Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.021

Marta Zawisza[1]

CYBERBEZPIECZEŃSTWO W BANKOWOŚCI – UJĘCIE REGULACYJNE I WYZWANIA TECHNOLOGICZNE

Streszczenie

Celem pracy jest analiza zagadnień związanych z cyberbezpieczeństwem w sektorze bankowym, ze szczególnym naciskiem na funkcjonowanie bankowości internetowej oraz zagrożeń pojawiających się wraz z intensywnym rozwojem technologii cyfrowych. W treści opracowania przedstawiono pojęcie cyberbezpieczeństwa, jego kluczowe zasady oraz najczęściej występujące rodzaje cyberataków, które mogą skutkować naruszeniem ochrony danych oraz stratami finansowymi po stronie użytkowników. Szczególną uwagę poświęcono metodom uwierzytelniania i zabezpieczeniom stosowanym przez instytucje bankowe, podkreślając ich rolę w minimalizowaniu ryzyka nieuprawnionego dostępu do systemów informatycznych. W pracy omówiono również obowiązujące w Unii Europejskiej regulacje prawne, w tym dyrektywy CER, NIS2 oraz przepisy RODO, które wyznaczają zasady działania instytucji finansowych w obszarze ochrony cyfrowej. Dodatkowo dokonano analizy znaczenia sztucznej inteligencji w kontekście cyberbezpieczeństwa, wskazując zarówno na zagrożenia wynikające z jej wykorzystywania przez cyberprzestępców, jak i potencjalne ryzyka, z jakimi mogą się mierzyć klienci rynku finansowego.

Słowa kluczowe: cyberbezpieczeństwo, bankowość, system finansowy, manipulacja, sztuczna inteligencja.

[1] Studentka II roku II stopnia, kierunek: finanse i rachunkowość, Wydział Ekonomii i Finansów, Uniwersytet Radomski im. Kazimierza Pułaskiego, e-mail: 113604@student.uthrad.pl.

Wstęp

Współczesna bankowość opiera się na cyfrowych kanałach dostępu, gdzie operacje realizowane za pomocą smartfonów czy smartwatchy stały się standardem rynkowym. Ta postępująca digitalizacja usług detalicznych i korporacyjnych wymusza ciągłe doskonalenie systemów ochrony danych. Tradycyjny model bankowości, kojarzony z fizycznymi wizytami w placówkach i pieczętowaniem dokumentów, niemal całkowicie ustąpił miejsca nowoczesnym rozwiązaniom online. Postępująca cyfryzacja usług stanowi obecnie jeden z kluczowych trendów rozwojowych w wielu sektorach gospodarki. Nowoczesne rozwiązania elektroniczne obejmują coraz większą liczbę branż, oferując użytkownikom szeroki wachlarz możliwości i udogodnień. Szczególne znaczenie w tym obszarze zyskała bankowość internetowa, która stała się przedmiotem zainteresowania instytucji finansowych, klientów indywidualnych, organów regulacyjnych, a także grup przestępczych. Dynamiczny rozwój bankowości elektronicznej wiąże się bowiem z równoległym doskonaleniem metod cyberprzestępczości. Choć zagrożenia te występują w wielu obszarach funkcjonowania gospodarki cyfrowej, to ataki wymierzone w systemy bankowości internetowej należą do najbardziej dotkliwych, ponieważ mogą skutkować bezpośrednimi stratami finansowymi po stronie użytkowników. W ostatnich dekadach zjawisko cyberprzestępczości wyraźnie się nasiliło, generując coraz poważniejsze konsekwencje społeczne oraz ekonomiczne. Problem ten ma szczególnie istotny charakter, gdyż rozwojowi innowacyjnych technologii niemal jednocześnie towarzyszy tworzenie narzędzi wykorzystywanych do nadużyć oraz działalności przestępczej.

Celem niniejszego artykułu jest omówienie problematyki cyberbezpieczeństwa w sektorze bankowym, ze szczególnym uwzględnieniem specyfiki funkcjonowania bankowości internetowej. Analiza koncentruje się na identyfikacji kluczowych zagrożeń oraz ocenie roli regulacji prawnych i nowoczesnych rozwiązań technologicznych – w tym systemów opartych na sztucznej inteligencji – w zapewnianiu bezpieczeństwa środowiska cyfrowego.

Struktura opracowania obejmuje trzy zasadnicze części merytoryczne. W pierwszej zaprezentowano definicję i zakres pojęcia cyberbezpieczeństwa oraz dokonano charakterystyki najczęściej występujących zagrożeń w obszarze bankowości internetowej. Druga część poświęcona została analizie wybranych regulacji prawnych Unii Europejskiej kształtujących standardy ochrony cyfrowej w sektorze finansowym. W trzeciej części przedstawiono zależności pomiędzy cyberbezpieczeństwem a rozwojem sztucznej inteligencji, ze szczególnym uwzględnieniem ryzyk wynikających z jej wykorzystania przez podmioty prowadzące działalność przestępczą. Całość opracowania kończy podsumowanie zawierające wnioski końcowe. Podstawę opracowania stanowiła analiza literatury przedmiotu, raporty instytucji nadzorczych (m.in. Komisji Nadzoru Finansowego oraz ENISA), a także akty prawne Unii Europejskiej, w tym dyrektywy CER i NIS2 oraz rozporządzenie RODO. Uzupełnieniem były raporty branżowe oraz opracowania eksperckie dotyczące zagadnień cyberbezpieczeństwa w sektorze finansowym.

1. Cyberbezpieczeństwo – pojęcie, zakres i zasady

1.1. Pojęcie cyberbezpieczeństwa

Cyberbezpieczeństwo w ujęciu prawnym zostało zdefiniowane w ustawie o Krajowym Systemie Cyberbezpieczeństwa jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[2].

Termin cyberbezpieczeństwa odnosi się do kompleksowego zestawu działań, zaawansowanych technik oraz wielopoziomowych procesów, których nadrzędnym celem jest zabezpieczenie użytkowników i instytucji w przestrzeni cyfrowej. Działania te mają na celu skuteczną obronę przed szerokim spektrum zagrożeń, w tym przed celowymi atakami hakerskimi, przypadkowymi uszkodzeniami infrastruktury oraz wszelkimi próbami nieautoryzowanego uzyskania dostępu do zasobów. Skuteczne wdrożenie tych mechanizmów jest kluczowe ponieważ ewentualne naruszenia w tym obszarze mogą skutkować dotkliwymi szkodami finansowymi, prawnymi oraz wizerunkowymi.

Jedną z podstawowych zasad cyberbezpieczeństwa jest ochrona danych osobowych. Wielu ludzi nieświadomie ujawnia zbyt wiele informacji w sieci, kompletnie nie zdając sobie sprawy z konsekwencji. Oszuści dokładnie wiedzą, kogo chcą zaatakować. Dodatkowo nigdy nie wiadomo, kiedy można paść ofiarą ataku online. Dlatego warto zabezpieczyć swoje urządzenia antywirusem. Aż 70% badanych uważa, że banki stosują bardzo wysokie, często najwyższe, standardy ochrony swoich klientów. Niestety, to przekonanie bywa wykorzystywane przez oszustów podszywających się pod instytucje finansowe. Dlatego najważniejsze jest, aby zawsze stosować się do zasad bezpieczeństwa podanych na stronie banku[3].

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), art. 2 pkt 4., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf, [dostęp: 11.02.2025].

[3] B. Chlabicz, J. Dobrzańska, M. Kondek, E. Rokicka, raport *Bezpieczeństwo w Cyberprzestrzeni*, dostępny w: https://www.wib.org.pl/wp-content/uploads/2022/07/raport-wib-zbp-cyberbezpieczny-portfel-2022.pdf, [dostęp: 3.12.2025].

Tabela 1. Pojęcie cyberbezpieczeństwa

Rok	Autor/ Instytucja	Pojęcie cyberbezpieczeństwa
2013	ENISA	Cyberbezpieczeństwo oznacza zdolność sieci oraz systemów teleinformatycznych do przeciwdziałania zdarzeniom, które mogą naruszać dostępność, autentyczność, integralność oraz poufność przetwarzanych informacji.
2016	Dyrektywa NIS	Jest to zdolność systemów informacyjnych do skutecznego reagowania na incydenty stanowiące zagrożenie dla bezpieczeństwa sieci oraz świadczonych usług cyfrowych.
2019	ISO/IEC 27032	Cyberbezpieczeństwo polega na zapewnieniu ochrony informacji w cyberprzestrzeni poprzez utrzymanie ich poufności, integralności oraz dostępności
2020	K. Liderman	To zbiór rozwiązań technicznych, organizacyjnych i regulacyjnych, których celem jest zagwarantowanie bezpiecznego funkcjonowania podmiotów działających w środowisku cyfrowym.
2022	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (Polska)	Oznacza zapewnienie odporności systemów informacyjnych na działania mogące prowadzić do naruszenia poufności, integralności, dostępności lub autentyczności danych.

Źródło: Opracowanie własne na podstawie: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L 194 z 19.07.2016), European Union Agency for Network and Information Security (ENISA), *Definition of Cybersecurity – Gaps and Overlaps in Standardisation*, Heraklion, 2015, ISO/IEC 27032/2019, *Information technology – Security techniques – Guidelines for cybersecurity*, International Organization for Standardization, Geneva, K. Liderman, *Cyberbezpieczeństwo w teorii i praktyce*, Warszawa 2020, s.15, ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, 1123, stan prawny na 2022 r.)

1.2. Charakterystyka najczęstszych zagrożeń

W ostatnich latach obserwowany jest systematyczny wzrost liczby incydentów naruszenia bezpieczeństwa informacji, przy czym według raportu Verizon Data Breach Investigations Report 2023 analiza ponad 16 tysięcy incydentów wykazała dalszą dominację ataków opartych na czynniku ludzkim, w szczególności *phishingu* i kradzieży danych uwierzytelniających[4]. Obecnie globalne straty wynikające z cyberataków szacuje się na około 500 miliardów dolarów rocznie. W licznych krajach koszty generowane przez przestępczość internetową osiągają poziom przekraczający 1% produktu krajowego brutto, co podkreśla skalę i znaczenie tego problemu dla gospodarek narodowych[5]. Wraz z postępującym rozwojem bankowości internetowej zwiększa się również skala zagrożeń skierowanych do użytkowników tego kanału, a jednocześnie pojawiają się coraz nowsze oraz bardziej złożone metody wyłudzania środków finansowych. Do najczęściej występujących form ataków związanych

[4] Verizon, 2023 Data Breach Investigations Report, Verizon Enterprise, 2023, s. 10-12.

[5] K. Podgórski, *Poradzić sobie z wyzwaniami*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 32.

z funkcjonowaniem usług online należą m.in.: nieautoryzowane włamania do systemów bankowych prowadzące do kradzieży danych lub środków, tworzenie fałszywych stron podszywających się pod serwisy instytucji finansowych w celu przejęcia loginów, haseł i kodów SMS, rozsyłanie wiadomości e-mail zawierających złośliwe oprogramowanie, infekcje aplikacji mobilnych, ataki hybrydowe łączące kilka technik cyberprzestępczości oraz *phishing* i *spear phishing*[6]. Warto skupić się na dwóch ostatnich, gdyż według ekspertów liczba tych ataków znacząco wzrośnie. *Phishing* stanowi jedną z metod pozyskiwania poufnych informacji od użytkowników usług cyfrowych. Pomimo faktu, iż w wielu przypadkach próby wyłudzeń okazują się nieskuteczne, technika ta pozostaje chętnie wykorzystywana przez cyberprzestępców ze względu na prostotę realizacji oraz możliwość jednoczesnego dotarcia do bardzo szerokiego grona odbiorców. Szczególną odmianą *phishingu* jest *spear phishing*, który polega na precyzyjnym kierowaniu ataku do ściśle określonej grupy lub konkretnej osoby. W przeciwieństwie do klasycznego *phishingu* wymaga on znacznie większego zaangażowania oraz wcześniejszego zebrania informacji na temat celu ataku. Indywidualnie przygotowane wiadomości zwiększają skuteczność tego rodzaju działań. Najczęściej ofiarami *spear phishingu* są osoby zajmujące stanowiska kierownicze, co w przypadku powodzenia ataku umożliwia uzyskanie dostępu do wrażliwych danych finansowych, kadrowych oraz handlowych[7].

Tabela 2. Rodzaj zagrożenia

Rodzaj zagrożenia	Opis
Phishing	Rozsyłanie spreparowanych wiadomości (np. e-mail lub SMS), których celem jest skłonienie odbiorcy do ujawnienia poufnych danych, takich jak dane uwierzytelniające czy informacje finansowe.
Spear phishing	Precyzyjnie ukierunkowana forma ataku wymierzona w konkretną osobę, grupę lub instytucję, poprzedzona analizą informacji o celu w celu zwiększenia wiarygodności komunikatu.
Malware	Złośliwe oprogramowanie instalowane na urządzeniu użytkownika bez jego wiedzy, służące m.in. do przechwytywania danych, monitorowania aktywności lub uzyskania nieuprawnionego dostępu do systemu.
Ransomware	Rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu lub zaszyfrowanych danych, uzależniając ich odzyskanie od zapłaty okupu.
Deepfake	Technologia wykorzystująca algorytmy sztucznej inteligencji do tworzenia realistycznych, lecz nieautentycznych materiałów audio lub wideo, które mogą zostać użyte w celach manipulacyjnych lub oszustwa.

[6] PAP, *Ataki ransomware to żyła złota dla cyberprzestępców. Google ujawnił kwoty*, [online], Warszawa 27.07.2017, witryna Internet Businessinsider, Warshttp://businessinsider.com.pl/technologie/ ile-pieniedzy-przenosza-ataki-ransomware/db6vghl [dostęp: 03.12.2025].

[7] M. Złoch, *Atak na szczyt*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 62-63.

Cd. Tabeli 2.

Rodzaj zagrożenia	Opis
BEC (Business Email Compromise)	Oszustwo polegające na podszywaniu się pod osoby zajmujące wysokie stanowiska w organizacji w celu nakłonienia pracowników do realizacji nieuprawnionych przelewów lub przekazania wrażliwych informacji.

Źródło: Opracowanie własne na podstawie: K. Podgórski, *Poradzić sobie z wyzwaniami*, BANK Miesięcznik finansowy, nr 4 (276) 2016, s. 32

1.3. Zasady wpływające na bezpieczeństwo korzystania z bankowości internetowej

Użytkownik bankowości internetowej, niezależnie od zabezpieczeń opartych na stosowaniu odpowiednich protokołów szyfrowania, powinien wykorzystywać również dodatkowe rozwiązania zwiększające ogólny poziom bezpieczeństwa realizowanych transakcji. Mechanizmy te mają na celu m.in. poprawne potwierdzenie tożsamości użytkownika oraz zapewnienie możliwości jednoznacznego przypisania wykonania danej operacji. W praktyce stosowane metody uwierzytelniania dzieli się często na rozwiązania podstawowe (proste) oraz bardziej zaawansowane (silne), charakteryzujące się wyższym stopniem złożoności. Podstawowe metody uwierzytelniania opierają się przede wszystkim na informacjach, które zna użytkownik rachunku bankowego. Dane te powinny być dostępne wyłącznie dla właściciela konta i służyć do potwierdzenia jego tożsamości podczas korzystania z usług bankowości internetowej. Do najczęściej wykorzystywanych elementów tego typu uwierzytelniania należą:

- Identyfikator użytkownika: unikalna nazwa przypisana klientowi, często stanowiąca skróconą formę imienia i nazwiska, umożliwiająca jednoznaczną identyfikację w systemie bankowym.
- Hasło: sekwencja liter, cyfr oraz znaków specjalnych znana wyłącznie użytkownikowi. W praktyce często stosowane są hasła maskowane, w których system wymaga podania jedynie wybranych znaków hasła zamiast całego ciągu.
- Numer PIN: ciąg kilku cyfr, zazwyczaj od czterech do ośmiu, wykorzystywany do potwierdzenia uprawnień użytkownika, na przykład podczas aktywacji lub obsługi dodatkowych urządzeń zabezpieczających.

Drugą grupę rozwiązań tworzą zaawansowane (silne) techniki uwierzytelniania. Ich istotą jest wykorzystanie unikalnych przedmiotów lub atrybutów fizycznych znajdujących się w wyłącznym posiadaniu użytkownika. Choć rzadziej stosuje się kosztowne systemy oparte na kluczach prywatnych oraz podpisie cyfrowym, powszechnie wykorzystuje się inne narzędzia autoryzacyjne, takie jak: tokeny sprzętowe, wykazy haseł jednorazowych, kody weryfikacyjne SMS, odpowiednie aplikacje na urządzenia mobilne. Dodatkową formą zabezpieczenia jest obrazek bezpieczeństwa. Użytkownik wybiera grafikę przy zakładaniu konta,

a system wyświetla ją podczas logowania lub autoryzacji transakcji. Dzięki temu, że dany obrazek jest znany tylko klientowi, jego wyświetlenie na stronie www potwierdza wiarygodność serwisu i chroni przed oszustwami[8].

1.4. Wyzwania i trendy

Obecnie obserwujemy globalny i niezwykle dynamiczny postęp w dziedzinie nowoczesnych technologii, który w sposób kluczowy oddziałuje na sferę bezpieczeństwa instytucji finansowych. Aby sprostać wymaganiom współczesnego rynku i utrzymać pożądany stopień ochrony, banki są zmuszone do wielowymiarowego zabezpieczania swoich zasobów – nie tylko przed coraz groźniejszymi atakami hakerskimi czy próbami kradzieży wrażliwych danych, ale również przed skutkami nieprzewidzianych awarii technicznych. Jednocześnie instytucje te muszą dbać o stałą i niezakłóconą dostępność swoich usług oraz aplikacji dla klientów. Realizacja tak sformułowanych celów jest procesem skomplikowanym, wymagającym nie tylko zaawansowanego zaplecza technicznego, ale przede wszystkim unikalnych kompetencji i wysokich kwalifikacji kadry eksperckiej. Sektor finansowy nieustannie stawia czoła ewoluującej przestępczości, zwłaszcza że techniki stosowane przez cyberprzestępców stają się z każdym rokiem coraz bardziej przebiegłe i trudniejsze do wykrycia[9]. Istnieją poważne przesłanki, by sądzić, że w przyszłości cyberprzestępczość wymierzona w sektor finansowy może stanowić zagrożenie nawet dla rozwoju państw, szczególnie tych rozwijających się, które dysponują ograniczonymi zasobami do przeciwdziałania skutkom takich działań. Dane Narodowego Banku Polskiego pokazują, że w latach 2019–2024 wartość oszustw związanych z poleceniem przelewu w Polsce zwiększyła się aż dziesięciokrotnie. Świadczy to o rosnącej skali zjawiska, napędzanej m.in. koncentracją przestępców na klientach indywidualnych, postrzeganych jako najsłabsze ogniwo w systemie bezpieczeństwa. W tym ujęciu szczególnego znaczenia nabiera biometria behawioralna. Technologia ta pozwala na stałe monitorowanie i analizowanie indywidualnych wzorców zachowań użytkowników w trakcie korzystania z bankowości internetowej. Wykrycie odchyleń od wcześniej zapisanego profilu umożliwia rozpoznanie prób nieuprawnionego dostępu lub przejęcia rachunku. Rozwiązanie to stanowi zatem dodatkową, równoległą do tradycyjnych metod uwierzytelniania, warstwę ochrony. Dzięki ciągłemu nadzorowi nad sesją utrudnia jej przejęcie, a jednocześnie jest rozwiązaniem nieinwazyjnym, które nie pogarsza komfortu korzystania z usług bankowych.

---

[8] Ł. Zakonnik, P. Dembowski*, Bezpieczeństwo bankowości internetowej w Polsce na przestrzeni lat 2002-2017*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", nr 355, 2018, s. 108-110.

[9] B. Chlabicz, J. Dobrzańska, M. Kondek, E. Rokicka, raport *Bezpieczeństwo w Cyberprzestrzeni*, https://www.wib.org.pl/wp-content/uploads/2022/07/raport-wib-zbp-cyberbezpieczny-portfel-2022.pdf, [dostęp: 3.12.2025].

Dynamiczny rozwój nowoczesnych usług bankowości elektronicznej, w połączeniu z napływem wielu mniej doświadczonych użytkowników w okresie pandemii COVID-19, doprowadził do nasilenia niekorzystnych zjawisk. Najbardziej widocznym z nich był znaczący wzrost cyberprzestępczości. Zwiększona liczba klientów oraz realizowanych zdalnie transakcji przełożyła się na gwałtowny przyrost przestępstw i ataków wymierzonych w użytkowników bankowości cyfrowej. Zjawisko to szczególnie przybrało na sile od początku 2020 r., czyli wraz z wybuchem pandemii. Istotnym czynnikiem była także łatwość przekazywania skradzionych środków za granicę oraz ich dalszego wykorzystania. Z danych Komendy Głównej Policji wynika, że w 2021 r. odnotowano 18,3 tys. przestępstw związanych z e-bankowością i *phishingiem*, podczas gdy w 2020 r. było ich 10 tys., co oznacza wzrost o 80%[10]. W obliczu tak zmiennych zagrożeń, wprowadzenie rozwiązań opartych na chmurze obliczeniowej jawi się jako najbardziej optymalny i najprostszy sposób na zagwarantowanie integralności danych oraz nieprzerwanego działania systemów bankowych. Jest to szczególnie istotne w sytuacjach krytycznych, takich jak fizyczna niedostępność lub awaria własnych centrów przetwarzania danych należących do instytucji finansowych. Należy jednak pamiętać, że migracja do chmury nie jest procesem wolnym od trudności. Wiąże się ona z szeregiem ryzyk w obszarze bezpieczeństwa, które wymagają rygorystycznego zarządzania, a także z licznymi wyzwaniami o charakterze operacyjnym oraz koniecznością dostosowania się do restrykcyjnych wymogów regulacyjnych stawianych przez nadzór finansowy[11].

2. Dyrektywy unii europejskiej i wymagania prawne

2.1. Dyrektywa CER

Dyrektywa CER[12] (Dyrektywa w sprawie odporności podmiotów krytycznych) zaczęła obowiązywać w 2022 roku, zastępując regulacje dotyczące infrastruktury krytycznej z 2008 roku. Jej głównym zadaniem jest wzmocnienie poziomu ochrony cyfrowej na terenie Unii Europejskiej. Wprowadza ona wymagania w zakresie bezpieczeństwa informatycznego dla operatorów usług cyfrowych oraz dostawców cyfrowych produktów i usług. Ponadto dyrektywa kładzie nacisk na usprawnienie współpracy między państwami członkowskimi w obszarze reagowania na cyberataki oraz zapobiegania incydentom w cyberprzestrzeni. Celem tych działań jest podniesienie cyberbezpieczeństwa Unii Europejskiej oraz wzmocnienie jej roli jako jednego z liderów w tej dziedzinie. W odróżnieniu od

---

[10] W. Macierzyński, M. Macierzyński, *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019-2024)*, Repozytorium Uniwersytetu Łódzkiego, Łódź, 2025, s. 105-107.

[11] B. Chlabicz i in., raport *Bezpieczeństwo w Cyberprzestrzeni*, op. cit., s. 10.

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych, https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych, [dostęp: 11.02.2025].

wcześniejszych aktów prawnych, dyrektywa CER rozszerza podejście do bezpieczeństwa, koncentrując się nie tylko na ochronie materialnych elementów infrastruktury, lecz także na wzmacnianiu jej odporności organizacyjnej i operacyjnej. Uwzględnia przy tym różnorodne kategorie zagrożeń, takie jak cyberataki czy terroryzm. Dyrektywa nakłada na podmioty obowiązek implementacji odpowiednich rozwiązań technicznych, organizacyjnych oraz proceduralnych, mających na celu ograniczanie prawdopodobieństwa wystąpienia incydentów oraz zapewnienie ciągłości realizowanych usług. W szczególności obejmuje to opracowywanie planów zwiększania odporności, wdrażanie mechanizmów zarządzania kryzysowego, zgłaszanie poważnych incydentów właściwym organom krajowym, a także przeprowadzanie regularnych testów oraz audytów bezpieczeństwa. W odniesieniu do sektora bankowego regulacja ta ma szczególne znaczenie, ponieważ instytucje finansowe zostały uznane za podmioty o fundamentalnym znaczeniu dla stabilności gospodarczej państw członkowskich. Wymogi wynikające z CER wzmacniają obowiązek zapewnienia ciągłości operacyjnej, odporności na zakłócenia oraz skutecznego reagowania na incydenty, w tym zdarzenia o charakterze cybernetycznym. W rezultacie dyrektywa CER stanowi istotny etap w budowie zintegrowanego systemu bezpieczeństwa Unii Europejskiej, ukierunkowanego na zwiększenie odporności wobec zagrożeń o charakterze złożonym i transgranicznym.

2.2. Dyrektywa o bezpieczeństwie sieci i systemów informacyjnych (NIS2)

Jest to inicjatywa Unii Europejskiej, której celem jest wzmocnienie odporności Unii Europejskiej na zagrożenia w cyberprzestrzeni poprzez ustanowienie wspólnych ram prawnych w zakresie cyberbezpieczeństwa na poziomie państw członkowskich. Przyjęta w 2016 roku dyrektywa NIS[13] stanowiła pierwszy etap harmonizacji unijnych regulacji dotyczących ochrony cyfrowej. Nakładała ona na państwa członkowskie obowiązek wskazania podmiotów funkcjonujących w sektorach o kluczowym znaczeniu oraz dostawców usług cyfrowych, a także zobowiązywała je do wdrażania określonych standardów bezpieczeństwa. Dyrektywa NIS 2 stanowi rozwinięcie i kontynuację tych działań, mających na celu skuteczniejsze zabezpieczenie infrastruktury cyfrowej Unii Europejskiej. Do jej najważniejszych założeń należą m.in. rozszerzenie katalogu podmiotów objętych regulacjami poprzez objęcie kolejnych sektorów istotnych dla gospodarki i społeczeństwa, zaostrzenie wymagań dotyczących bezpieczeństwa informatycznego oraz wprowadzenie obowiązku stosowania konkretnych środków ochronnych. Istotnym elementem dyrektywy jest również wzmocnienie współpracy między państwami członkowskimi, w tym wymiany informacji o zagrożeniach i incydentach cybernetycznych. Ponadto NIS 2 przewiduje surowsze sankcje

[13] Dyrektywa UE 2022/2555 z dnia 14 grudnia 2022 o bezpieczeństwie sieci i systemów informacyjnych (NIS2), https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html, [dostęp: 11.02.2025].

za nieprzestrzeganie przepisów, co ma zwiększyć skuteczność ich egzekwowania. Głównym celem dyrektywy NIS 2 jest podniesienie poziomu odporności Unii Europejskiej na cyberzagrożenia oraz zapewnienie spójnych i efektywnych działań państw członkowskich w obszarze cyberbezpieczeństwa. Realizacja tych założeń ma przyczynić się do poprawy bezpieczeństwa cyfrowego obywateli, przedsiębiorstw oraz instytucji na terenie Unii Europejskiej.

2.3. Dyrektywa o atakach na systemy informacyjne

Jest to Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. z zakresu cyberbezpieczeństwa, koncentrująca się na przeciwdziałaniu atakom wymierzonym w systemy informatyczne, takim jak: włamania hakerskie, przestępstwa komputerowe oraz inne formy aktywności zaliczane do cyberprzestępczości. Skuteczne przeciwdziałanie cyberprzestępczości wymaga skoordynowanych działań nie tylko na poziomie pojedynczego państwa członkowskiego, lecz w całej Unii Europejskiej. Oznacza to konieczność zapewnienia jednolitego uznawania określonych zachowań za przestępstwa we wszystkich państwach członkowskich, a także wyposażenia organów ścigania w odpowiednie narzędzia pozwalające na efektywne działanie oraz współpracę transgraniczną. Dyrektywa ta została opracowana na podstawie decyzji ramowej Rady 2005/222/WSiSW dotyczącej ataków na systemy informatyczne i jednocześnie ją zastępuje. Uwzględnia również postanowienia Konwencji Rady Europy z 2001 roku o cyberprzestępczości, która stanowi punkt odniesienia dla krajowych i regionalnych regulacji w tym obszarze oraz zapewnia wspólne ramy współpracy zarówno w Unii Europejskiej, jak i poza jej granicami[14].

2.4. Cyberprzestępcy a RODO

Podstawowym celem RODO[15] jest ochrona praw jednostki. Przepisy wynikające z tego rozporządzenia, a także kolejne akty prawne, zapewniają szeroki zestaw narzędzi umożliwiających dochodzenie ochrony dóbr osobistych. Dodatkowo wraz z wejściem w życie RODO utworzono Urząd Ochrony Danych Osobowych (UODO), do którego można zgłaszać przypadki naruszeń. Instytucja ta wspiera obywateli w przeciwdziałaniu nieuczciwym praktykom związanym z przetwarzaniem danych osobowych. Wprowadzenie nowych regulacji oraz związane z nimi ryzyko dotkliwych sankcji niewątpliwie przyczyniło się do ograniczenia nielegalnych i etycznie wątpliwych działań dotyczących przetwarzania

[14] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2013-40-ue-dotyczaca-atakow-na-systemy-informatyczne-i-zastepujaca-68348646, [dostęp: 11.02.2025].

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, https://uodo.gov.pl/pl/404/224 [dostęp: 11.02.2025].

danych osobowych w internecie. Przedsiębiorstwa, szczególnie te działające na arenie międzynarodowej, zazwyczaj decydują się na przestrzeganie przepisów ze względu na wysokie kary finansowe oraz obawy o wizerunek i utratę zaufania klientów. Inaczej sytuacja wygląda w przypadku osób fizycznych lub niewielkich podmiotów, które traktują oszustwa internetowe jako podstawowe źródło dochodu i nie zawsze respektują obowiązujące regulacje[16].

3. Cyberbezpieczeństwo a sztuczna inteligencja

3.1. *Zagrożenia technologii stosujących sztuczną inteligencję*

Obecnie sztuczna inteligencja jest wykorzystywana w coraz szerszym zakresie sektorów, takich jak finanse, bankowość, ochrona zdrowia, handel czy administracja publiczna, gdzie przyczynia się do automatyzacji działań oraz poprawy ich skuteczności. Jednocześnie obserwowany jest bezprecedensowy wzrost liczby incydentów, w tym zdarzeń o charakterze krytycznym z punktu widzenia cyberbezpieczeństwa. Ataki są przeprowadzane średnio co 11 sekund, a globalne koszty cyberataków w 2021 roku oszacowano na 5,5 biliona euro – przy czym prognozy wskazują na dalszy wzrost tych strat. Wraz z dynamicznym rozwojem i popularyzacją rozwiązań opartych na AI, coraz większa liczba przedsiębiorstw wdraża je do swoich systemów informatycznych. Jednocześnie zwiększa to wagę zagadnień związanych z cyberbezpieczeństwem, ponieważ systemy sztucznej inteligencji operują na dużych zbiorach danych, często zawierających informacje wrażliwe. Skuteczna ochrona algorytmów, modeli oraz danych jest niezbędna do zapewnienia poufności, integralności i dostępności informacji, a także do budowania i utrzymania zaufania do systemów wykorzystujących sztuczną inteligencję[17]. Wykorzystanie sztucznej inteligencji przedsiębiorstw w obszarze cyberbezpieczeństwa wymaga starannego uwzględnienia kwestii etycznych. Do głównych wyzwań należą ochrona prywatności, stronniczość algorytmów oraz ryzyko nadużyć, które muszą być uwzględnione, aby zapewnić odpowiedzialne wdrożenie AI. Ryzyka związane ze sztuczną inteligencją obejmują nie tylko możliwość błędów w działaniu systemów, ale również potencjalne nadużycia związane z masowym gromadzeniem danych osobowych. Użytkownicy często nie są świadomi tych zagrożeń, natomiast brak zaufania do systemów AI może hamować wdrażanie nawet dobrze opracowanych technologii. Systemy te generują zagrożenia charakterystyczne zarówno dla szeroko pojętej technologii ICT (Information and Communications Technology), jak i specyficzne dla samej technologii, np. stronniczość algorytmiczną. Istotnym ryzykiem jest również jakość danych – algorytmy oparte na danych niskiej jakości lub niewystarczającej ich ilości mogą

[16] https://instytutcyber.pl/artykuly/cyberbezpieczenstwo-w-epoce-rodo/, [dostęp: 04.12.2025].

[17] K. Silicki, *Cyberbezpieczeństwo systemów wykorzystujących sztuczną inteligencję w świetle raportów ENISA*, Państwowy Instytut Badawczy NASK (NASK-PIB) – Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni we współpracy z ekspertami zewnętrznymi, Warszawa, s. 10-21.

generować nieprawidłowe wyniki. Kolejnym zagrożeniem stosowania AI w technologiach jest naruszenie prywatności i bezpieczeństwa danych. Gromadzenie i przetwarzanie informacji niezbędnych do działania systemów sztucznej inteligencji może prowadzić do naruszenia prywatności pracowników i klientów. Dlatego konieczne są odpowiednie inwestycje w ochronę danych oraz przestrzeganie regulacji dotyczących prywatności. Sztuczna inteligencja wpływa też na pogorszenie jakości i różnorodności danych, co ogranicza efektywność przetwarzania i zrozumienia kontekstu społecznego. Algorytmy mogą nie uwzględniać subtelności kulturowych czy językowych, co prowadzi do błędnych lub nieadekwatnych decyzji. Innym zagrożeniem jest tzw. *analysis paralysis* – paraliż analityczny, który występuje, gdy organizacje mają do dyspozycji tak ogromną liczbę danych, że nie są w stanie wyciągnąć z nich praktycznych wniosków. Przykładem może być firma analizująca dane milionów klientów, gdzie każdy generuje dziesiątki lub setki punktów danych dziennie, co utrudnia efektywną analizę. Wdrożenie AI w organizacji nie ogranicza się jedynie do aspektów technologicznych – wymaga także zmian w strategiach, procesach operacyjnych i kulturze organizacyjnej. Aby w pełni wykorzystać potencjał sztucznej inteligencji, konieczna jest kultura sprzyjająca innowacjom, eksperymentowaniu, uczeniu się oraz adaptacji, w której błędy są postrzegane jako wartościowy element rozwoju[18].

3.2. *Wykorzystanie sztucznej inteligencji jako zagrożenie dla klientów rynku finansowego*

Rynek finansowy jest ściśle powiązany z rozwojem technologii i w dużym stopniu od niej uzależniony. Można stwierdzić, że współczesne finanse nie są już w stanie funkcjonować bez zaplecza technologicznego, ponieważ niemal wszystkie kluczowe procesy realizowane przez instytucje tego sektora, zostały przeniesione do środowiska cyfrowego. Nieliczne, wciąż istniejące rozwiązania o charakterze analogowym pełnią obecnie jedynie rolę awaryjną i są wykorzystywane w ramach planów ciągłości działania, uruchamianych w sytuacjach awarii lub braku dostępności systemów oraz technologii cyfrowych. Najczęściej wykorzystywaną przez cyberprzestępców metodą kradzieży środków finansowych nie są – wbrew powszechnym przekonaniom – zaawansowane rozwiązania technologiczne, lecz techniki socjotechniczne i manipulacyjne. Stosowane są one w różnych wariantach *phishingu* oraz w oszustwach związanych z tzw. fałszywymi inwestycjami. Taki wybór narzędzi wynika z kalkulacji opartej na analizie BCR (Benefit Cost Ratio), czyli relacji kosztów do potencjalnych korzyści. Socjotechnika jest bowiem skuteczna, tania w realizacji i nie wymaga rozbudowanej infrastruktury technicznej, a jednocześnie umożliwia osiągnięcie zamierzonych celów finansowych. Przykładem może być

[18] K. Łusiakowski, *Rola sztucznej inteligencji (AI) w kształtowaniu cyberbezpieczeństwa przedsiębiorstwa*, „Zeszyty Naukowe Akademii Górnośląskiej", Nr 27 (3/2025), s. 62-73.

złośliwe oprogramowanie na urządzenia mobilne, służące m.in. do przechwytywania danych uwierzytelniających do bankowości elektronicznej, które bardzo często rozprzestrzeniane jest właśnie przy użyciu technik manipulacyjnych. Nowym kierunkiem w działalności cyberprzestępczej jest coraz częstsze wykorzystywanie algorytmów sztucznej inteligencji do usprawniania i optymalizacji działań przestępczych. Odbywa się to głównie poprzez automatyzację procesów oraz generowanie wiarygodnych treści tekstowych, głosowych oraz wizualnych. Tego typu działania stanowią poważne zagrożenie dla bezpieczeństwa środków finansowych klientów. Choć aktualne badania wskazują, że społeczeństwo posiada świadomość zagrożeń związanych z korzystaniem z internetu, rzeczywiste straty ponoszone przez polskich obywateli w wyniku cyberprzestępczości sięgają setek milionów złotych. Wykorzystanie technologii *deepfake* (od ang. *deep learning* – „głębokie uczenie" oraz *fake* – „fałszywy") do kradzieży środków finansowych, jako relatywnie nowe zjawisko stanowi istotne ryzyko. Wynika ono z dynamicznego rozwoju oraz powszechnej dostępności narzędzi umożliwiających tworzenie fałszywych treści, które coraz trudniej odróżnić od autentycznych. Zarówno klienci, jak i instytucje rynku finansowego będą zmuszeni do modyfikacji swoich zachowań oraz zdobywania wiedzy na temat skutecznych metod przeciwdziałania cyberprzestępczości[19].

Do głównych ryzyk ujawniających się w wyniku działań cyberprzestępczych na rynku finansowym – zarówno wobec klientów indywidualnych, jak i instytucji – należą przede wszystkim straty finansowe, w tym oszustwa internetowe i nieautoryzowane transakcje, naruszenia prywatności danych oraz ryzyko reputacyjne, szczególnie istotne dla instytucji finansowych. Analizując rozwój scenariuszy przestępczych wykorzystujących sztuczną inteligencję poza granicami Polski, można przypuszczać, że w najbliższym czasie grupy cyberprzestępcze, atakujące polskich obywateli oraz krajowe instytucje finansowe, również zaczną wdrażać AI do swoich działań. Przewidywane obszary wykorzystania tej technologii obejmują w szczególności:

- Zwiększenie skuteczności *phishingu* poprzez zastosowanie modeli językowych AI do tworzenia oszukańczych wiadomości napisanych poprawną i naturalną polszczyzną. Mimo istnienia mechanizmów zabezpieczających, modele sztucznej inteligencji mogą być relatywnie łatwo manipulowane.
- Wykorzystanie sztucznej inteligencji jako elementu narracyjnego mającego na celu nakłonienie ofiar do działań niekorzystnych dla nich samych. Tematyka AI, szeroko obecna w mediach i debacie publicznej jako innowacyjna technologia, sprzyja rozpowszechnianiu fałszywych i wprowadzających w błąd informacji.

[19] K. Zieliński, A. Ślusarek, *Wykorzystanie sztucznej inteligencji jako zagrożenie dla klientów rynku finansowego*, Urząd Komisji Nadzoru Finansowego, Departament Cyberbezpieczeństwa, 2023, s. 82-100.

- Tworzenie zmanipulowanych treści wideo oraz nagrań głosowych, umożliwiających obejście mechanizmów weryfikacji głosowej i wideoweryfikacji.
- Budowanie fałszywych tożsamości, wykorzystywanych do zakładania rachunków bankowych oraz prowadzenia różnorodnych działań przestępczych.
- Zastosowanie AI do bardziej precyzyjnych ataków *spearphishingowych*, m.in. poprzez generowanie treści głosowych i wideo z użyciem wizerunku lub głosu członków rodziny ofiary.
- Zwiększenie skuteczności ataków typu *spearphishing* oraz BEC (Business Email Compromise), np. dzięki wykorzystaniu próbek głosu lub nagrań wideo osób zlecających realizację wysokokwotowych transakcji finansowych.
- Potencjalna manipulacja odpowiedziami generowanymi przez systemy sztucznej inteligencji, prowadząca do sytuacji, w której użytkownik otrzymuje zafałszowaną informację jako najbardziej prawdopodobną odpowiedź na zadane zapytanie[20].

Podsumowanie

Intensywny rozwój bankowości cyfrowej oraz coraz większa rola technologii informatycznych powodują, że kwestia cyberbezpieczeństwa stały się jednym z fundamentalnych warunków zapewnienia stabilności sektora finansowego. Przeprowadzona analiza dowodzi, że postępująca digitalizacja usług finansowych wiąże się ze wzrostem zarówno liczby, jak i stopnia zaawansowania zagrożeń. Bankowość, jako obszar oparty na przetwarzaniu danych wrażliwych oraz realizacji transakcji o znacznej wartości, stanowi szczególnie atrakcyjny cel dla cyberprzestępców. Skutki skutecznych ataków wykraczają poza straty finansowe i obejmują również konsekwencje prawne, wizerunkowe oraz spadek zaufania klientów do instytucji finansowych.

Celem niniejszego artykułu było przedstawienie problematyki cyberbezpieczeństwa w sektorze bankowym, ze szczególnym uwzględnieniem bankowości internetowej, unijnych regulacji prawnych oraz znaczenia sztucznej inteligencji. Realizacja tego celu obejmowała identyfikację kluczowych zagrożeń, omówienie stosowanych mechanizmów ochronnych oraz analizę obowiązujących aktów prawnych, w tym dyrektyw CER i NIS2 oraz przepisów RODO. W toku rozważań wykazano, że efektywność wielu współczesnych ataków nie wynika przede wszystkim z niedoskonałości systemów technologicznych, lecz z wykorzystywania podatności czynnika ludzkiego, takich jak brak świadomości zagrożeń czy uleganie technikom socjotechnicznym. Wskazuje to na potrzebę łączenia inwestycji w nowoczesne rozwiązania technologiczne z intensyfikacją działań edukacyjnych skierowanych zarówno do klientów, jak i pracowników sektora finansowego.

Analiza podkreśliła także rosnącą rolę regulacji unijnych w kształtowaniu jednolitego systemu bezpieczeństwa cyfrowego. Dyrektywy CER i NIS2 przyczyniają

[20] K. Zieliński, A. Ślusarek, *Wykorzystanie sztucznej inteligencji…,* op. cit., s. 82-100.

się do zwiększenia odporności infrastruktury krytycznej oraz systemów teleinformatycznych, natomiast RODO ustanawia rygorystyczne standardy ochrony danych osobowych. Wspomniane regulacje tworzą spójne ramy prawne funkcjonujące na poziomie całej Unii Europejskiej, co ma szczególne znaczenie w obliczu transgranicznego charakteru współczesnych zagrożeń cybernetycznych.

Istotnym elementem rozważań była również sztuczna inteligencja, której znaczenie w obszarze cyberbezpieczeństwa systematycznie rośnie. Technologie oparte na AI wspomagają wykrywanie nieprawidłowości, analizę ryzyka oraz automatyzację procesów ochronnych. Jednocześnie narzędzia te są wykorzystywane przez cyberprzestępców do tworzenia coraz bardziej zaawansowanych form ataków, w tym spersonalizowanego *phishingu* czy materiałów typu *deepfake*. Dwuznaczny charakter tej technologii wskazuje na konieczność rozwijania bezpiecznych standardów jej wdrażania oraz budowania kompetencji w zakresie odpowiedzialnego i kontrolowanego wykorzystania.

Podsumowując, cyberbezpieczeństwo w sektorze bankowym należy postrzegać jako proces permanentny i kompleksowy, wymagający integracji rozwiązań technologicznych, regulacyjnych oraz edukacyjnych. Zapewnienie skutecznej ochrony możliwe jest jedynie przy ścisłej współpracy instytucji finansowych, organów nadzorczych, ustawodawcy oraz użytkowników usług bankowych. W nadchodzących latach znaczenie cyberbezpieczeństwa będzie nadal wzrastać, stając się jednym z kluczowych czynników warunkujących stabilność oraz poziom zaufania do systemu finansowego.

Bibliografia

1. Chlabicz B., Dobrzańska J., Kondek M., Rokicka E. , raport *Bezpieczeństwo w Cyberprzestrzeni*, https://www.wib.org.pl/wp-content/uploads/2022/07/raport-wib-zbp-cyberbezpieczny-portfel-2022.pdf, [dostęp: 03.12.2025].
2. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2013-40-ue-dotyczaca-atakow-na-systemy-informatyczne-i-zastepujaca-68348646,[dostęp: 11.02.2025].
3. Dyrektywa (UE 2022/2555) o bezpieczeństwie sieci i systemów informacyjnych (NIS2), https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html, [dostęp: 11.02.2025].
4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych, https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych, [dostęp: 11.02.2025].
5. Łusiakowski K., *Rola sztucznej inteligencji (AI) w kształtowaniu cyberbezpieczeństwa przedsiębiorstwa*, Zeszyty Naukowe Akademii Górnośląskiej, Nr 27 (3/2025), s. 62-73.

6. Macierzyński W., Macierzyński M., *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019-2024)*, Repozytorium Uniwersytetu Łódzkiego, Łódź, 2025, s. 105-107.
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), art.2 pkt 4., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf, [dostęp: 11.02.2025].
8. Podgórski K., *Poradzić sobie z wyzwaniami*, BANK Miesięcznik Finansowy, nr 4 (276) 2016, s. 32.
9. Silicki K., *Cyberbezpieczeństwo systemów wykorzystujących sztuczną inteligencję w świetle raportów ENISA*, Państwowy Instytut Badawczy NASK (NASK-PIB) – Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni we współpracy z ekspertami zewnętrznymi, Warszawa, s. 10-21.
10. Zakonnik Ł., Dembowski P., *Bezpieczeństwo bankowości internetowej w Polsce na przestrzeni lat 2002-2017*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", 2018, nr 355, s. 108-110.
11. Zieliński K., Ślusarek A., *Wykorzystanie sztucznej inteligencji jako zagrożenie dla klientów rynku finansowego*, Urząd Komisji Nadzoru Finansowego, Departament Cyberbezpieczeństwa, 2023, s. 82-100.
12. Złoch M., *Atak na szczyt*, BANK Miesięcznik Finansowy, nr 4 (276) 2016, s. 62-63.
13. Verizon, 2023 *Data Breach Investigations* Report, Verizon Enterprise, 2023, s. 10-12.

CYBERSECURITY IN BANKING – REGULATORY FRAMEWORK AND TECHNOLOGICAL CHALLENGES

Abstract

The aim of this paper is to analyze issues related to cybersecurity in the banking sector, with particular emphasis on the functioning of online banking and the threats emerging with the rapid development of digital technologies. The paper presents the concept of cybersecurity, its key principles, and the most common types of cyberattacks that can result in data breaches and financial losses for users. Particular attention is paid to the authentication methods and security measures used by banking institutions, emphasizing their role in minimizing the risk of unauthorized access to IT systems. The paper also discusses current European Union regulations, including the CER and NIS2 directives, as well as the GDPR, which define the principles of operation of financial institutions in the area of digital security. Additionally, the paper

analyzes the importance of artificial intelligence in the context of cybersecurity, highlighting both the threats posed by its use by cybercriminals and the potential risks faced by financial market customers.

Keywords: cybersecurity, banking, financial system, artificial intelligence (AI).