfrowej, niezbędna jest integracja technologii, procedur operacyjnych, edukacji i regulacji. Kompleksowe podejście zwiększa odporność systemów na ataki oraz wspiera zaufanie użytkowników i instytucji finansowych.

Literatura

1. Binance. (2022). *Security notice: Cryptocurrency theft incident report*. Binance. Pobrano z: https://www.binance.com/en/support/announcement/security-2022 (dostęp: 20.12.2025).

2. EBA. (2022). *Risk assessment of crypto-assets: EBA report*. European Banking Authority. Pobrano z: https://www.eba.europa.eu/crypto-assets (dostęp: 20.12.2025).
3. ENISA. (2023). *Threat landscape for cryptocurrencies and virtual assets*. European Union Agency for Cybersecurity. Pobrano z: https://www.enisa.europa.eu/publications/crypto-threats-2023 (dostęp: 20.12.2025).
4. ESET. (2022). *Ransomware attacks targeting cryptocurrency exchanges*. ESET Research. Pobrano z: https://www.eset.com/int/research (dostęp: 20.12.2025).
5. FATF. (2022). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Financial Action Task Force. Pobrano z: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/virtual-assets-guidance.html (dostęp: 20.12.2025).
6. Fed. (2022). *Security considerations for a central bank digital currency*. Federal Reserve. Pobrano z: https://www.federalreserve.gov/econres/notes/feds-notes/security-considerations-for-a-central-bank-digital-currency-20220203.html (dostęp: 20.12.2025).
7. Gasz, M. i Smalara, R. (2025). Cyfrowy pieniądz banku centralnego – analiza korzyści i ryzyk związanych z wprowadzeniem nowego instrumentu płatniczego. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 69*(3), 21-37. https://doi.org/10.15611/pn.2025.3.02
8. IMF. (2024). *Central bank digital currencies: Financial stability implications*. International Monetary Fund. Pobrano z: https://www.imf.org/en/Publications/WP/Issues/2024/01/01 (dostęp: 20.12.2025).
9. Karpiuk-Wawryszuk, N. (2023). Uwarunkowania prawne emisji cyfrowego pieniądza banku centralnego w świetle raportów banków centralnych europejskich państw stojących u progu jego wdrożenia. *Ius et Administratio, 51*(2), 75-93. https://doi.org/10.15584/iuseta.2023.2.6
10. Kshetri, N., Bhushal, C., Pandey, P. (2022). *Blockchain Technology Applications for Cyber Defense and Cybersecurity*. Pobrano z: https://thesai.org/Publications/ViewPaper?Code=IJACSA&Issue=11&SerialNo=40&Volume=13 (dostęp: 20.12.2025).
11. Sayeed, S., Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

12. OECD. (2024). *Tokenisation of assets and digital finance: Implications for financial stability*. OECD Publishing. Pobrano z: https://www.oecd.org/finance/tokenisation-assets (dostęp: 20.12.2025).
13. Ryś, D. (2023). Kryptowaluty oraz waluty cyfrowe w polskich i międzynarodowych uwarunkowaniach prawno-gospodarczych. *Studia Ekonomiczne. Gospodarka, Społeczeństwo, Środowisko, 12*(2), 112-124.
14. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153-174. https://doi.org/10.2139/ssrn.3571335
15. WEF. (2021). *Central bank digital currencies: Key cyber risks and mitigation strategies*. World Economic Forum. Pobrano z: https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies (dostęp: 20.12.2025).



ISBN 978-83-68103-35-9