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.2025.020

Ola Rdzanek[1], Zuzanna Sulima[2]

STRATEGIE I WYZWANIA CYBERBEZPIECZEŃSTWA W BANKOWOŚCI

Streszczenie

W artykule omówiono współczesne zagrożenia w bankowości elektronicznej, obejmujące zarówno ataki socjotechniczne, jak i zagrożenia techniczne związane ze złośliwym oprogramowaniem. Szczególne znaczenie przypisano rosnącej roli sztucznej inteligencji i technologii generatywnych, które umożliwiają automatyzację oszustw finansowych i utrudniają ich wykrycie przy użyciu tradycyjnych metod ochrony. Bankowość prezentuje konieczność stosowania zintegrowanego podejścia do bezpieczeństwa, obejmującego zaawansowany monitoring transakcji, silne mechanizmy uwierzytelniania, szyfrowanie danych oraz stały nadzór centrów operacji bezpieczeństwa. Regulacje prawne pełnią kluczową funkcję w budowaniu rzeczywistej odporności cyfrowej instytucji finansowych. Pomimo rosnącej świadomości użytkowników, wielu z nich nadal nie stosuje podstawowych zasad bezpieczeństwa, co zwiększa podatność na ataki. Efektywna ochrona bankowości elektronicznej wymaga kompleksowego, wielowymiarowego podejścia łączącego nowoczesne technologie, regulacje prawne, współpracę międzynarodową oraz systematyczną edukację klientów i pracowników sektora finansowego.

Słowa kluczowe: bankowość, cyberbezpieczeństwo, cyberzagrożenia, sektor finansowy.

[1] Studentka 2 roku I stopnia, kierunek finanse i rachunkowość, Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 118449@student.uthrad.pl.
[2] Studentka 2 roku I stopnia, kierunek finanse i rachunkowość, Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 117678@student.uthrad.pl.

Wstęp

Dynamiczny rozwój technologii cyfrowych w ostatnich dekadach doprowadził do głębokiej transformacji sektora finansowego. Bankowość elektroniczna, płatności mobilne, zdalna identyfikacja klientów oraz automatyzacja procesów operacyjnych stały się standardem funkcjonowania współczesnych instytucji finansowych. Cyfryzacja znacząco zwiększyła dostępność i wygodę usług bankowych, jednak równocześnie doprowadziła do powstania nowych obszarów ryzyka, których skala i złożoność rosną wraz z postępem technologicznym.

Współczesne środowisko bezpieczeństwa sektora finansowego charakteryzuje się wysoką dynamiką zmian oraz coraz większym stopniem profesjonalizacji cyberprzestępczości. Ataki wymierzone w banki oraz ich klientów nie mają już wyłącznie charakteru incydentalnego – coraz częściej stanowią element zorganizowanej działalności przestępczej, wykorzystującej zaawansowane technologie, w tym sztuczną inteligencję oraz narzędzia automatyzujące procesy ataku. Jednocześnie sektor bankowy jako część infrastruktury krytycznej państwa, podlega rosnącym wymaganiom regulacyjnym w zakresie budowania odporności cyfrowej i zarządzania ryzykiem operacyjnym.

Zrozumienie istoty cyberzagrożeń, ich źródeł oraz mechanizmów działania jest kluczowe dla oceny poziomu bezpieczeństwa bankowości elektronicznej. Ważne jest więc określenie czym są cyberzagrożenia. Jest to ogół niebezpieczeństw związanych ze szkodliwymi działaniami, do których dochodzi za pośrednictwem Internetu oraz nowoczesnych technologii komunikacyjnych. Zjawisko to obejmuje szeroki wachlarz ataków wymierzonych w systemy komputerowe, sieci i gromadzone w nich dane – od prób nieautoryzowanego dostępu, przez infekcje złośliwym oprogramowaniem, aż po paraliżujące ataki serwerów poprzez zalanie je sztucznym ruchem z wielu źródeł. Istotne znaczenie ma również analiza postaw społecznych wobec zagrożeń w przestrzeni cyfrowej, ponieważ czynnik ludzki pozostaje jednym z najsłabszych ogniw systemu bezpieczeństwa.

Celem niniejszego artykułu jest charakterystyka współczesnych cyberzagrożeń, identyfikacja głównych źródeł ryzyka w bankowości elektronicznej oraz omówienie systemów ochrony i kierunków rozwoju cyberbezpieczeństwa w sektorze finansowym. Analiza obejmuje zarówno aspekt technologiczny, organizacyjny, jak i społeczny, co pozwala na szerokie ujęcie problematyki bezpieczeństwa w erze cyfrowej transformacji.

1. Źródła cyberzagrożeń

W czasie dynamicznego rozwoju technologii, cyfryzacji oraz postępującej globalizacji świat funkcjonuje w rzeczywistości nieustannej zmiany. Nowoczesne systemy informatyczne, powszechny dostęp do Internetu, rozwój sztucznej inteligencji oraz automatyzacja procesów przynoszą społeczeństwom ogromne korzyści, ale jednocześnie generują nowe, często trudne do przewidzenia zagrożenia. Współczesne

środowisko bezpieczeństwa staje się coraz bardziej złożone, a granice pomiędzy sferą fizyczną i cyfrową ulegają zmianom[3].

Jednym z klasycznych źródeł zagrożeń są hakerzy, czyli osoby nieuprawnione, uzyskujące dostęp do systemów informatycznych. Ich działalność może mieć charakter jednostkowy i być motywowana chęcią osiągnięcia korzyści majątkowej, jak również zdobycia prestiżu w środowisku cyberprzestępczym. Wykorzystują oni przede wszystkim luki w oprogramowaniach, błędy konfiguracyjne systemów, niewystarczające zabezpieczenia sieciowe, słabe mechanizmy uwierzytelniania.

W bankowości elektronicznej zagrożenie to dotyczy zarówno bezpośrednich prób włamania do systemów bankowych, jak i ataków na urządzenia końcowe klientów (komputery, telefony). Często hakerzy sprzedają uzyskany dostęp do infrastruktury finansowej innym podmiotom, funkcjonującym w ramach podziemnej gospodarki cyfrowej[4].

Coraz częściej z działalności indywidualnej, hakerzy dołączają do zorganizowanych grup cyberprzestępczych, które funkcjonują na zasadach zbliżonych do profesjonalnych struktur biznesowych. Ich działalność charakteryzuje się między innymi ścisłym podziałem ról (programiści, analitycy danych, operatorzy *phishingu*, osoby zajmujące się praniem pieniędzy), działaniem transgranicznym, wykorzystującym infrastruktury serwerowe w wielu państwach oraz stosowaniem kryptowalut do transferu i ukrywania środków. Grupy te tworzą gotowe narzędzia przestępcze (np. pakiety *phishingowe*, złośliwe oprogramowanie typu „malware-as-a-service"), które są następnie sprzedawane w tzw. darknecie[5]. Umożliwia to wejście w działalność przestępczą osobom bez zaawansowanej wiedzy technicznej. Zorganizowane grupy przestępcze często łączą różne techniki typu *phishing*, *malware*, kradzież tożsamości oraz wykorzystanie podstawionych osób do transferu środków, przy czym tworzą wieloetapowy model oszustwa. Z punktu widzenia bankowości elektronicznej zagrożenie to jest szczególnie niebezpieczne, ponieważ działania te mają charakter zazwyczaj masowy (atakują tysiące klientów jednocześnie), zautomatyzowany oraz trudny do wykrycia w początkowej fazie[6].

[3] *Współczesne wyzwania w zakresie cyberbezpieczeństwa,* 2024, blog (Współczesne wyzwania w zakresie cyberbezpieczeństwa, Nomios Polska) [dostęp: 13.12.2025].

[4] *Sektor finansowy a cyberzagrożenia – czy nasze pieniądze są bezpieczne,* 2024, Instytut cyberbezpieczeństwa, 2024. https://instytutcyber.pl/artykuly/sektor-finansowy-a-cyberzagrozenia/ [dostęp: 13.12.2025].

[5] Darknet to część Internetu niedostępna przez standardowe wyszukiwarki i przeglądarki, wymagająca specjalnego oprogramowania, takiego jak Tor. Zapewnia użytkownikom wysoki poziom anonimowości poprzez ukrywanie ich adresu IP i szyfrowanie ruchu sieciowego. Choć bywa wykorzystywany do celów przestępczych (np. handlu nielegalnymi danymi), służy także dziennikarzom, aktywistom i osobom żyjącym w krajach o silnej cenzurze Internetu.

[6] K. Dmowska, *Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego*, Bank i Kredyt, Nr 4, 2022, BIK_04_2022_01.pdf [dostęp: 13.12.2025].

Istotnym źródłem zagrożeń pozostaje czynnik ludzki. Nawet najbardziej zaawansowane systemy bezpieczeństwa mogą zostać osłabione przez nieświadome działanie pracowników instytucji finansowych lub podmiotów współpracujących. Do najczęstszych błędów zalicza się, gdy pracownik banku: otwiera zainfekowane załączniki, korzysta z niezabezpieczonych sieci Wi-Fi, stosuje jednakowe hasła w wielu systemach, nie przestrzega regulaminu bezpieczeństwa lub udziela informacji poufnych osobom nieuprawnionym. Szczególnie niebezpieczne są ataki typu *spear-phishing*, które są precyzyjnie ukierunkowane na konkretnego pracownika posiadającego dostęp do wrażliwych danych lub systemów autoryzacyjnych. Takie ataki mogą wykorzystywać różne techniki manipulacyjne, aby zwiększyć wiarygodność wiadomości i skłonić pracowników do popełnienia błędów. Bezpieczeństwo bankowości elektronicznej zależy nie tylko od zabezpieczeń technicznych, lecz także od poziomu świadomości, wiedzy oraz ciągłego rozwoju umiejętności pracowników banku[7].

Rozwój sztucznej inteligencji jest jednym z czynników, który umożliwia przestępcom automatyzację ataków na większą skalę i maksymalizację ich skuteczności. Oszuści wykorzystują AI między innymi do generowania realistycznych wiadomości *phishingowych* pozbawionych błędów językowych, tworzenia *deepfake'ów* (fałszywych nagrań głosu lub wideo), analizowania zachowań użytkowników w celu personalizacji oszustwa czy automatycznego testowania podatności systemów. Szczególnie niebezpieczne są przypadki wykorzystania *deepfake'ów* do imitowania głosu przełożonych lub członków zarządu, co może prowadzić do autoryzowania fikcyjnych przelewów o znacznej wartości. Takie zastosowanie AI powoduje, że ataki stają się bardziej spersonalizowane, szybsze, masowe, a jednocześnie trudniejsze do odróżnienia od autentycznej komunikacji[8].

Źródła zagrożeń w bankowości elektronicznej mają charakter wielopoziomowy i obejmują zarówno działania indywidualnych hakerów, zorganizowanych grup przestępczych, czynniki ludzkie wewnątrz organizacji, jak i nowe technologie, w tym sztuczną inteligencję.

[7] N. Siemieniuk, A. Zalewska-Bochenko, *Bezpieczeństwo systemów informatycznych w instytucjach bankowych*, „Roczniki Kolegium Analiz Ekonomicznych"/Szkoła Główna Handlowa, Nr 44, 2017 (roczniki_kae_z44_05.pdf) [dostęp: 13.12.2025].

[8] Warszawski Instytut Bankowości. Związek Banków Polskich, 2025. *Raport Postawy Polaków wobec cyberbezpieczeństwa 2025,* https://share.google/LlibRUK6IssYyKq0k [dostęp: 13.12.2025].

Bezpieczeństwo sektora finansowego wymaga zatem integracji zabezpieczeń technicznych i organizacyjnych, stałej edukacji użytkowników i pracowników, monitorowania nowych trendów technologicznych oraz współpracy międzynarodowej w zwalczaniu cyberprzestępczości[9].

2. Rodzaje cyberzagrożeń

Współczesne cyberzagrożenia nie mają jednolitego charakteru, tworzą złożony system różnorodnych ataków, które można klasyfikować w zależności od sposobu działania przestępców. W przeciwieństwie do ogólnych incydentów cyberbezpieczeństwa, ataki na bankowość elektroniczną są precyzyjnie projektowane pod kątem procesów logowania, autoryzacji transakcji oraz komunikacji bank-klient[10].

Najczęściej wykorzystywane są działania opierające się na socjotechnice, czyli manipulacji psychologicznej. Przestępcy starają się wywołać w ofierze silne emocje, informując na przykład o „niepowtarzalnej okazji" finansowej lub – co gorsza – straszą zablokowaniem konta, aby skłonić użytkownika do szybkich i nieprzemyślanych działań[11]. Jedną z takich metod ataku na użytkowników bankowości elektronicznej jest *phishing*. To forma oszustwa, w której przestępca podszywa się pod zaufaną osobę lub instytucję – najczęściej bank – w celu wyłudzenia poufnych informacji, takich jak dane logowania czy kody autoryzacyjne. Często wysyłane są wiadomości e-mail zawierające linki do fałszywych stron bankowości internetowej, które wizualnie do złudzenia przypominają oryginalne witryny internetowe[12]. Inną formą *phishingu* w sieci jest *pharming*. W tym przypadku użytkownik nie musi nawet popełnić błędu przy wpisywaniu adresu, mimo podania prawidłowej strony banku zostaje automatycznie przekierowany na fałszywą witrynę przygotowaną przez przestępców w celu wyłudzenia danych. Podobnym sposobem ataku są rozmowy telefoniczne (tzw. *Vishing*), podczas których oszuści podają się za pracowników banku i proszą o podanie haseł lub kodów, argumentując to rzekomą awarią systemu lub koniecznością zwiększenia bezpieczeństwa. Cyberprzestępcy rozsyłają również wiadomości zawierające „ostateczne wezwania do zapłaty" lub informacje

---

[9] M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną, Poradnik klienta usług KNF*, 2014, Bezp_finansowe_39005.pdf [dostęp: 13.12.2025].

[10] K. Dmowska, 2022. *Cyberbezpieczeństwo…,* op. cit.

[11] *Socjotechnika – dlaczego cyberprzestępcy są skuteczni?*, 2023, https://www.gov.pl/web/baza-wiedzy/socjotechnika--dlaczego-cyberprzestepcy-sa-skuteczni [dostęp: 13.12.2025].

[12] J. Simola, T. Leppanen. 2025. *Identification of the Emerging Sources Cybersecurity Threats,* University of Jyväskylä, Finland, https://www.researchgate.net/publication/393049451_Identification_of_the_Emerging_Sources_of_Cybersecurity_Threats) [dostęp: 13.12.2025]; E. Woollacott, 2024, *What Is Phishing? Understanding Cyber Attacks.* Forbes (https://www.forbes.com/sites/technology/article/what-is-phishing/) [dostęp: 13.12.2025].

o rzekomym zadłużeniu. Celem jest wywołanie presji i skłonienie ofiary do otwarcia zainfekowanego załącznika albo dokonania przelewu. Mechanizm ten łączy elementy socjotechniki z techniczną infekcją systemu[13].

Równie niebezpieczną grupą zagrożeń są metody techniczne oparte na szpiegowaniu i cichej kradzieży danych bez interakcji z użytkownikiem, często realizowane poprzez złośliwe oprogramowanie (*malware*), którego celem jest zniszczenie zasobów lub ich przejęcie. Wśród nich znajdują się zarówno tradycyjne wirusy komputerowe, które uszkadzają pliki i rozsyłają spam, jak i konie trojańskie (trojany), podszywające się pod przydatne programy, aby przejąć kontrolę nad komputerem i wykradać wprowadzane dane, takie jak loginy i hasła. Ponadto cyberprzestępcy wykorzystują programy szpiegujące (*spyware*), które gromadzą informacje o użytkowniku i przesyłają je bez jego wiedzy autorowi programu. W tym *keyloggery*, czyli rejestratory klawiatury, które bez wiedzy użytkownika zapisują każde naciśnięcie klawisza, łącznie z wprowadzanymi hasłami. Cyberprzestępcy stosują również mechanizmy wymuszeń i blokowania dostępu, przypominające działanie *ransomware*. Jest to oprogramowanie blokujące dostęp do systemu lub szyfrujące dane użytkownika, a następnie żądające okupu za ich odblokowanie. Skutkiem może być całkowite uniemożliwienie korzystania z komputera lub utrata dostępu do kluczowych danych[14].

Do kradzieży informacji dochodzi również poprzez nasłuchiwanie ruchu sieciowego (*sniffing*), które umożliwia przechwytywanie haseł przesyłanych w sieciach lokalnych lub publicznych sieciach Wi-Fi. W rzeczywistości odpowiednikiem takich działań jest *skimming*, polegający na kopiowaniu danych z pasków magnetycznych kart płatniczych za pomocą specjalnych nakładek instalowanych na bankomatach oraz rejestrowaniu kodów PIN przy użyciu ukrytych kamer, co następnie umożliwia zdublowanie takiej karty[15].

Na szerszą skalę zagrożenia obejmują ataki sieciowe, których celem jest destabilizacja i zakłócanie działania systemów. Wykorzystuje się tu m.in. *spoofing*, polegający na podszywaniu się pod inny komputer w celu wykorzystania go jako narzędzia do ataków na określone strony internetowe. Infrastrukturę mogą przeciążać także robaki komputerowe (*worms*), które samodzielnie rozpowszechniają się w sieciach, powodując np. paraliż serwerów pocztowych. Ataki typu DDoS (Distributed Denial of Service) również polegają na przeciążeniu systemu, serwera lub usługi internetowej ogromną liczbą jednoczesnych zapytań z wielu źródeł. Do przeprowadzenia ataku często wykorzystuje się sieci zainfekowanych urządzeń (botnety). Skutkiem jest czasowa niedostępność usług, spowolnienie systemów lub całkowity paraliż infrastruktury[16].

---

[13] M. Górnisiewicz, R. Obczyński, M. Pstruś. 2014. *Bezpieczeństwo finansowe*..., op. cit.

[14] *Baza wiedzy* (Aktualności – Baza wiedzy – Portal Gov.pl) [dostęp: 13.12.2025].

[15] N. Siemieniuk, A. Zalewska-Bochenko. 2017. *Bezpieczeństwo systemów...,* op. cit.

[16] 2023. *Bezpieczna łączność dla sektora bankowego w erze cyfrowej* (Bezpieczna łączność dla sektora bankowego w erze cyfrowej - 5G: sieci telekomunikacyjne nowej generacji – Portal Gov.pl) [dostęp: 13.12.2025].

3. Systemy i strategie ochrony w bankowości

Wraz z rozwojem usług finansowych systemy bezpieczeństwa muszą być stale aktualizowane lub tworzone od nowa. Wynika to z faktu, że wiele zagrożeń pojawia się dopiero w momencie, gdy klienci zaczynają aktywnie korzystać z nowych technologii. To właśnie codzienne użytkowanie produktów weryfikuje ich odporność i ujawnia słabe punkty, które wymagają naprawy. Z tego powodu strategia ochrony w bankowości opiera się na dynamicznym reagowaniu na incydenty oraz współpracy między bankiem a klientem[17].

Podstawowym elementem bezpieczeństwa jest ochrona poufności danych. Informacje zawarte w dowodzie osobistym pozwalają na jednoznaczną identyfikację osoby, co przestępcy mogą wykorzystać do wyłudzenia kredytu lub założenia fałszywego rachunku bankowego. Kluczową zasadą jest nieudostępnianie tych danych osobom nieuprawnionym oraz unikanie przesyłania ich przez niezabezpieczone kanały internetowe. Należy pamiętać, że Internet nie zapewnia anonimowości, a raz opublikowane dane mogą zostać odzyskane nawet po usunięciu. To samo dotyczy kart płatniczych. Do kradzieży środków często nie jest potrzebna fizyczna karta – przestępcom wystarczy jej numer oraz kod zabezpieczający, dlatego nigdy nie należy udostępniać zdjęć kart w sieci. Nawet najlepsze rozwiązania techniczne tracą skuteczność, gdy użytkownik nie zachowuje podstawowej higieny cyfrowej[18].

Kolejnym istotnym zagrożeniem, na które muszą odpowiadać systemy bezpieczeństwa, są ataki socjotechniczne. Przestępcy rzadziej atakują infrastrukturę banku, a częściej manipulują klientem. Wykorzystują oni emocje, takie jak strach przed rzekomą blokadą konta, zdenerwowanie lub ekscytacja fałszywą okazją, aby zmusić ofiarę do działania pod presją czasu, która wywierana celowo przez oszustów, ma na celu wyłączenie krytycznego myślenia ofiary. W takich sytuacjach ludzie często zapominają o podstawowych zasadach ostrożności. Skuteczna obrona wymaga więc weryfikacji każdego nietypowego komunikatu i zachowania zdrowego rozsądku, aby wspierać użytkowników, banki wdrażają zaawansowane rozwiązania techniczne, które działają automatycznie. Podstawą jest tu system monitoringu transakcji. Oprogramowanie to analizuje zachowania klientów w czasie rzeczywistym i wykrywa anomalie, takie jak logowanie z nietypowej lokalizacji czy zlecenie przelewu na bardzo dużą kwotę. Jeśli system uzna operację za podejrzaną, może ją automatycznie zablokować[19].

Dodatkowym zabezpieczeniem jest silne uwierzytelnianie dwuskładnikowe (MFA). Polega ono na tym, że do zalogowania lub potwierdzenia transakcji nie wystarczy samo hasło. Konieczne jest użycie drugiego składnika, np. kodu SMS, potwierdzenia w aplikacji mobilnej lub odcisku palca. Uzupełnieniem tych metod jest

[17] K. Dmowska. 2022. *Cyberbezpieczeństwo...,* op. cit.

[18] M. Górnisiewicz, R. Obczyński, M. Pstruś. 2014. *Bezpieczeństwo finansowe...,* op. cit.; Warszawski Instytut Bankowości, Związek Banków Polskich *Raport...,* op. cit.

[19] N. Siemieniuk, A. Zalewska-Bochenko, 2017, *Bezpieczeństwo systemów...,* op. cit.

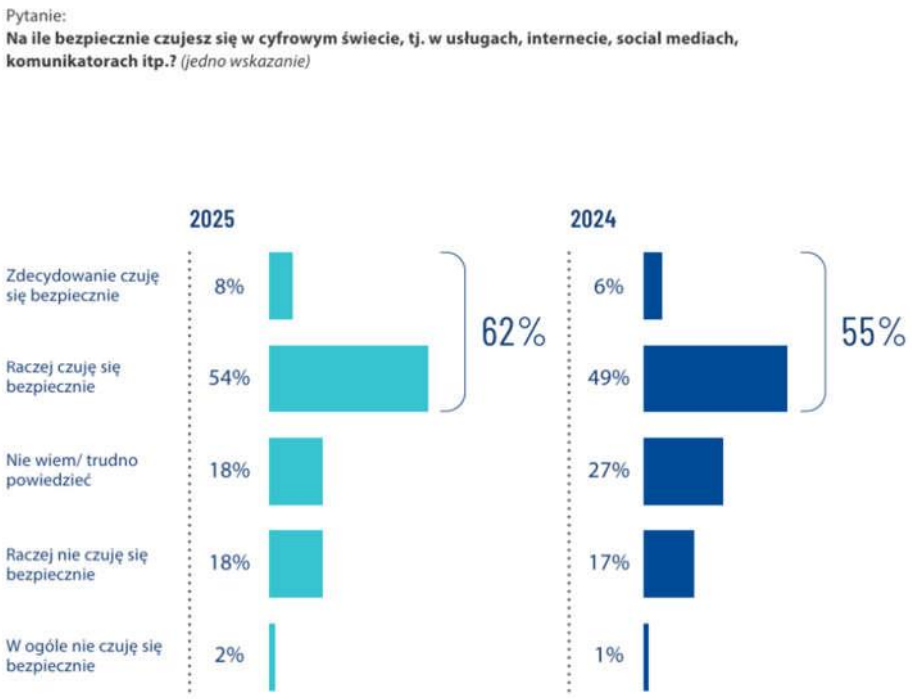
szyfrowanie połączeń, które uniemożliwia osobom trzecim podgląd przesyłanych danych. Skuteczne bezpieczeństwo bankowości opiera się więc na połączeniu technologii monitorujących i szyfrujących z odpowiedzialnym zachowaniem klienta[20].

4. Postawy Polaków wobec cyberbezpieczeństwa

Nie każdy obywatel w pełni zdaje sobie sprawę z zakresu zagrożeń, które występują w środowisku cyfrowym. Internet, będący integralnym elementem współczesnego życia codziennego, zapewnia nie tylko wygodę i niemal nieograniczony dostęp do informacji, ale również stwarza potencjalne ryzyko dla użytkowników. Nawet krótkotrwała nieuwaga, interakcja z podejrzanymi odnośnikami lub niekontrolowane udostępnianie danych osobowych może prowadzić do poważnych konsekwencji. Sprawcy cyberprzestępczości często wykorzystują zaufanie użytkowników, ich ograniczoną wiedzę bądź presję czasu w celu osiągnięcia własnych korzyści. W związku z tym istotne jest systematyczne rozwijanie świadomości zagrożeń cyfrowych oraz kształtowanie zachowań ostrożnościowych, które mogą ograniczyć ryzyko wystąpienia nieodwracalnych skutków naruszeń bezpieczeństwa w sieci.

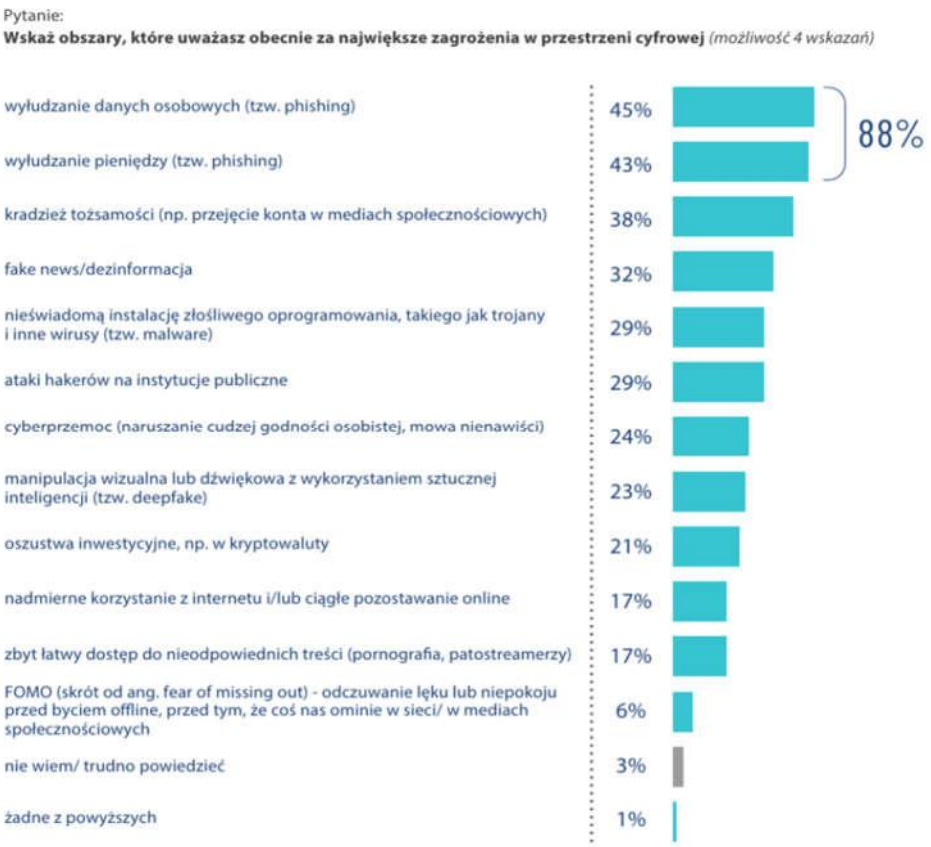
Poniżej przedstawiono wyniki badań Polaków na temat poczucia bezpieczeństwa w przestrzeni cyfrowej. W 2024 roku możemy zaobserwować, że 55% badanych nie odczuwa zagrożenia, natomiast 27% respondentów nie potrafi określić swojego odczucia, czy czuję się pewnie w omawianej kwestii, a pozostałe 18% ankietowanych nie czuje się bezpiecznie. Ponowne badanie z 2025 roku wykazało wyraźny wzrost poczucia bezpieczeństwa wśród Polaków – o 7 punktów procentowych. Co istotne, nieznacznie wzrosła także grupa osób odczuwających brak bezpieczeństwa.

[20] K. Dmowska, 2022, *Cyberbezpieczeństwo...,* op. cit.



Rys. 1. Poczucie bezpieczeństwa w przestrzeni cyfrowej
Źródło: *Postawy Polaków wobec cyberbezpieczeństwa 2025*, Raport WIB/ZBP

Do największych zagrożeń w przestrzeni cyfrowej należą *phishing*, kradzież tożsamości, dezinformacja oraz *fake newsy*. Warto podkreślić, że niemal co trzeci respondent (29%) wyraża obawy związane z atakami hakerskimi na instytucje publiczne oraz zagrożeniami typu malware, takimi jak nieświadome zainstalowanie złośliwego oprogramowania (np. trojanów czy wirusów). Ankietowani zwracają również uwagę na problem mowy nienawiści oraz naruszania godności osobistej – 24% badanych postrzega cyberprzemoc jako poważne zagrożenie. Respondenci dostrzegają także ryzyko związane z oszustwami wykorzystującymi sztuczną inteligencję. Blisko jedna czwarta badanych (23%) uważa *deepfaki* w Internecie za realne niebezpieczeństwo. Co więcej, technologia ta może być wykorzystywana do różnego rodzaju manipulacji, w tym mistyfikacji inwestycyjnych, np. związanych z kryptowalutami – 21% respondentów wskazuje oszustwa inwestycyjne jako istotne zagrożenie.



Rys. 2. Największe zagrożenia w przestrzeni cyfrowej
Źródło: *Postawy Polaków wobec cyberbezpieczeństwa 2025*, Raport WIB/ZBP

Mimo że ponad połowa Polaków nadal zabezpiecza smartfony kodem PIN, równie wielu korzysta już z biometrii – odcisku palca czy skanu twarzy, przy czym w ciągu ostatnich trzech lat rozwiązania te wyraźnie zyskały na popularności, a szczególnie rozpoznawanie twarzy, którego użycie niemal się podwoiło. Zmieniają się więc nasze nawyki w zakresie ochrony urządzeń mobilnych, coraz częściej sięgamy po wygodniejsze i nowocześniejsze metody zabezpieczeń. Jednocześnie nie wszystkie narzędzia zwiększające bezpieczeństwo cieszą się takim samym zainteresowaniem, rzadko kiedy korzystamy z generatorów haseł automatycznie tworzących silne kombinacje, ponieważ zamiast tego wolimy samodzielnie wymyślać hasła, opierając je na własnych skojarzeniach. Dodatkowo ponad połowa obywateli deklaruje posiadanie aktualnego oprogramowania antywirusowego na smartfonie i komputerze, ale co trzecia osoba robi je tylko sporadycznie, jednocześnie narażając się na ataki malware. Młodzież większą uwagę przywiązuje do ochrony telefonu niż

komputera, podczas gdy starsze osoby częściej dbają o regularne aktualizacje systemu na komputerach.

Choć rośnie nasza świadomość zagrożeń cyfrowych, wciąż nie wykorzystujemy w pełni dostępnych narzędzi ochrony. Większość osób deklaruje troskę o dane osobowe i finansowe oraz unikanie podejrzanych linków i załączników. Połowa właściwie zabezpiecza dostęp do bankowości elektronicznej, jednak mniej użytkowników dba o prywatność w mediach społecznościowych, stosuje uwierzytelnianie dwuskładnikowe czy pobiera aplikacje wyłącznie z oficjalnych źródeł. Wciąż zbyt rzadko weryfikujemy także tożsamość rzekomych pracowników banku, co zwiększa ryzyko oszustw typu *vishing* i *spoofing* – jedynie jedna trzecia osób oddzwania bezpośrednio do banku, by potwierdzić autentyczność rozmówcy.

W sytuacji zagrożenia reagujemy zazwyczaj szybko, choć nie zawsze wiemy, gdzie szukać specjalistycznego wsparcia. W przypadku podejrzenia wycieku danych większość osób natychmiast blokuje kartę lub kontaktuje się z bankiem. Ponad połowa zgłosiłaby próbę *phishingu* policji, natomiast niespełna jedna trzecia poinformowałaby o incydencie CERT Polska.

Podsumowując wyniki badania przeprowadzonego przez Warszawski Instytut Bankowości i Związek Banków Polskich, można zauważyć, że postawy Polaków wobec cyberbezpieczeństwa stają się coraz bardziej świadome. Dostrzegamy szerokie spektrum zagrożeń, choć jednocześnie często jesteśmy przekonani, że dotyczą one raczej innych niż nas samych. Coraz więcej osób deklaruje, że wie, jak się przed nimi bronić, jednak wciąż zbyt mała część społeczeństwa zna i konsekwentnie stosuje podstawowe zasady bezpiecznych zachowań w sieci. Z jednej strony doceniamy nowe technologie jako skuteczną tarczę ochronną w cyfrowym świecie, z drugiej nie wykorzystujemy w pełni ich możliwości. Nawet niewielkie zwiększenie wiedzy w zakresie cyberbezpieczeństwa oraz świadomość, że nasze codzienne decyzje online mogą zarówno zwiększać ryzyko, jak i je ograniczać, sprawiają, że czujemy się w sieci pewniej i bezpieczniej[21].

5. Wyzwania, luki i kierunki rozwoju cyberbezpieczeństwa w bankowości

Sektor bankowy znajduje się obecnie w centrum globalnych zagrożeń cybernetycznych. Dynamika rozwoju technologii cyfrowych, rosnąca liczba usług online oraz postępująca automatyzacja procesów finansowych powodują, że cyberbezpieczeństwo stało się jednym z kluczowych filarów stabilności instytucji finansowych. Wyzwania te mają charakter wieloaspektowy – obejmują zarówno zagrożenia technologiczne, jak i regulacyjne, organizacyjne oraz operacyjne[22].

[21] Warszawski Instytut Bankowości, Związek Banków Polskich, 2025, *Raport...,* op. cit.

[22] K. Dmowska. 2022. *Cyberbezpieczeństwo...,* op. cit.; T. Góreczny. 2025. *Współczesna bankowość w Polsce i perspektywy jej rozwoju*, „Nauki Ekonomiczne", 41, https://czasopismanaukowe.mazowiecka.edu.pl/index.php/ne/article/view/585 [dostęp: 13.12.2025].

Rozwój generatywnej sztucznej inteligencji oraz uczenia maszynowego w istotny sposób zmienia funkcjonowanie systemów bezpieczeństwa w sektorze bankowym. Nowoczesne algorytmy pozwalają na analizę ogromnych wolumenów danych transakcyjnych w czasie rzeczywistym, co znacząco zwiększa skuteczność identyfikowania zagrożeń. Dzięki temu możliwe jest szybkie wykrywanie anomalii oraz prób oszustw finansowych, a także automatyzacja procesów monitoringu bezpieczeństwa[23].

Sztuczna inteligencja umożliwia również tworzenie precyzyjnych raportów ryzyka, które wspierają procesy decyzyjne zarządów banków oraz spełnianie wymogów regulacyjnych. W praktyce rozwiązania oparte na AI znajdują zastosowanie między innymi w systemach przeciwdziałania praniu pieniędzy, wykrywaniu fraudów kartowych oraz analizie behawioralnej klientów, co przekłada się na wyższy poziom ochrony zarówno instytucji finansowych, jak i ich klientów. Jednocześnie ta sama technologia może być wykorzystywana przez cyberprzestępców. Generatywna AI umożliwia tworzenie spersonalizowanych kampanii phishingowych, deepfake'ów[24] podszywających się pod członków zarządu czy automatyczne generowanie złośliwego oprogramowania. Choć obecnie tradycyjne metody ataków nadal dominują, banki muszą przygotowywać się na scenariusz, w którym AI stanie się standardowym narzędziem cyberprzestępców[25].

Jednym z najpoważniejszych długoterminowych wyzwań dla sektora finansowego są obliczenia kwantowe. W przyszłości komputery kwantowe mogą potencjalnie zagrozić obecnie stosowanym algorytmom kryptograficznym, które stanowią fundament bezpieczeństwa bankowości elektronicznej. Choć technologia ta nie znajduje się jeszcze na etapie umożliwiającym łamanie współczesnych standardów szyfrowania, sektor bankowy już dziś musi planować migrację do kryptografii postkwantowej (PQC). Strategia ta powinna obejmować identyfikację systemów krytycznych, analizę cyklu życia danych (zwłaszcza tych przechowywanych długoterminowo) oraz ścisłą współpracę z dostawcami technologii nad wdrażaniem algorytmów odpornych na ataki kwantowe. W praktyce oznacza to, że banki muszą myśleć o bezpieczeństwie w perspektywie dekad, a nie wyłącznie w kontekście bieżących zagrożeń[26].

Bankowość pozostaje jednym z najbardziej atrakcyjnych celów dla grup ransomware, a współczesne ataki znacząco wykraczają poza samo szyfrowanie danych. Coraz częściej obejmują one również kradzież informacji, groźby ich ujawnienia

---

[23] N. Siemieniuk, A. Zalewska-Bochenko, 2017, *Bezpieczeństwo systemów...,* op. cit.; A. Narang, P. Vashisht, S. Bhaskar, 2024, *Artificial Intelligence in Banking and Finance*, Amity University, Gurugram, Haryna, India. (https://www.researchgate.net/publication/380119377_Artificial_Intelligence_in_Banking_and_Finance) [dostęp: 13.12.2025].

[24] Deepfake – fałszywy, realistycznie wyglądający obraz, film video lub nagranie dźwiękowe, wygenerowane z użyciem sztucznej inteligencji *Słownik Języka Polskiego* (https://sjp.pl) [dostęp: 13.12.2025].

[25] 2024, *Współczesne wyzwania...,* op. cit.

[26] N. Siemieniuk, A. Zalewska-Bochenko, 2017, *Bezpieczeństwo systemów...,* op. cit.

oraz wielopoziomowe wymuszenia, co zwiększa presję na instytucje finansowe i potęguje skalę potencjalnych strat wizerunkowych oraz finansowych. Dodatkowym wyzwaniem jest dynamiczny rozwój modelu *cybercrime-as-a-service* (CaaS), który umożliwia mniej zaawansowanym przestępcom korzystanie z gotowych narzędzi i infrastruktury do przeprowadzania ataków, a tym samym znacząco zwiększa skalę oraz dostępność zagrożeń. Źródłem podatności w infrastrukturze bankowej są przede wszystkim opóźnienia w aktualizacjach oprogramowania, błędy konfiguracyjne, niewystarczające wydzielenie segmentów sieci oraz ryzyka przenoszone przez systemy partnerów technologicznych. W odpowiedzi na te zagrożenia sektor finansowy coraz częściej wdraża architekturę cyberbezpieczeństwa. Banki wprowadzają wszelakie modele bezpieczeństwa, które dzielą się na rożne segmenty takie jak Zero Trust, który zapobiega włamaniom do systemu, a model SOC 24/7 zajmuje się ciągłym monitoringiem bezpieczeństwa systemów. Instytucje regularnie przeprowadzają testy i ćwiczenia typu *red teaming*, które polegają na symulowanym ataku hakerskim na firmę, tak aby skontrolować, jak działa jej bezpieczeństwo oraz identyfikować jej słabe punkty i szybko eliminować przed rzeczywistymi atakami cyberprzestępców[27].

Dodatkowo sektor bankowy podlega coraz surowszym regulacjom, takim jak unijne rozporządzenia, które w coraz większym stopniu koncentrują się na budowaniu odporności cyfrowej. Ważnym przykładem jest DORA, która dotyczy odporności cyfrowej sektora finansowego, zabezpieczając banki, ubezpieczycieli i inne instytucje finansowe przed cyberatakami oraz awariami systemów IT. Przepisy te określają zasady zarządzania ryzykiem ICT, raportowania incydentów, przeprowadzania testów bezpieczeństwa oraz kontroli nad dostawcami zewnętrznymi. Dzięki temu cyberbezpieczeństwo staje się ważnym elementem zarządzania całym bankiem, a nie tylko kwestią techniczną[28].

Banki coraz częściej opierają swoje modele operacyjne na współpracy z podmiotami zewnętrznymi – dostawcami usług chmurowych, fintechami, firmami IT czy operatorami płatności. Integracja systemów i wymiana danych z partnerami technologicznymi zwiększają jednak powierzchnię potencjalnego ataku, a tym samym poziom ryzyka cybernetycznego[29].

Incydent bezpieczeństwa po stronie jednego dostawcy może wywołać efekt domina, oddziałując na wiele instytucji finansowych jednocześnie i wpływając na stabilność całego sektora. W odpowiedzi na te zagrożenia banki rozwijają kompleksowe podejście do zarządzania ryzykiem stron trzecich. Obejmuje ono w szczególności weryfikację bezpieczeństwa dostawców na etapie wyboru, ciągły monitoring poziomu ryzyka, regularne audyty bezpieczeństwa oraz zawieranie umów uwzględniających szczegółowe klauzule dotyczące cyberbezpieczeństwa i odpowiedzialności za incydenty. W praktyce oznacza to, że odporność banku nie zależy już wyłącznie od jego

[27] 2024. Artykuł publicystyczny *Sektor finansowy...,* op. cit.
[28] *Czym jest DORA?*(Czym jest DORA? | PwC) [dostęp: 13.12.2025].
[29] N. Siemieniuk, A. Zalewska-Bochenko. 2017. *Bezpieczeństwo systemów...,* op. cit.

wewnętrznych systemów i procedur, ale również od zewnętrznych kontrahentów. Dlatego we współpracy pomiędzy tak ważnymi instytucjami ważne jest stawianie na jakość usług, aby każdej ze stron zapewnić bezpieczeństwo na najwyższym poziomie[30].

Podsumowanie

Cyberzagrożenia stanowią dziś jedno z kluczowych wyzwań dla sektora finansowego i użytkowników bankowości elektronicznej. Obejmują one zarówno ataki socjotechniczne, takie jak *phishing*, *pharming* czy *vishing*, jak i zagrożenia techniczne związane ze złośliwym oprogramowaniem, *sniffingiem*, *skimmingiem* oraz atakami typu DDoS. Źródłem tych zagrożeń są nie tylko indywidualni hakerzy i zorganizowane grupy cyberprzestępcze, lecz także czynnik ludzki oraz dynamiczny rozwój sztucznej inteligencji, która umożliwia automatyzację i skalowanie ataków. Szczególnie niebezpiecznym zjawiskiem są współczesne oszustwa finansowe wykorzystujące deepfaki i generatywną AI. Mają one charakter masowy, zautomatyzowany i coraz trudniejszy do wykrycia przy użyciu tradycyjnych metod ochrony. W konsekwencji bezpieczeństwo bankowe nie może opierać się na pojedynczych narzędziach, lecz wymaga zintegrowanego, systemowego podejścia. Obejmuje ono zaawansowany monitoring transakcji, silne mechanizmy uwierzytelniania, szyfrowanie danych, wdrażanie modelu Zero Trust, stały nadzór centrów operacji bezpieczeństwa oraz regularne testy penetracyjne. Istotne znaczenie mają także regulacje prawne, w tym rozporządzenie UE DORA, które nakłada na instytucje finansowe obowiązek budowania rzeczywistej odporności cyfrowej, a nie jedynie formalnej zgodności z przepisami. Badania Warszawskiego Instytutu Bankowości oraz Związku Banków Polskich pokazują, że świadomość Polaków w zakresie cyberbezpieczeństwa systematycznie rośnie. Użytkownicy coraz częściej dostrzegają zagrożenia związane z *phishingiem*, kradzieżą tożsamości, dezinformacją czy wykorzystaniem sztucznej inteligencji w oszustwach. Jednocześnie jednak wielu z nich nie stosuje konsekwentnie podstawowych zasad bezpieczeństwa, takich jak weryfikacja źródeł informacji czy korzystanie z dodatkowych zabezpieczeń, co zwiększa podatność na ataki. W rezultacie skuteczna ochrona bankowości elektronicznej wymaga kompleksowego i wielowymiarowego podejścia, łączącego nowoczesne technologie, odpowiednie regulacje prawne, współpracę międzynarodową oraz systematyczną edukację klientów i pracowników sektora finansowego. Przyszłość bezpieczeństwa finansowego zależy od ciągłej adaptacji do zmieniających się zagrożeń, inwestycji w kompetencje cyfrowe oraz ścisłej współpracy instytucji finansowych z regulatorami i społeczeństwem.

---

[30] *Współczesne wyzwania w zakresie cyberbezpieczeństwa,* 2024, blog (Współczesne wyzwania w zakresie cyberbezpieczeństwa, Nomios Polska) [dostęp: 13.12.2025]; A.T. Oyewole, C.C Okoye, O.C. Ofodile, C.E. Ugochukwu, 2024, *Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio* https://www.researchgate.net/publication/379428581_Cybersecurity_risks_in_online_banking_A_detailed_review_and_preventive_strategies_applicatio [dostęp: 13.12.2025].

Bibliografia

1. *Baza wiedzy* (Aktualności – Baza wiedzy – Portal Gov.pl) [dostęp 13.12.2025].
2. *Bezpieczna łączność dla sektora bankowego w erze cyfrowej*, 2023 (Bezpieczna łączność dla sektora bankowego w erze cyfrowej – 5G: sieci telekomunikacyjne nowej generacji – Portal Gov.pl) [dostęp: 13.12.2025].
3. *Czym jest DORA?*(Czym jest DORA? | PwC) [dostęp: 13.12.2025].
4. Dmowska K. *Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego*, Bank i Kredyt, 2022, nr 4, 2022 (BIK_04_2022_01.pdf) [dostęp: 13.12.2025].
5. Góreczny T., *Współczesna bankowość w Polsce i perspektywy jej rozwoju.* Nauki Ekonomiczne, 2025, https://czasopismanaukowe.mazowiecka.edu.pl/index.php/ne/article/view/585.
6. Górnisiewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej- przestępstwa finansowe związane z bankowością elektroniczną, Poradnik klienta usług KNF*, 2014 *(*Bezp_finansowe_39005.pdf) [dostęp: 13.12.2025].
7. Narang A., Vashisht. P, Bhaskar S., *Artificial Intelligence in Banking and Finance*, Amity University, Gurugram, Haryna, India, 2024 (https://www.researchgate.net/publication/380119377_Artificial_Intelligence_in_Banking_and_Finance) [dostęp: 18.12.2025].
8. Oyewole A.T., Okoye C.C., Ofodile O.C., Ugochukwu C.E. *Cybersecurity risks in online banking: A detailed review and preventive strategies application*, 2024 *(*https://www.researchgate.net/publication/379428581_Cybersecurity_risks_in_online_banking_A_detailed_review_and_preventive_strategies applicatio) [dostęp: 16.12.2025].
9. *Sektor finansowy a cyberzagrożenia – czy nasze pieniądze są bezpieczne*, 2024. https://instytutcyber.pl/artykuly/sektor-finansowy-a-cyberzagrozenia/ [dostęp: 13.12.2025].
10. Siemieniuk N., Zalewska-Bochenko A., *Bezpieczeństwo systemów informatycznych w instytucjach bankowych,* „Roczniki Kolegium Analiz Ekonomicznych"/Szkoła Główna Handlowa, Nr 44, 2017 (roczniki_kae_z44_05.pdf) [dostęp: 13.12.2025].
11. Simola J., Leppanen T., Identification of the Emerging Sources Cybersecurity Threats, University of Jyväskylä, Finland, 2025 (https://www.researchgate.net/publication/393049451_Identification_of_the_Emerging_Sources_of_Cybersecurity_Threats) [dostęp: 18.12.2025].
12. *Słownik Języka Polskiego* (https://sjp.pl) [dostęp: 13.12.2025].
13. *Socjotechnika – dlaczego cyberprzestępcy są skuteczni?*, 2023 (Socjotechnika – dlaczego cyberprzestępcy są skuteczni – Baza wiedzy – Portal Gov.pl) [dostęp: 13.12.2025].

14. Warszawski Instytut Bankowości, Związek Banków Polskich. 2025. *Raport Postawy Polaków wobec cyberbezpieczeństwa 2025* [dostęp: 13.12.2025] Raport_z_badania_Postawy_Polaków_wobec_cyberbezpieczeństwa_2025.pdf https://share.google/LlibRUK6IssYyKq0k [dostęp: 13.12.2025].
15. *Wielki Słownik Języka Polskiego* (https://wsjp.pl) [dostęp: 13.12.2025].
16. Woolacott E., *What Is Phishing? Understanding Cyber Attacks.* Forbes, 2024 (https://www.forbes.com/sites/technology/article/what-is-phishing/) [dostęp: 18.12.2025].
17. *Współczesne wyzwania w zakresie cyberbezpieczeństwa,* 2024, blog (Współczesne wyzwania w zakresie cyberbezpieczeństwa | Nomios Polska) [dostęp: 13.12.2025].

CYBERSECURITY STRATEGIES AND CHALLENGES IN THE BANKING SECTOR

Abstract

The article discusses contemporary threats in electronic banking, including both social engineering attacks and technical threats related to malicious software. Particular attention is given to the growing role of artificial intelligence and generative technologies, which enable the automation of financial fraud and make its detection more difficult using traditional protection methods. Banking highlights the need to apply an integrated approach to security, including advanced transaction monitoring, strong authentication mechanisms, data encryption, and continuous supervision by security operations centers. Legal regulations play a key role in building the real digital resilience of financial institutions. Despite the growing awareness among users, many of them still do not follow basic security principles, which increases their vulnerability to attacks. Effective protection of electronic banking requires a comprehensive, multidimensional approach combining modern technologies, legal regulations, international cooperation, and systematic education of clients and employees in the financial sector.

Keywords: banking, cybersecurity, cyber threats, phishing, financial sector.