Cyberbezpieczeństwo
systemu finansowego

70 LAT WYDAWNICTWA
UNIWERSYTETU EKONOMICZNEGO
WE WROCŁAWIU
1955-2025

Dariusz Wawrzyniak

Cyberbezpieczeństwo systemu finansowego

Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu
Wrocław 2025

Recenzja
Oleksiy Druhov

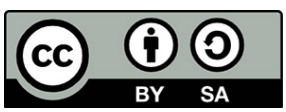
Redakcja wydawnicza
Agnieszka Flasińska

Korekta
Agata Dobosz

Skład i łamanie
Beata Mazur

Projekt okładki
Beata Dębska

Na okładce wykorzystano zdjęcie z zasobów Adobe Stock



ISBN 978-83-68394-96-2 (wersja drukowana)
ISBN 978-83-68394-97-9 (wersja elektroniczna)

DOI: 10.15611/2025.97.9

Cytuj jako: Wawrzyniak, D. (2025). *Cyberbezpieczeństwo systemu finansowego*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Dariusz Wawrzyniak ORCID: 0000-0002-0896-6171

Spis treści

Rozdział 3

Wstęp

Współczesny system finansowy znajduje się w fazie dynamicznych przemian wywołanych intensywnym rozwojem technologii informatycznych. Transformacja cyfrowa nie ogranicza się już do modernizacji infrastruktury informatycznej, lecz obejmuje całościowe przeformułowanie sposobu działania instytucji finansowych, modeli biznesowych oraz architektury ryzyka. Wydaje się, że to właśnie modyfikacja znaczenia poszczególnych rodzajów ryzyka zdefiniuje przyszłość tego systemu. Rodzajem ryzyka, którego znaczenie w praktyce gospodarczej nieustannie wzrasta, jest ryzyko operacyjne. Od momentu, gdy zostało ono formalnie zdefiniowane w dokumentach Komitetu Bazylejskiego, doczekało się wielu interpretacji teoretycznych i praktycznych. Nieco mniej formalne, ale ciekawe podejście opisuje ryzyko operacyjne jako niepożądany koszt prowadzenia działalności gospodarczej (*unwanted cost of doing business*), podkreślając jego nieunikniony i nieplanowany charakter. Współczesna perspektywa zarządzania ryzykiem skłania się jednak ku uznaniu, że problemy wynikające z czynników personalnych, procesowych czy technologicznych nie powinny być traktowane jedynie jako niepożądane skutki uboczne, lecz jako integralny, immanentny element funkcjonowania każdej organizacji. Zwłaszcza aspekty technologiczne, które dynamicznie kształtują warunki konkurencji i definiują standardy usług, determinują obecnie w sposób zasadniczy skuteczność i bezpieczeństwo procesów biznesowych. Obszarem gospodarki, w którym zjawisko to ma bodajże największe znaczenie, są finanse. Tytułowe cyberbezpieczeństwo systemu finansowego jest stanem będącym efektem implementacji technologii, strategii, regulacji, polityk oraz procedur mających na celu ochronę zasobów cyfrowych sektora finansowego przed nieuprawnionym dostępem, zakłóceniami, manipulacjami i zniszczeniem. Cyberbezpieczeństwo obejmuje nie tylko zabezpieczenie infrastruktury teleinformatycznej, lecz także ochronę danych klientów, transakcji finansowych oraz stabilności funkcjonowania rynku. W perspektywie regulacyjnej cyberbezpieczeństwo finansowe jest postrzegane jako kluczowy element odporności sektora finansowego na zagrożenia płynące ze strony zarówno przestępczości zorganizowanej czy legalnych użytkowników systemów, jak i potencjalnych działań o charakterze geopolitycznym.

Książka jest próbą prezentacji wybranych aspektów tego interdyscyplinarnego i niezwykle bogatego merytorycznie zagadnienia. Kompleksowe ujęcie wszystkich problemów w jednym opracowaniu jest już w zasadzie niemożliwe, a literatura przedmiotu obejmująca te problemy, sięgająca od matematycznych podstaw kryptografii, przez teorię i praktykę informatyki, do psychologicznych aspektów bezpieczeństwa – przytłacza swoim ogromem. Co więcej, zakres tych problemów stale się zwiększa. Autor niniejszej publikacji postawił sobie za cel przybliżenie tych zagadnień cyberbezpieczeństwa, które determinują bezpieczeństwo systemu finansowego. Wybór

zagadnień jest pochodną zarówno krytycznej literatury przedmiotu oraz wyników analizy dostępnych obserwacji, jak i subiektywnych przemyśleń autora.

W rozdziale pierwszym ukazano główne trendy technologiczne, które warunkują obecny i przyszły kształt systemu finansowego oraz wpływają na jego stabilność, bezpieczeństwo i odporność operacyjną. Rozdział otwierają ogólne rozważania na temat roli informatyzacji w sektorze finansowym, wskazujące konieczność adaptacji do nowej rzeczywistości cyfrowej. Następnie przedstawiono sześć kluczowych grup technologii: sztuczną inteligencję, Internet rzeczy, *blockchain*, przetwarzanie w chmurze, analizę danych w modelu *Big Data* oraz interfejsy programistyczne. Każda z tych technologii jest analizowana nie tylko z perspektywy funkcjonalnej, lecz także pod kątem zagrożeń i wyzwań dla cyberbezpieczeństwa. Szczególną uwagę poświęcono dualnej naturze innowacji technologicznych: z jednej strony umożliwiają one zwiększenie efektywności operacyjnej, lepszą personalizację usług oraz rozwój nowych modeli biznesowych, z drugiej – generują nowe kategorie ryzyk, wymagających adaptacji istniejących regulacji i modeli kontroli wewnętrznej. W tym kontekście rozdział dostarcza również refleksji nad wpływem technologii na stabilność systemu finansowego, wskazując, że cyberodporność i zdolność do zarządzania złożonymi zagrożeniami informatycznymi stają się integralnymi elementami procesów ukierunkowanych na utrzymywanie długookresowej stabilności, szczególnie w instytucjach finansowych.

Rozdział drugi rozpoczyna się dyskusją terminologiczną. Pomimo wieloletniej już historii publikacji polskojęzycznych z obszaru omawianego zagadnienia podstawowe pojęcia często nadal nie są właściwie interpretowane. Celem rozdziału jest więc usystematyzowanie tych pojęć, a także przedstawienie typowych zagrożeń, które są najbardziej negatywne – w ujęciu zarówno ilościowym, jak i jakościowym – z punktu widzenia stabilności systemu finansowego. Poza ogólną dyskusją na temat zagrożeń, ich systematyki i specyfiki, zaprezentowano bardziej szczegółowo najważniejsze obecnie kategorie zagrożeń cyberbezpieczeństwa: *phishing*, *malware*, ataki typu *denial of service*, ryzyka związane z wykorzystaniem chmury obliczeniowej, wysoce zaawansowane i ukierunkowane kampanie znane jako *advanced persistent threats* oraz zagrożenia wynikające z rozwoju algorytmów sztucznej inteligencji. Rozdział opisuje nie tylko charakter tych zagrożeń, ale także ich wpływ na podatności systemu finansowego oraz mechanizmy, dzięki którym mogą się one rozprzestrzeniać w ekosystemie finansowym. Oprócz systematycznego ujęcia omawianej problematyki rozdział zawiera także krótką analizę wybranych przypadków ukierunkowaną na prezentację destrukcyjnego potencjału zagrożeń cyberbezpieczeństwa. Zaprezentowano również systematykę środków ochrony, a zawarta w rozdziale dyskusja nad problemem transmisyjności zagrożeń jest oryginalnym ujęciem rzadko poruszanego w literaturze zagadnienia. Rozdział zawiera wiele krytycznych i subiektywnych opinii autora, wynikających z wyników badań, a także z własnych obserwacji.

Determinanty cyberbezpieczeństwa systemu finansowego stanowią zbiór czynników, które w sposób istotny warunkują poziom ochrony infrastruktury krytycznej oraz zapewniają odporność na coraz bardziej zaawansowane cyberzagrożenia. W związku

z rosnącą złożonością środowiska technologicznego w sektorze finansowym identyfikacja i analiza tych determinant stają się niezbędne zarówno dla teoretyków, jak i dla praktyków zajmujących się bezpieczeństwem informatycznym. W rozdziale trzecim omówiono kluczowe obszary determinujące poziom bezpieczeństwa systemu finansowego. Wyboru obszarów dokonano w oparciu o krytyczną analizę raportów branżowych prezentujących jak najbardziej kompleksowo aktualne statystyki zagrożeń, a także na podstawie przeglądu narracyjnego, dającego autorowi pole do własnych interpretacji i wniosków.

Szczególną uwagę poświęcono zagadnieniom związanym z silnym uwierzytelnieniem, w tym kontroli dostępu, technikom weryfikacji tożsamości użytkowników oraz stosowanym metodom uwierzytelniania. Wskazano kierunki rozwoju metod uwierzytelniania, które powinny systematycznie eliminować hasła statyczne i wadliwe rozwiązania biometryczne. Kolejne części rozdziału podkreślają znaczenie edukacji i świadomości informatycznej uczestników rynku finansowego, wskazując, że czynnik ludzki nadal pozostaje jednym z najsłabszych ogniw cyberochrony. Zaprezentowane zostały liczne wyniki badań obejmujących różne aspekty edukacyjne i świadomościowe, co posłużyło do sformułowania ważnych wniosków. Bardzo istotnym elementem rozważań zawartych w rozdziale jest również rola kryptografii, w tym wyzwań związanych z rozwojem komputerów kwantowych i algorytmów postkwantowych, a także znaczenie złożoności obliczeniowej jako fundamentu współczesnego cyberbezpieczeństwa. Rozdział zamyka omówienie możliwości wykorzystania sztucznej inteligencji w systemach wykrywania włamań, co stanowi jeden z najbardziej perspektywicznych kierunków rozwoju technologii zabezpieczeń w sektorze finansowym.

Wspólnym mianownikiem prezentowanych w książce treści pozostaje narracyjny przegląd literatury, oparty na aktualnych źródłach naukowych, uzupełniony autorskimi refleksjami oraz subiektywną oceną omawianych zjawisk. Autor wyraża przekonanie, iż taka forma prezentacji problematyki przyczyni się do lepszego zrozumienia tematu i zostanie przychylnie odebrana przez grono Czytelników.

Rozdział 1
System finansowy w obliczu informatyzacji

1.1. Wprowadzenie

System finansowy[1] podlega dynamicznym zmianom pod wpływem rozwoju technologii informacyjno-komunikacyjnych. Postępujące procesy globalizacji oraz intensywna cyfryzacja struktur gospodarczych stanowią fundamentalne determinanty jego transformacji. Wobec rosnącej presji ze strony innowacyjnych podmiotów z rynku fintech[2], a także zmieniających się oczekiwań klientów w zakresie dostępności, personalizacji i szybkości usług, tradycyjne instytucje finansowe zmuszone są do rekonfiguracji swoich modeli biznesowych w kierunku adaptacji nowoczesnych technologii informatycznych. Transformacja ta nie ma charakteru czysto technologicznego – wiąże się również z redefinicją strategii organizacyjnej, modeli zarządzania ryzykiem czy mechanizmów zgodności z regulacjami prawnymi, w tym normami sektorowymi. Wzrost znaczenia i powszechności technologii informatycznych postawił sektor finansowy przed szeregiem wyzwań, które wymagają systematycznych analiz i strategii adaptacyjnych. Cyfryzacja stanowi kluczowy filar współczesnej gospodarki, a sektor finansowy jest jednym z jej największych beneficjentów, dynamicznie adaptując innowacyjne technologie w celu optymalizacji procesów oraz podnoszenia efektywności usług, ale także w kontekście walki konkurencyjnej. Rozwój bankowości internetowej, mobilnych systemów płatniczych, przetwarzania w chmurze, technologii łańcucha bloków oraz algorytmów sztucznej inteligencji fundamentalnie przekształcił sposób interakcji użytkowników z instytucjami finansowymi. Współczesne rozwiązania technologiczne zapewniają klientom nie tylko większą wygodę i szybkość realizacji transakcji, lecz także nieprzerwaną dostępność do usług finansowych, niezależnie od barier geograficznych czy czasowych. Instytucje finansowe, wdrażając zaawansowane narzędzia cyfrowe, dążą do optymalizacji procesów operacyjnych oraz redukcji kosztów i jednocześnie podnoszą poziom satysfakcji użytkowników. Zjawiska te mają jednak też swoją negatywną stronę. Wraz z rosnącą zależnością sektora finansowe-

[1] W niniejszej książce pojęcia „system finansowy" oraz „sektor finansowy" są stosowane zamiennie, przy pełnej świadomości różnic semantycznych i zakresowych między nimi. Zjawisko cyberbezpieczeństwa analizowane jest w ujęciu holistycznym – obejmuje zarówno poszczególne instytucje finansowe, jak i relacje zachodzące pomiędzy nimi, ramy regulacyjne, a także interakcje z uczestnikami rynku, w szczególności z odbiorcami produktów i usług finansowych.

[2] Pod tą ogólną nazwą kryje się sektor rynku oraz rozwiązania przez ten sektor oferowane, związane z innowacjami finansowymi wykorzystującymi nowe technologie informatyczne.

go od technologii cyfrowych obserwuje się równie dynamiczny wzrost liczby i skali zagrożeń cybernetycznych. Zjawisko to nie jest nowe – jego początki sięgają ostatnich dekad XX w., kiedy to zaczęto dostrzegać, że systemy informatyczne staną się nie tylko fundamentem funkcjonowania, lecz także katalizatorem rozwoju globalnej gospodarki. Ostatnie trzy dziesięciolecia to okres nieprzerwanej ekspansji technologii cyfrowych w sektorze finansowym, której nieodłącznym skutkiem ubocznym jest ewolucja zagrożeń cybernetycznych. Równolegle z postępem technologicznym następuje rozwój coraz bardziej wyrafinowanych metod, narzędzi i mechanizmów wykorzystywanych w atakach na infrastrukturę finansową, dlatego też zagadnienia związane z cyberbezpieczeństwem dawno już nabrały strategicznego znaczenia, nie tylko dla pojedynczych instytucji finansowych, lecz także dla stabilności całego systemu finansowego, będącego tworem podlegającym dynamicznym procesom rozwojowym, uwarunkowanym w głównej mierze aspektami technologicznymi.

Wspomniana już cyfryzacja, będąca ciągłym procesem konwergencji rzeczywistego i wirtualnego świata, stała się głównym motorem innowacji i zmian w większości sektorów gospodarki. Należy podkreślić, że zjawisko cyfryzacji można postrzegać z wielu różnych perspektyw. Najczęściej definiuje się cyfryzację jako proces rozpowszechniania i popularyzacji technologii cyfrowych (PWN, b.d.). Coraz istotniejsza jest jednak identyfikacja kontekstu, w jakim oceniamy procesy cyfryzacyjne. Jak podkreślają Brennen i Kreiss (2016), cyfryzacja nie ogranicza się jedynie do wdrażania technologii informacyjno-komunikacyjnych, lecz wiąże się również z głębokimi zmianami organizacyjnymi, kulturowymi i społecznymi. Autorzy ci zwracają uwagę, że proces ten modyfikuje logikę funkcjonowania instytucji, modeli biznesowych oraz samego rozumienia wartości w gospodarce. Ponadto, na przykład według Parviainena i in. (2017), cyfryzacja powinna być rozpatrywana jako wielowymiarowy proces transformacyjny, obejmujący zarówno zmiany technologiczne, jak i adaptacyjne zdolności organizacji do wykorzystywania danych, automatyzacji i sztucznej inteligencji.

Do najważniejszych kontekstów analizy współczesnych procesów cyfryzacji gospodarki należy zaliczyć:

- kontekst ekonomiczny, podkreślający zwiększenie konkurencyjności i innowacyjności przedsiębiorstw (Kuźnar, 2019),
- kontekst strategiczny, opisujący cyfryzację jako intencjonalny proces zarządczy, mający na celu dostosowanie działalności przedsiębiorstw do dynamicznego środowiska technologicznego (Klimczak i in., 2022),
- kontekst administracyjny, odnoszący się do implementacji usług cyfrowych w administracji publicznej.

Uzupełnieniem tych perspektyw jest również kontekst społeczny, który uwzględnia wpływ cyfryzacji na zmiany wzorców zachowań konsumentów, a także kształtowanie nowych kompetencji cyfrowych wśród uczestników rynku. Istotny pozostaje ponadto kontekst prawny, obejmujący regulacje dotyczące bezpieczeństwa danych,

prywatności oraz interoperacyjności systemów cyfrowych. Wielowymiarowa analiza cyfryzacji pozwala dzięki temu lepiej zrozumieć jej konsekwencje dla funkcjonowania współczesnych organizacji i całego ekosystemu gospodarczego.

1.2. Rozwój technologii informatycznych

1.2.1. Transformacja cyfrowa świata finansów

Współczesny system finansowy funkcjonuje w dynamicznie zmieniającym się otoczeniu technologicznym, którego intensyfikacja w ostatnich dekadach radykalnie przekształciła mechanizmy operacyjne, instytucjonalne i regulacyjne. Rozwój technologii informacyjno-komunikacyjnych, sztucznej inteligencji, rozproszonego rejestru danych, automatyzacji procesów oraz inżynierii danych wprowadza nowe paradygmaty zarówno w sposobie świadczenia usług finansowych, jak i w zakresie kształtowania relacji między uczestnikami rynku, w formowaniu ryzyk systemowych czy w projektowaniu instrumentów polityki nadzorczej. Transformacja ta ma charakter nie tylko ilościowy – polegający na zwiększeniu efektywności czy szybkości operacji – lecz przede wszystkim jakościowy, wpływając na strukturę i logikę funkcjonowania całego systemu.

W tradycyjnym ujęciu system finansowy opiera się na zaufaniu do instytucji pośredniczących – takich jak banki, giełdy czy fundusze inwestycyjne – które pełnią funkcje transmisji kapitału, alokacji ryzyka oraz zapewnienia płynności. W miarę postępu technologicznego rola tych instytucji podlega jednak stopniowej rekonfiguracji: pojawiają się nowe podmioty (np. fintechy, platformy *peer-to-peer*, giełdy kryptowalut), nowe formy instrumentów finansowych (np. tokeny cyfrowe, *stablecoins*), a także nowe modele pośrednictwa, zautomatyzowane i algorytmiczne. Znaczne przesunięcie funkcji finansowych do środowiska cyfrowego sprawia, że infrastruktura technologiczna staje się nieodłączną częścią struktury systemu finansowego – do tego stopnia, że granice między sektorem finansowym a sektorem technologicznym zaczynają się zacierać. Rozwój technologiczny prowadzi również do intensyfikacji tzw. efektów sieciowych – zjawisk, w których wartość i siła danego rozwiązania rośnie wraz z liczbą jego użytkowników (Lickus, 2012, s. 181 i n.). Przejawia się to m.in. w konsolidacji danych w globalnych platformach płatniczych czy hegemonii dużych korporacji technologicznych. Taka koncentracja władzy informacyjnej i infrastrukturalnej rodzi nowe wyzwania systemowe, gdyż zakłócenia w działaniu tych kluczowych węzłów mogą mieć globalne skutki dla płynności, zaufania i ciągłości operacji finansowych. Koncentracja ta ma także coraz więcej implikacji podatkowych, społecznych, a nawet politycznych. Jej przyszłość nie jest więc przewidywalna.

Niezwykle istotnym aspektem transformacji cyfrowej jest także zmiana w charakterze ryzyka finansowego. Tradycyjne modele ryzyka – oparte na zmienności cen aktywów, niewypłacalności kredytobiorców czy zmianach stóp procentowych – muszą

zostać uzupełnione o nowe klasy ryzyk operacyjnych, w szczególności technologicznych, związanych przede wszystkim z (Buckley i in., 2019):

- cyberzagrożeniami,
- zawodnością algorytmów,
- nieprzejrzystością modeli sztucznej inteligencji,
- podatnościami systemowymi w łańcuchach dostaw,
- asymetriami informacyjnymi związanymi z automatyzacją decyzji inwestycyjnych.

Te nowe ryzyka są trudniejsze do modelowania, charakteryzują się permanentną zmianą kluczowych atrybutów, a ich efekty mogą się kumulować w sposób nieliniowy. Co więcej, mają charakter transgraniczny, co czyni je problemem o wymiarze nie tylko narodowym, lecz także globalnym. Należy również podkreślić, że ryzyka z grupy technologicznych nigdy nie były łatwe w szacowaniu i ten ich atrybut staje się coraz silniejszy[3]. Pochodną wzrostu znaczenia ryzyk technologicznych jest także ryzyko reputacyjne, trudno definiowalne i charakteryzujące się nieprzewidywalnym wpływem na funkcjonowanie instytucji finansowych, szczególnie banków komercyjnych[4]. W odpowiedzi na te zjawiska regulatorzy oraz instytucje nadzorcze podejmują próby dostosowania narzędzi analitycznych i legislacyjnych do nowych realiów. Powstają instytucje zajmujące się oceną ryzyka systemowego w środowisku cyfrowym (np. jednostki do spraw technologii finansowej w bankach centralnych), a także nowe ramy prawne dotyczące m.in. sztucznej inteligencji, przejrzystości algorytmów, ochrony danych i odpowiedzialności za mechanizmy automatycznego podejmowania decyzji. Tempo rozwoju regulacji nie zawsze jednak nadąża za dynamiką innowacji technologicznych, co prowadzi do powstawania luk regulacyjnych i wzrostu asymetrii między możliwościami technologii a zdolnością instytucjonalną do ich nadzorowania. Do najbardziej aktualnych źródeł regulacyjnych związanych z szeroko rozumianym cyberbezpieczeństwem systemu finansowego w Europie należy zaliczyć[5]:

- Digital Operational Resilience Act (DORA) – rozporządzenie wprowadzające jednolite wymagania dla banków, instytucji płatniczych i ubezpieczeniowych, funduszy inwestycyjnych, giełd, fintechów i podmiotów infrastruktury rynku w celu ujednolicenia i wzmocnienia odporności cyfrowej instytucji finansowych w UE

[3] Jednym z przejawów rozwoju technologicznego jest brak praktycznej możliwości wykorzystywania danych historycznych. Przykładowo, zdarzenia ryzyka informatycznego sprzed kilku lat dziś mogą już nie występować w ogóle lub być zastąpione innymi, o różnej specyfice.

[4] Coraz więcej badań wskazuje, że istotnym elementem budowania zaufania klientów do instytucji finansowych jest wysoki poziom zabezpieczeń informatycznych oraz brak informacji o naruszeniach cyberbezpieczeństwa; zob. np. (Laxman i in., 2024, s. 205 i n.).

[5] Liczba regulacji, norm i standardów stale rośnie. Nie każdy dokument tego typu ma istotne znaczenie dla omawianego zagadnienia. Warto jednak zauważyć, że w niektórych przypadkach obserwujemy proces odwrotny. Przykładowo, Komisja Nadzoru Finansowego wycofała obowiązującą od wielu lat Rekomendację D, argumentując tę decyzję zbieżnością zakresu przedmiotowego Rekomendacji z obowiązkami wynikającymi z Rozporządzenia DORA oraz powiązanych z nim aktów wykonawczych (KNF, 2024).

wobec zagrożeń informatycznych, w tym cyberataków i awarii technologicznych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554…);
- Dyrektywę NIS2 uzupełniającą DORA w zakresie cyberbezpieczeństwa infrastruktury krytycznej, w tym usług finansowych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555…);
- *Guidelines on ICT and Security Risk Management* – wytyczne European Banking Authority dla banków dotyczące zarządzania ryzykiem informatycznym (EBA, 2025).

Z perspektywy instytucji finansowych adaptacja do zmian technologicznych staje się nie tylko kwestią konkurencyjności, ale także przetrwania. Jednocześnie rośnie znaczenie strategicznego zarządzania transformacją technologiczną jako elementu odporności organizacyjnej i ryzyka reputacyjnego. Instytucje, które nie są w stanie efektywnie zarządzać transformacją cyfrową, mogą stać się ofiarą tzw. zjawiska wyparcia technologicznego (*technological displacement*), tracąc zdolność do utrzymania relacji z klientami oraz płynności operacyjnej. Warto również zauważyć, że rozwój technologiczny wpływa na strukturę całej gospodarki, modyfikując relacje między systemem finansowym a realną sferą ekonomiczną. Z jednej strony nowe technologie pozwalają na lepszą alokację kapitału i na szybszy dostęp do finansowania dla małych i średnich przedsiębiorstw oraz zwiększają inkluzywność finansową, z drugiej jednak permanentnie generują nowe problemy na gruncie prawa, edukacji, a przede wszystkim bezpieczeństwa. Wpływ rozwoju technologicznego na funkcjonowanie systemu finansowego należy zatem postrzegać jako złożony proces transformacji, w którym zmieniają się zarówno narzędzia, jak i fundamenty logiki działania systemu. Analiza tego wpływu wymaga podejścia interdyscyplinarnego – łączącego ekonomię, prawo, nauki o zarządzaniu, informatykę i teorię systemów złożonych – oraz nowego podejścia metodologicznego, uwzględniającego zmienność, nieprzewidywalność i emergentność współczesnych zjawisk finansowych. W tym kontekście dalsze badania nad implikacjami technologii dla stabilności systemu finansowego stają się nie tylko uzasadnione, ale wręcz konieczne z perspektywy długoterminowego bezpieczeństwa gospodarczego.

Najważniejszymi determinantami rozwoju gospodarki cyfrowej w obszarze finansowym są obecnie (Basel Committee on Banking Supervision, 2024; Pieriegud, 2016):

- zastosowania sztucznej inteligencji (*Artificial Intelligence*, AI),
- cyberbezpieczeństwo oparte na AI (*AI-driven cybersecurity*),
- Internet rzeczy (*Internet of Things* – IoT) oraz Internet wszechrzeczy (*Internet of Everything* – IoE),
- wszechobecna łączność (*hyperconnectivity*),
- aplikacje i usługi oparte na chmurze obliczeniowej (*cloud computing*),
- analityka dużych zbiorów danych (*Big Data Analytics* – BDA) oraz związane z nimi usługi (*Big-Data-as-a-Service* – BDaaS),
- automatyzacja (*automation*) oraz robotyzacja (*robotisation*),

- wielokanałowe (*multi-channel*) oraz wszechkanałowe (*omni-channel*) modele dystrybucji produktów i usług,
- implementacje rozwiązań wykorzystujących technologię łańcucha bloków (*blockchain*),
- rozwój komputerów kwantowych,
- sztuczna inteligencja kwantowa (*Quantum AI*),
- rozwój technologii rozszerzonej rzeczywistości (*Augmented Reality* – AR) i rzeczywistości wirtualnej (*Virtual Reality* – VR),
- *edge computing*[6] i analiza danych w czasie rzeczywistym,
- zdecentralizowane finanse i fintech 4.0[7],
- personalizacja oparta na analizie behawioralnej,
- integracja mediów społecznościowych z systemami finansowymi.

Lista nie obejmuje z pewnością wszystkich obszarów, które kreują zmiany w systemie finansowym, mimo to jej zakres merytoryczny przytłacza, ukazując jednoznacznie wszechobecność oraz nadrzędność zastosowań informatyki, także tam, gdzie jeszcze do niedawna obecność czynnika ludzkiego wydawała się nieodzowna. Szczegółowy opis wszystkich powyższych zjawisk i technologii wykraczałby poza ramy merytoryczne książki, w dalszej części rozdziału przedstawiono jednak krótką charakterystykę wybranych determinant.

1.2.2. Sztuczna inteligencja

Sztuczna inteligencja[8] stanowi obecnie jeden z kluczowych czynników transformujących sektor finansowy i wyznacza nowe kierunki rozwoju gospodarki cyfrowej.

[6] Przetwarzanie brzegowe – architektura przetwarzania danych, która polega na przesuwaniu części obliczeń z centralnych centrów danych (np. chmury) bliżej źródła danych, czyli do urządzeń końcowych lub lokalnych węzłów sieci.

[7] Autor książki nie jest zwolennikiem wersjonowania zjawisk ekonomicznych i informatycznych, szczególnie w tych przypadkach, w których dynamika i ciągłość rozwoju nie tworzą w sposób jednoznaczny granic pomiędzy postulowanymi wersjami. Literatura przedmiotu, szczególnie nastawiona na większy krąg odbiorców, preferuje jednak takie podejście; zob. np. (Surabhi i Shiva, 2024, s. 49 i n.).

[8] Dynamika rozwoju narzędzi zaliczanych do obszaru sztucznej inteligencji generatywnej oraz ich stosunkowo szybkie upowszechnienie – w szczególności fascynacja modelami językowymi – odsunęły na dalszy plan krytyczną analizę samego zjawiska oraz jego kontekst historyczny. Pojęcie sztucznej inteligencji po raz pierwszy zostało oficjalnie użyte w 1956 r. podczas legendarnej konferencji w Dartmouth College w Hanowerze, w stanie New Hampshire (USA). Celem konferencji było zbadanie możliwości stworzenia maszyny zdolnej do „symulowania inteligencji ludzkiej". To wydarzenie uważane jest za symboliczny początek dziedziny sztucznej inteligencji jako samodzielnej dyscypliny naukowej, chociaż warto zauważyć, że pierwsza publikacja pioniera tej dyscypliny pochodzi z 1950 r. (Turing, 1950). Początkowo obszarem zainteresowań dyscypliny były systemy eksperckie oraz modele językowe. Nieco symbolicznym – ze względu na kontrowersje związane z samym wydarzeniem – jednak niezwykle ważnym w procesie rozwoju narzędzi sztucznej inteligencji było zwycięstwo komputera Deep Blue nad ówczesnym mistrzem świata w szachach Kasparowem.

Jej wdrażanie zmienia fundamentalne obszary działalności instytucji finansowych, wpływając na sposób zarządzania ryzykiem, wykrywania oszustw, obsługi klienta oraz funkcjonowania rynków kapitałowych. Dzięki dynamicznemu rozwojowi metod uczenia maszynowego, głębokiego uczenia, przetwarzania języka naturalnego oraz technik generatywnych instytucje finansowe zyskują możliwość przetwarzania ogromnych wolumenów danych w czasie rzeczywistym, optymalizacji procesów decyzyjnych oraz tworzenia usług opartych na personalizacji i automatyzacji. Do ważniejszych obszarów implementacji sztucznej inteligencji należą zarządzanie ryzykiem i analiza predykcyjna. Tradycyjne modele oparte na metodach statystycznych, takich jak regresja logistyczna czy klasyczne scoringi kredytowe, są dziś coraz częściej zastępowane przez bardziej zaawansowane podejścia oparte na sieciach neuronowych, które umożliwiają identyfikację złożonych, nieliniowych zależności, np. w danych dotyczących kredytów (Giudici i Raffinetti, 2023). Co więcej, zastosowanie generatywnej AI pozwala na analizę raportów finansowych i przewidywanie kondycji przedsiębiorstw na podstawie sentymentu zawartego w narracjach zarządczych (Chen i in., 2023). Dodatkowo uczenie ze wzmocnieniem ma zastosowanie w dynamicznej optymalizacji polityk kredytowych na podstawie historycznych wyników (Feng, 2024). Zgodnie z badaniami Xu i in. (2024) wdrożenie AI w systemach oceny ryzyka kredytowego przynosi wzrost dokładności prognoz niewypłacalności o 20%, co znacznie ogranicza ryzyko kredytowe. Jednocześnie AI jest wykorzystywana do analizy ryzyka rynkowego, w szczególności przez monitorowanie zmienności cen aktywów, identyfikację anomalii oraz predykcję zawirowań gospodarczych. W tym kontekście instytucje finansowe implementują zaawansowane metody NLP[9] do analizy treści raportów giełdowych i wiadomości ekonomicznych, umożliwiając ocenę nastrojów inwestorów w czasie rzeczywistym (Giudici i in., 2024). Modele probabilistyczne, takie jak sieci bayesowskie, wspierają modelowanie niepewności, techniki *Big Data Analytics* natomiast pozwalają na wykrywanie potencjalnych baniek spekulacyjnych przez analizę milionów transakcji dziennie (Feng, 2024).

Innym istotnym zastosowaniem AI w finansach jest detekcja oszustw. Dzięki zastosowaniu algorytmów klasyfikacyjnych oraz technik wykrywania anomalii możliwa jest identyfikacja odstających wzorców transakcyjnych, które mogą wskazywać na próbę wyłudzenia lub prania pieniędzy (Dhieb i in., 2020). AI uczy się na bieżąco i potrafi

Współczesna przewaga programów komputerowych nad ludzkim umysłem w grach logicznych nadal jest przedmiotem dyskusji nad istotą sztucznej inteligencji, a ściślej rzecz ujmując, istotą relacji między inteligencją a świadomością. Analizując rolę narzędzi sztucznej inteligencji w sektorze finansowym, warto zwrócić także uwagę, że pojęcie stało się na tyle modne i powszechnie rozpoznawane, że wielu producentów sprzętu i oprogramowania korzysta z niego, nie tworząc w rzeczywistości rozwiązań innowacyjnych. Niniejsza książka posługuje się pojęciem sztucznej inteligencji w odniesieniu do wielu różnych rozwiązań informatycznych z pełną świadomością nadużywania tego terminu przez rynek producentów oprogramowania.

[9] Metody NLP (*Natural Language Processing*, czyli przetwarzanie języka naturalnego) to techniki i algorytmy, które umożliwiają komputerom analizowanie i rozumienie ludzkiego języka, a następnie generowanie tekstu.

dynamicznie dostosowywać reguły detekcji do nowych schematów ataków, co stanowi znaczną przewagę nad tradycyjnymi, statycznymi systemami regułowymi. Jak pokazują Xu i in. (2024), wdrożenie AI umożliwiło redukcję liczby fałszywych alarmów o 60% oraz zwiększenie skuteczności wykrywania oszustw o 40%, co przekłada się na wymierne korzyści finansowe i reputacyjne.

AI odgrywa również kluczową rolę w rozwoju handlu algorytmicznego, umożliwiając natychmiastową analizę danych rynkowych i automatyczne podejmowanie decyzji inwestycyjnych. Modele uczenia ze wzmocnieniem są w stanie adaptować się do zmieniających się warunków rynkowych, a generatywne sieci neuronowe służą do symulacji scenariuszy giełdowych oraz testowania strategii inwestycyjnych. Równolegle rozwija się analiza sentymentu – technologie takie jak BERT (*Bidirectional Encoder Representations from Transformers*) pozwalają analizować emocjonalne tło publikacji giełdowych, co ułatwia prognozowanie zachowań inwestorów (Giudici i in., 2024).

W obszarze relacji z klientami AI zrewolucjonizowała sposób świadczenia usług poprzez wdrożenie chatbotów i wirtualnych asystentów, które dostępne są przez cały czas i umożliwiają natychmiastową reakcję na potrzeby użytkowników. Badania Fenga (2024) wykazały, że implementacja chatbotów doprowadziła do wzrostu retencji klientów o 40% oraz zwiększenia korzystania z bankowości mobilnej o 25%. Systemy te potrafią nie tylko obsługiwać podstawowe zapytania (np. sprawdzenie salda, wykonanie przelewu), lecz także świadczyć usługi doradcze, analizując dane klienta i rekomendując odpowiednie produkty finansowe. Coraz częściej wykorzystuje się tu modele generatywne, które umożliwiają bardziej naturalną i kontekstową konwersację (Chen i in., 2023).

AI wspiera również personalizację ofert bankowych – algorytmy rekomendacyjne analizują dane behawioralne, transakcyjne oraz kontekstowe, aby dostosować produkty do indywidualnych potrzeb klienta. Możliwe są na przykład prognozowanie nadchodzących wydatków, ostrzeganie przed przekroczeniem budżetu, a także dynamiczne ustalanie limitów kredytowych i proponowanie strategii inwestycyjnych dopasowanych do profilu ryzyka użytkownika. Taka hiperpersonalizacja zwiększa lojalność klientów i skuteczność działań marketingowych, stając się jednym z najważniejszych trendów w cyfrowej bankowości.

AI ma zastosowanie również w zaawansowanych systemach cyberbezpieczeństwa. Temat ten będzie przedmiotem dalszych rozdziałów. Pomimo licznych korzyści wynikających z wdrożenia sztucznej inteligencji istotne pozostają wyzwania związane z etyką, prywatnością danych, przejrzystością algorytmów oraz akceptacją społeczną. Niektóre grupy klientów preferują tradycyjne kanały kontaktu, a ograniczenia technologii NLP mogą prowadzić do nieporozumień. W odpowiedzi na te wyzwania rozwijane są koncepcje przezroczystej AI (*Explainable AI* – XAI), której celem jest zwiększenie zaufania użytkowników do systemów inteligentnych. W rezultacie sztuczna inteligencja staje się nieodzownym elementem infrastruktury finansowej, transformując modele operacyjne, strategie zarządzania oraz sposoby interakcji

z klientami. Jej rola będzie wzrastać i najprawdopodobniej stanie się czynnikiem warunkującym konkurencyjność i innowacyjność sektora finansowego w dobie gospodarki cyfrowej (Tyagi i in., 2025).

1.2.3. Internet rzeczy

Internet rzeczy (*Internet of Things* – IoT) zyskuje coraz większe znaczenie jako jeden z kluczowych katalizatorów transformacji cyfrowej sektora finansowego. Zjawisko to można opisać jako system połączonych ze sobą urządzeń fizycznych wyposażonych w czujniki, oprogramowanie oraz inne technologie, umożliwiające im zbieranie i wymianę danych przez sieć Internet w celu podejmowania decyzji, automatyzacji procesów i zwiększenia efektywności. Integracja IoT z usługami finansowymi prowadzi do usprawnienia procesów operacyjnych, poprawy doświadczenia klienta, a także zwiększenia bezpieczeństwa i efektywności zarządzania ryzykiem. Pomimo tego, że większość literatury przedmiotu koncentruje się na podejściach koncepcyjnych lub wczesnych wdrożeniach, dostępne analizy ukazują potencjał tej technologii do fundamentalnego przeobrażenia sposobu działania instytucji finansowych (Karmańska, 2021, s. 23 i n.). Zastosowanie IoT w finansach przyczynia się przede wszystkim do wzrostu efektywności operacyjnej poprzez automatyzację zadań, przetwarzanie danych w czasie rzeczywistym oraz lepsze zarządzanie zasobami. Badania empiryczne del Giudice i in. (2016) wykazały, że instytucje oferujące usługi zintegrowane z IoT osiągały wyższy wskaźnik zwrotu z kapitału, co potwierdza ekonomiczny sens ich wdrożenia.

Efektywne zarządzanie zasobami materialnymi w instytucjach finansowych, w tym w zakresie zarządzania infrastrukturą i obiektami, również zyskuje dzięki IoT. Höhenberger i Redlein (2020) wskazują, że integracja czujników środowiskowych umożliwia monitorowanie zużycia energii, zarządzanie zasobami informatycznymi oraz planowanie konserwacji predykcyjnej. Cytowana już Karmańska (2021) dodaje, że systemy śledzenia aktywów oparte na IoT wspomagają zarządzanie majątkiem trwałym oraz kontrolę jakości danych księgowych. W rezultacie podejmowanie decyzji operacyjnych staje się bardziej dynamiczne i oparte na faktach, co podkreślają także inni badacze (Allioui i Mourdi, 2023). IoT wpływa również na przekształcenie relacji z klientami, oferując nowe możliwości w zakresie personalizacji, natychmiastowego reagowania na potrzeby użytkowników oraz kreowania innowacyjnych modeli obsługi. Arora i Kaur (2020) zauważają, że dzięki IoT możliwe jest dostosowywanie ofert do indywidualnych preferencji klientów, a także optymalizacja ścieżek użytkownika w kanałach mobilnych oraz przewidywanie potrzeb klientów na podstawie analizy danych behawioralnych. IoT umożliwia również zbieranie i analizę danych dotyczących zachowań użytkowników w czasie rzeczywistym, co ma zastosowanie m.in. w systemach doradztwa finansowego oraz zarządzania kontem osobistym (Ramalingam i Venkatesan, 2019). Dostarczanie rekomendacji opartych na analizie bieżącej aktywności klienta znacznie poprawia jakość obsługi oraz umożliwia tworzenie dynamicznych modeli scoringowych.

Jedną z bardziej obiecujących ścieżek rozwoju jest integracja IoT z usługami cyfrowymi w celu zwiększenia inkluzywności finansowej. Według Thirumagala i in. (2024) zastosowanie tanich urządzeń IoT oraz aplikacji mobilnych umożliwia dostęp do usług finansowych dla osób z wykluczonych obszarów geograficznych. Bansal i in. (2021) wskazują z kolei rozwój modelu bankowości mobilnej, w którym IoT umożliwia obsługę klienta w modelu *anytime, anywhere*, co szczególnie przyczynia się do zwiększenia satysfakcji użytkowników. Zastosowanie IoT w zarządzaniu ryzykiem kredytowym i ubezpieczeniowym pozwala na ciągłą analizę sytuacji klienta dzięki sensorom zainstalowanym w pojazdach, nieruchomościach czy urządzeniach noszonych (Schulte i Liu, 2017). Zbierane w ten sposób dane wspierają dynamiczną ocenę ryzyka oraz umożliwiają lepsze dopasowanie ofert kredytowych lub polis ubezpieczeniowych w ramach koncepcji *pay-as-you-live*[10].

Z punktu widzenia bezpieczeństwa i zarządzania ryzykiem IoT oferuje liczne mechanizmy wspierające detekcję nadużyć, poprawę cyberbezpieczeństwa oraz zgodność z regulacjami. Lande i in. (2018) podkreślają, że monitoring w czasie rzeczywistym umożliwia wczesne wykrywanie prób oszustwa finansowego, co przekłada się na obniżenie strat instytucji. Johri i in. (2023) zwracają uwagę na możliwość integracji systemów identyfikacji biometrycznej oraz nadzoru wideo w celu zwiększenia kontroli dostępu do danych i zasobów fizycznych. Jednakże, jak zauważają Shepherd i in. (2017), IoT wprowadza również nowe ryzyka bezpieczeństwa – sieci czujników mogą stać się celem ataków hakerskich, dlatego konieczne jest wdrażanie zaawansowanych strategii ochrony danych i systemów. Skuteczne wdrożenie IoT w sektorze finansowym wymaga zatem zaawansowanej infrastruktury technologicznej. W literaturze wskazuje się kluczową rolę chmury obliczeniowej, platform *Software-as-a-Service* (SaaS), rozwiązań do przechowywania i przetwarzania danych, a także integracji z systemami AI (Arora i Kaur, 2020).

Wśród wyzwań implementacyjnych, jakie nadal stoją przed IoT, dominują: integracja z innymi systemami, brak standardów danych, problemy ze skalowalnością oraz złożoność integracji międzydziałowej[11] (Zhang i in., 2017). Wdrożenia wymagają także strategicznego podejścia, zgodności z regulacjami prawnymi oraz współpracy z partnerami technologicznymi (Schulte i Liu, 2017). IoT stanowi kluczowy komponent transformacji sektora finansowego, wnosząc wartość w trzech fundamentalnych obszarach: efektywności operacyjnej, innowacyjności usług oraz zarządzania

[10] To wyjątkowo ciekawa koncepcja. Jest to nowoczesny model ustalania składek ubezpieczeniowych, który polega na ich kalkulacji w oparciu o bieżące, indywidualne zachowania ubezpieczonego. W odróżnieniu od klasycznych modeli opartych na statystycznie uśrednionych profilach ryzyka, *pay-as-you-live* wykorzystuje rzeczywiste dane o stylu życia, np. aktywności fizycznej, sposobie odżywiania czy parametrach zdrowotnych, pozyskiwane z urządzeń noszonych lub aplikacji mobilnych. Takie podejście pozwala bardziej precyzyjnie dostosować wysokość składki do faktycznego poziomu ryzyka, co zwiększa poczucie sprawiedliwości wśród klientów, a jednocześnie motywuje ich do prozdrowotnych zachowań; zob. np. (Małek, 2020, s. 177 i n.).

[11] Współdziałanie i połączenie systemów, procesów lub danych pomiędzy różnymi działami (np. organizacyjnymi, biznesowymi lub technologicznymi) w ramach jednej organizacji.

ryzykiem. Choć większość analiz ma charakter koncepcyjny, dostępne badania jednoznacznie wskazują potencjał tej technologii do zwiększania rentowności, poprawy doświadczenia klienta i wzmacniania bezpieczeństwa. Wymaga to jednak rozwoju odpowiedniej infrastruktury, strategii implementacyjnych oraz wzmocnienia regulacji i mechanizmów ochrony danych. W dłuższej perspektywie IoT może nie tylko wspierać konkurencyjność instytucji finansowych, ale także sprzyjać inkluzywności i transparentności globalnych rynków kapitałowych.

1.2.4. *Blockchain*

Wraz ze wzrostem popularności kryptowaluty bitcoin, której początki datuje się na 2009 r., odnotowano dynamiczny wzrost zainteresowania technologią rozproszonego rejestru (*Distributed Ledger Technology* – DLT), powszechnie znaną pod nazwą „łańcuch bloków" (*blockchain*). Ten stosunkowo krótki, lecz wyjątkowo intensywny okres fascynacji nowatorskim podejściem do rejestrowania i weryfikowania transakcji cechował się eksplozją badań akademickich, eksperymentów technologicznych oraz prób praktycznego wdrożenia rozwiązań wykorzystujących *blockchain* w różnych sektorach gospodarki.

Blockchain można zdefiniować jako rozproszoną, zdecentralizowaną bazę danych, pozbawioną jednostki centralnej, wykorzystującą zaawansowane, kryptograficzne środki ochrony poufności, integralności i autentyczności oraz mechanizm tzw. konsensusu – algorytmu, który zapewnia wiarygodny zapis historii transakcji, dzięki czemu historia ta jest wspólna i w pełni dostępna dla wszystkich użytkowników oraz nie jest podatna na żadne modyfikacje. W kategoriach technicznych można postrzegać technologię łańcucha bloków jako rozproszoną bazę danych działającą w architekturze *peer-to-peer*, niewymagającą istnienia centrum przetwarzania, wykorzystującą kryptografię asymetryczną i jednokierunkowe funkcje skrótu oraz zapewniającą brak praktycznej możliwości modyfikacji i usuwania danych. Kryptoekonomiczny punkt widzenia skupia się natomiast na istniejących w łańcuchach bloków mechanizmach konsensusu, takich jak *Proof-of-Work* czy *Proof-of-Stake*, oraz poszukiwaniu nowych mechanizmów, niekoniecznie uniwersalnych, ale spełniających wymagania zastosowań w określonych obszarach. Złożoność problematyki *blockchain*, zarówno teoretyczna, jak i praktyczna, a także prawna, dość skutecznie niweluje próby stworzenia jednoznacznych i kategorycznych ram klasyfikacyjnych i definicyjnych. Co więcej, fundamentalne założenia koncepcji łańcucha bloków nierzadko są modyfikowane pod kątem wartości dodanych, jakie implementacja *blockchain* może stworzyć w danej branży czy danym podmiocie gospodarczym. Przypisanie jakiegoś rozwiązania do obszaru *blockchain* nie jest zatem wystarczające do identyfikacji jego cech, zarówno technologicznych, jak i organizacyjnych. Istnieje natomiast zbiór fundamentów, które w zależności od wymagań mogą być w różnym zakresie wykorzystywane. Fundamenty te zaprezentowano w tabeli 1.

Tabela 1. Fundamentalne założenia koncepcji *blockchain*

Cecha	Opis
Autonomia	Istnienie mechanizmów konsensusu daje pełną autonomię wszystkim węzłom sieci.
Anonimowość	*Blockchain* zapewnia pełne bezpieczeństwo transakcji przy zachowaniu anonimowości jej stron. Podmioty w sieci identyfikowane są tylko przez klucze publiczne.
Cyberodporność	W przeciwieństwie do tradycyjnych, zcentralizowanych systemów informatycznych *blockchain* jest praktycznie niemożliwy do zniszczenia. Dane sieci *blockchain* można zniszczyć jedynie przez zniszczenie wszystkich węzłów sieci.
Decentralizacja	Sieć *blockchain* nie zakłada istnienia elementu centralnego. Wszystkie węzły sieci mają takie same uprawnienia i nie istnieje konieczność wyróżniania jakiegokolwiek z nich.
Dezintermediacja	*Blockchain* eliminuje konieczność istnienia pośredników. Dotyczy to zarówno transakcji finansowych, jak i realizacji warunków umów.
Mechanizm konsensusu	Decentralizacja oraz dezintermediacja nie byłyby możliwe do osiągnięcia bez kryptoekonomicznego mechanizmu konsensusu, który – zaakceptowany przez wszystkich użytkowników – gwarantuje poprawność walidacji danych oraz prawidłowości ich rejestrowania.
Niemodyfikowalność	Dane zarejestrowane i uznane przez sieć *blockchain* za poprawne w praktyce nie podlegają modyfikacji. To jedna z najbardziej nowatorskich cech odróżniających *blockchain* od tradycyjnych systemów.
Otwarte oprogramowanie	Większość środowisk *blockchain* funkcjonuje w ramach koncepcji *open source*, czyli otwartego oprogramowania, dzięki czemu możliwe jest tworzenie wielu różnych rozwiązań wykorzystujących to samo środowisko.
Transparentność	Dane w *blockchain* są dostępne dla wszystkich węzłów sieci.
Zastosowanie algorytmów kryptograficznych	*Blockchain* wykorzystuje algorytmy kryptograficzne w celu zapewnienia bezpieczeństwa transakcji oraz uniemożliwienia modyfikacji zarejestrowanych przez sieć danych. Są to jednokierunkowe funkcje skrótu oraz algorytmy asymetryczne.

Źródło: opracowanie własne na podstawie (Lin i Liao, 2017).

Szczególnie podatnym gruntem dla rozwoju technologii *blockchain* okazał się sektor finansowy, w którym *blockchain* został początkowo entuzjastycznie przyjęty jako potencjalne panaceum na szereg istniejących problemów strukturalnych, w tym m.in. zagrożenia związane z cyberatakami, brakiem transparentności procesów czy wysokimi kosztami pośrednictwa. Warto jednak zauważyć, że wiele z tych oczekiwań miało charakter wysoce spekulatywny i nie zostało poparte empirycznymi dowodami. Zwłaszcza wizja *blockchain* jako uniwersalnego rozwiązania systemowego nie uwzględniała głębokich różnic między logiką funkcjonowania systemów zdecentra-

lizowanych a zasadami działania scentralizowanych struktur finansowych, takich jak banki komercyjne, centralne izby rozliczeniowe czy instytucje nadzorcze, o bankach centralnych nie wspominając. Fundamentalną cechą sieci *blockchain* jest bowiem decentralizacja, zakładająca brak zaufanego pośrednika i opierająca się na mechanizmach kryptograficznej weryfikacji oraz jakiejś formy rozproszonego konsensusu. Tego typu założenia stoją w jawnej sprzeczności z modelem operacyjnym instytucji finansowych, który opiera się na centralnym przetwarzaniu danych, jednoznacznej odpowiedzialności prawnej oraz regulacjach zapewniających przejrzystość i bezpieczeństwo transakcji. W konsekwencji, pomimo początkowej euforii, technologia *blockchain* nie doprowadziła do rewolucji systemowej w sektorze finansowym. Jej wpływ ograniczył się raczej do wprowadzenia lokalnych innowacji i udoskonaleń – głównie w zakresie cyfryzacji procesów, tokenizacji oraz zwiększenia zainteresowania alternatywnymi modelami transakcyjnymi, takimi jak zdecentralizowane finanse.

Znaczna część literatury akademickiej koncentruje się na potencjalnych korzyściach wynikających z zastosowania technologii łańcucha bloków w kontekście finansowym. Do najczęściej podkreślanych należą: redukcja kosztów operacyjnych przez eliminację pośredników i automatyzację procesów, skrócenie czasu potrzebnego na finalizację i rozliczenie transakcji, a także ogólny wzrost efektywności dzięki większej przejrzystości i niezmienności danych (Chiu i Koeppl, 2018). Pomimo tych potencjalnych atutów należy jednak zaznaczyć, że związek między implementacją technologii *blockchain* a wspomnianymi korzyściami nie jest jednoznaczny. W rzeczywistości wiele z tych zalet można osiągnąć także poprzez zastosowanie tradycyjnych narzędzi informatycznych, wzbogaconych jedynie o pewne funkcjonalności wykorzystujące istniejące od dawna technologie[12].

Niewątpliwie jedną z unikalnych cech technologii *blockchain*, która wyróżnia ją spośród innych rozwiązań, jest całkowita decentralizacja, eliminująca potrzebę istnienia centralnego ośrodka weryfikacji i przechowywania danych. To zaś rodzi konieczność opracowania nowych modeli konsensusu w środowiskach *peer-to-peer*, takich jak *Proof-of-Work* czy *Proof-of-Stake* – uznawanych za jedne z kluczowych innowacji tej technologii, niemniej również ten aspekt technologiczny napotyka poważne ograniczenia w kontekście zastosowań w scentralizowanych systemach bankowych, które z definicji wymagają jednoznacznych ram prawnych, hierarchii odpowiedzialności oraz centralnych węzłów decyzyjnych[13].

---

[12] Na przykład często eksponowany atrybut niezmienności danych historycznych jest możliwy do osiągnięcia w praktycznie każdym współczesnym systemie informatycznym, bez konieczności zastępowania go łańcuchem bloków. Kwestią dyskusyjną pozostaje jedynie centralny charakter przetwarzania.

[13] *Proof-of-Work* (PoW) jest jednym z najwcześniej stosowanych i najbardziej rozpowszechnionych mechanizmów konsensusu w sieciach *blockchain*. Jego głównym celem jest zapewnienie integralności i bezpieczeństwa rozproszonego rejestru, umożliwiając uczestnikom sieci wspólne uzgadnianie stanu łańcucha bloków bez potrzeby istnienia zaufanego centralnego organu. W modelu PoW weryfikacja nowych bloków odbywa się poprzez poszukiwanie rozwiązania złożonego –

Integracja koncepcji *blockchain* z istniejącą infrastrukturą finansową jest procesem złożonym i wielowymiarowym, wymagającym nie tylko adaptacji technologicznej, lecz także głębokiej przebudowy procesów biznesowych oraz struktury organizacyjnej instytucji. Jak wskazują Chiu i Koeppl (2018), *blockchain* nie jest rozwiązaniem typu *plug-and-play* – jego wdrożenie wymaga kompleksowego reengineeringu, co z kolei powoduje znaczne koszty transformacyjne oraz ryzyko operacyjne. Dodatkowo brak pełnej interoperacyjności między blockchainem a tradycyjnymi systemami transakcyjnymi stanowi istotną barierę dla szerokiego zastosowania technologii (Chiu i Koeppl, 2018). Jednym z kluczowych wyzwań jest również kwestia skalowalności. Jak zauważają Khan i State (2020), systemy bankowe operujące na ogromną skalę muszą być w stanie obsługiwać dziesiątki tysięcy transakcji na sekundę przy zachowaniu spójności danych, niskich opóźnień i wysokiej dostępności. Aktualne rozwiązania wykorzystujące koncepcję *blockchain*, szczególnie te oparte na konsensusie *Proof-of-Work*, nie spełniają jeszcze tych wymogów w stopniu satysfakcjonującym dla instytucji finansowych.

Podsumowując, należy podkreślić, że przegląd literatury wskazuje na potrzebę przyjęcia elastycznego podejścia do wdrażania technologii *blockchain* w sektorze finansowym. Kluczowe jest uwzględnienie specyfiki operacyjnej, wymogów regulacyjnych oraz dojrzałości technologicznej poszczególnych instytucji. W tym kontekście wskazane jest projektowanie rozwiązań szytych na miarę, które nie próbują bezkrytycznie implementować rozwiązań znanych z obszaru kryptowalutowego, lecz selektywnie adaptują elementy technologii *blockchain* tam, gdzie faktycznie mogą one przynieść wymierne korzyści.

1.2.5. *Cloud computing*

Rozwój technologii chmurowych (*cloud computing*) stanowi jeden z kluczowych wektorów transformacji cyfrowej w sektorze finansowym. Zastosowanie rozwiązań chmurowych w systemie finansowym nie tylko zwiększa efektywność operacyjną instytucji, lecz także redefiniuje fundamenty działania systemów bankowych, płatniczych, ubezpieczeniowych oraz inwestycyjnych. *Cloud computing* przekształca sposób przetwarzania danych, zarządzania infrastrukturą informatyczną i świadczenia usług, oferując jednocześnie skalowalność, elastyczność oraz nowe możliwości analityczne, w tym integrację z technologiami sztucznej inteligencji i uczenia maszynowego. Naturalną korzyścią wynikającą z zastosowań rozwiązań chmurowych jest znaczna

---

w sensie obliczeniowym – problemu matematycznego. Kluczową cechą PoW jest asymetria: proces wytworzenia dowodu pracy jest kosztowny i czasochłonny, natomiast jego weryfikacja przez pozostałych uczestników sieci – szybka i tania. Model PoW, zastosowany m.in. w protokole Bitcoin (Nakamoto, 2008), stał się fundamentem dla pierwszych generacji sieci *blockchain*, jednak ze względu na wysokie zużycie energii i ograniczenia skalowalności coraz częściej jest zastępowany lub uzupełniany przez bardziej efektywne mechanizmy konsensusu, takie jak *Proof-of-Stake* (PoS) czy *Delegated Proof-of-Stake* (DPoS); zob. np. (Narayanan i in., 2016).

redukcja konieczności zarządzania lokalną infrastrukturą informatyczną, w wymiarze zarówno sprzętowym, jak i programowym. W literaturze wskazuje się także, że jednym z najważniejszych obszarów zastosowania chmury w finansach jest wykrywanie oszustw i przeciwdziałanie nadużyciom w czasie rzeczywistym. Choudhary (2025) przedstawia studium przypadków ilustrujących, jak analiza danych w chmurze, połączona z algorytmami AI, umożliwia wykrywanie podejrzanych transakcji w czasie rzeczywistym i redukcję fałszywych alarmów w procesach monitorowania. Dzięki zastosowaniu infrastruktury chmurowej możliwe jest zbieranie, analizowanie i korelowanie ogromnych wolumenów danych transakcyjnych z wielu kanałów i źródeł, co wcześniej było logistycznie i kosztowo nieosiągalne w modelach lokalnych. Zastosowania *cloud computing* obejmują również zaawansowane modele analityczne na potrzeby zarządzania ryzykiem, oceny zdolności kredytowej, optymalizacji portfeli inwestycyjnych oraz predykcyjnej analizy zachowań klientów. Badania Vegesny (2025) pokazują, że chmura obliczeniowa umożliwia implementację złożonych modeli opartych na danych behawioralnych, historycznych i rynkowych przy zachowaniu niskich kosztów obliczeniowych oraz szybkiego wdrażania. Zdolność szybkiego przetwarzania danych (np. przez platformy typu PaaS) otwiera nowe możliwości w dziedzinie personalizacji usług finansowych, mikrotargetowania oraz modelowania scenariuszy stresowych. *Cloud computing* wprowadza także istotne zmiany w architekturze technicznej i bezpieczeństwie danych w sektorze finansowym. Tradycyjne instytucje muszą dostosować swoje systemy do hybrydowych lub w pełni chmurowych środowisk, co rodzi zarówno korzyści, jak i wyzwania. Współczesna bankowość coraz częściej korzysta z rozwiązań typu *multi-cloud*, które pozwalają dywersyfikować infrastrukturę i unikać uzależnienia od pojedynczego dostawcy. Z punktu widzenia systemowego chmura obliczeniowa wpływa także na funkcjonowanie banków centralnych oraz instytucji nadzorczych. Na przykład Gahane i in. (2025) wskazują, że systemy *cloud-based* wykorzystywane są w monitorowaniu rynków finansowych, przetwarzaniu danych makroekonomicznych oraz testowaniu scenariuszy polityki monetarnej z wykorzystaniem modeli predykcyjnych. Możliwość przechowywania i analizy ogromnych zbiorów danych w czasie zbliżonym do rzeczywistego zwiększa zdolność organów publicznych do reagowania na zagrożenia i niestabilności rynkowe, co ma bezpośredni wpływ na stabilność finansową państw. Z chmurą związane są również nowe zjawiska w zakresie usług płatniczych i finansów konsumenckich. Platformy fintechowe, takie jak Revolut, Stripe, Adyen czy Nubank, opierają swoje operacje w dużej mierze na infrastrukturze chmurowej, co pozwala im konkurować z bankami o znacznie większym potencjale. Według Salampasisa (2025) coraz większa rola dostawców usług finansowych opartych na chmurze prowadzi do redefinicji łańcucha wartości w finansach – przesuwa nacisk z infrastruktury i fizycznej obecności na elastyczność, szybkość wdrażania oraz zdolność do integracji z systemami zewnętrznymi. Wdrażanie rozwiązań *cloud computing* w sektorze finansowym wymaga jednak ostrożności i odpowiedniego przygotowania. Istotne są kwestie lokalizacji danych, przetwarzania informacji w jurysdykcjach zróżnicowanych regulacyjnie, jak również odporność

na awarie i ataki typu blokowania usług. Tao i in. (2025) zauważają, że chmura może zwiększyć odporność instytucji finansowych dzięki redundancji systemów, ale jednocześnie wymaga znacznie bardziej zaawansowanego podejścia do architektury bezpieczeństwa i zarządzania dostępem. Znaczenie takich rozwiązań, jak zarządzanie tożsamością w chmurze, szyfrowanie homomorficzne oraz segmentacja danych na poziomie aplikacyjnym, staje się coraz większe.

Podsumowując, można zauważyć, że zastosowania *cloud computing* w systemie finansowym są szerokie, głęboko transformacyjne i stale się rozwijają. Obejmują nie tylko usprawnienia operacyjne, lecz także strategiczne zmiany w sposobie działania instytucji, zarządzania ryzykiem oraz interakcji z klientami. Przyszłość sektora finansowego w dużej mierze zależeć będzie od zdolności jego uczestników do skutecznego i bezpiecznego wykorzystania potencjału chmury.

1.2.6. *Big Data*

Współczesny system finansowy coraz intensywniej opiera się na danych jako podstawowym zasobie strategicznym. Wraz z cyfryzacją gospodarki instytucje finansowe generują, przetwarzają i analizują olbrzymie wolumeny danych – zarówno strukturalnych, jak i niestrukturalnych – które pochodzą z rozmaitych źródeł: transakcji klientów, zapisów giełdowych, mediów społecznościowych, danych geolokalizacyjnych, rejestrów kredytowych czy czujników IoT. W tym kontekście technologia *Big Data*, definiowana przez swoje kluczowe cechy, takie jak: wielkość (*volume*), zmienność (*velocity*), różnorodność (*variety*), wiarygodność (*veracity*) i wartość (*value*), staje się fundamentem nowej architektury zarządzania finansami i podejmowania decyzji inwestycyjnych (Tabakow i in., 2014, s. 138 i n.). Zastosowania *Big Data* w systemie finansowym mają charakter wielowymiarowy. Jednym z najbardziej rozwiniętych obszarów jest wykrywanie nadużyć finansowych oraz przeciwdziałanie praniu pieniędzy. Analiza anomalii i wzorców transakcyjnych w czasie rzeczywistym pozwala identyfikować nietypowe zachowania klientów, które mogą świadczyć o oszustwach lub działaniach niezgodnych z prawem. Bokkena (2024) wykazuje, że zaawansowane techniki analizy *Big Data*, oparte na modelach predykcyjnych i uczeniu maszynowym, przewyższają tradycyjne metody regułowe pod względem skuteczności i redukcji fałszywych alarmów. Kolejnym istotnym zastosowaniem jest ocena zdolności kredytowej klientów, szczególnie w przypadku osób i podmiotów niemających historii kredytowej w tradycyjnych bazach danych. Dzięki analizie alternatywnych źródeł danych – takich jak historia płatności za media, aktywność w Internecie czy geolokalizacja – instytucje finansowe mogą rozszerzać dostęp do finansowania dla wcześniej wykluczonych grup społecznych. Przykłady takich rozwiązań funkcjonują już w praktyce, szczególnie w krajach rozwijających się, gdzie *Big Data* odgrywa kluczową rolę w procesie tzw. inkluzywności finansowej. Nie mniej istotnym obszarem jest analiza nastrojów rynkowych, w szczególności w kontekście podejmowania decyzji inwestycyjnych. Jadhav i Mirza (2025) przedstawiają wykorzystanie dużych modeli języko-

wych do przetwarzania treści medialnych, analiz raportów analitycznych i wpisów w mediach społecznościowych, co umożliwia ocenę zbiorowych emocji inwestorów i próby przewidywania zmian cen akcji. Integracja *Big Data* z analizą semantyczną pozwala generować tzw. sygnały predykcyjne na podstawie informacji, które wcześniej były trudno mierzalne lub niedostępne. Zdolność do szybkiego przetwarzania i korelowania dużych zbiorów danych znajduje także zastosowanie w zarządzaniu ryzykiem systemowym. Jak podkreślają Basha i in. (2025), modele predykcyjne oparte na *Big Data* pozwalają na symulację scenariuszy rynkowych z uwzględnieniem danych historycznych, makroekonomicznych i mikrozachowań uczestników rynku. Dzięki temu banki centralne i instytucje nadzorcze mogą z większą precyzją przewidywać skutki potencjalnych wstrząsów oraz projektować odpowiednie mechanizmy przeciwdziałania destabilizacji.

Big Data wykorzystywany jest również w zarządzaniu relacjami z klientami, personalizacji usług oraz tworzeniu dynamicznych modeli segmentacji użytkowników. Luong i in. (2025) analizują, w jaki sposób algorytmy uczenia maszynowego oparte na zbiorach *Big Data* umożliwiają przewidywanie tzw. *customer churn*, czyli ryzyka odejścia klienta, co z kolei pozwala na wdrażanie strategii prewencyjnych i zwiększenie retencji, a także może być podstawą konstruowania modeli zarządzania ryzykiem reputacyjnym. Takie podejście staje się szczególnie istotne w sektorze bankowości detalicznej, gdzie konkurencja o lojalność klienta staje się coraz bardziej intensywna. W kontekście giełd i platform tradingowych *Big Data* służy do automatyzacji podejmowania decyzji inwestycyjnych. Modele *quantitative trading* czy *high-frequency trading* są oparte na błyskawicznej analizie danych rynkowych i podejmowaniu decyzji w ciągu ułamków sekund. Warto także zauważyć, że *Big Data* ma zastosowanie w nadzorze finansowym oraz tworzeniu tzw. regtechów (*regulatory technologies*). Systemy te umożliwiają automatyzację procesów raportowania, identyfikację ryzyk prawnych, ocenę zgodności operacji z przepisami prawa oraz wspierają audyty i kontrolę wewnętrzną. Karina i in. (2025) zwracają uwagę na znaczenie integracji omawianej technologii w systemach zarządzania wydajnością, które wpływają na efektywność nadzoru i jakość decyzji strategicznych. Choć zalety *Big Data* są bezsprzeczne, nie należy pomijać zagrożeń związanych z jego wykorzystaniem. Wśród najczęściej podnoszonych kwestii znajdują się: ochrona prywatności, przejrzystość algorytmów, ryzyko błędów systemowych oraz zagrożenia związane z bezpieczeństwem danych. Williams i in. (2021) wskazują, że mimo znaczących postępów w detekcji nadużyć technologia *Big Data* wciąż wymaga rozwoju w zakresie odporności na błędy predykcyjne i cyberataki.

Podsumowując, warto zauważyć, że *Big Data* stanowi jeden z najważniejszych czynników transformujących współczesny system finansowy. Jego zastosowania obejmują niemal każdy aspekt działalności finansowej: od zapobiegania oszustwom, przez analitykę ryzyka, po automatyzację decyzji inwestycyjnych i personalizację usług. W miarę dalszego rozwoju technik obliczeniowych, sztucznej inteligencji oraz regulacji danych rola tej technologii będzie tylko rosła, tworząc nowe możliwości, ale także wyzwania dla stabilności, przejrzystości i zrównoważonego rozwoju sektora finansowego.

1.2.7. *Application Programming Interfaces* (API)

Szczególnie wymownym przejawem dynamiki rozwoju technologicznego współczesnego sektora finansowego jest wzrost liczby interfejsów programistycznych (*Application Programming Interfaces* – API), czyli rozwiązań, które umożliwiają komunikowanie się systemów między sobą. Zakres wykorzystania API w danej branży może wręcz stanowić miarę jej dojrzałości technologicznej. W systemach bankowych oraz płatniczych API są standardem od wielu lat, a na ich powszechność wpłynęła dodatkowo opublikowana pod koniec 2019 r. dyrektywa unijna PSD2, tzw. Payment Services Directive (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366…), otwierająca drogę do implementacji koncepcji *open banking* (Leżoń, 2019). API to zestaw jasno określonych reguł i standardów, które umożliwiają aplikacjom wzajemną komunikację i wymianę danych. API definiuje strukturę żądań i odpowiedzi między komponentami oprogramowania, eliminując konieczność poznawania szczegółów działania drugiego systemu. Dzięki temu aplikacje mogą korzystać z funkcji lub danych innego systemu w sposób ustandaryzowany i bezpieczny. W praktyce API działa jako warstwa pośrednia, która obsługuje zapytania klientów (np. aplikacji mobilnej) do serwera i przesyła odpowiedzi. Najpopularniejsze architektury API to:

- REST (*Representational State Transfer*) – oparty na protokole HTTP, prosty, łatwy w implementacji i szeroko stosowany w aplikacjach internetowych,
- SOAP (*Simple Object Access Protocol*) – bardziej formalny, oparty na XML, często wykorzystywany w systemach korporacyjnych,
- GraphQL – nowoczesne podejście pozwalające klientowi definiować dokładnie, jakie dane chce otrzymać, ograniczając nadmiarowe transfery danych.

Interfejsy programistyczne umożliwiają bezpieczną i automatyczną wymianę danych pomiędzy systemami, nawet jeżeli są to systemy o bardzo wysokich wymaganiach dotyczących bezpieczeństwa (Zachariadis i Ozcan, 2017). Potencjał tej automatyzacji jest jednak ogromny, a o efektach można będzie mówić najprawdopodobniej w kontekście zmian o charakterze rewolucyjnym. Analiza trendu wykorzystania API nakazuje mówić dziś o zjawisku zwanym *API Economy*[14]. Jest to nowoczesny model gospodarki cyfrowej, w którym interfejsy programowania aplikacji stają się kluczowym zasobem biznesowym. W tym modelu organizacje udostępniają funkcje, dane i procesy poprzez API innym podmiotom – partnerom, klientom lub twórcom aplikacji – co pozwala tworzyć nowe usługi, zwiększać interoperacyjność i przyspieszać transformację cyfrową. Wśród kluczowych cech *API Economy* wyróżnia się (Chen, 2025; *A New Frontier*…, 2022):

- platformizację usług: organizacje przekształcają się w platformy oferujące zestawy funkcji dostępnych przez API,
- monetyzację API: interfejsy stają się nowym strumieniem przychodów,

[14] Globalny rynek bankowości opartej na API został oszacowany na 3,5 mld USD w 2023 r. i przewiduje się, że osiągnie ok. 17,5 mld USD do 2032 r., zwiększając się w średnim tempie rocznym wynoszącym ok. 23% w latach 2023-2032; zob. np. (Purnell, 2025).

- ekosystemowość: API umożliwia szybkie tworzenie partnerstw B2B i B2C,
- wzrost innowacyjności: firmy mogą łatwo integrować zewnętrzne technologie.

Jednym ze skutków dynamicznego rozwoju implementacji API w systemie finansowym będzie równie dynamiczny rozwój zjawiska *embedded finance*, związanego z integracją usług finansowych (np. płatności, kredytów, ubezpieczeń, inwestycji) bezpośrednio w niebankowych platformach i aplikacjach – takich jak sklepy internetowe, platformy *e-commerce*, aplikacje mobilne czy serwisy społecznościowe (Ozili, 2023).

1.3. Wpływ rozwoju technologii na stabilność systemu finansowego

Kryzysy finansowe od zawsze wpływały destrukcyjnie na procesy ekonomiczno-społeczne. Obawy przed kryzysami nie wyeliminowały wprawdzie z życia gospodarczego zjawisk powodujących kryzysy, zdeterminowały jednak w naturalny sposób cel funkcjonowania systemów i instytucji, jakim jest ich długookresowa stabilność. Stabilność systemu finansowego jest współcześnie dobrem nadrzędnym i chociaż ciągle trudno zdefiniować ją w sposób uniwersalny, to potrafimy identyfikować zdarzenia, procesy i działania, które mają potencjał jej zakłócania. Najczęściej wśród prób definicji pojęcia stabilności systemu finansowego można odnaleźć te, które kładą nacisk na efektywne i sprawne realizowanie przez system swych funkcji oraz możliwość wywiązywania się instytucji finansowych ze zobowiązań. Złożoność zagadnienia wprowadziła do rozważań naukowych także odwrotny kierunek terminologiczny, związany z definiowaniem niestabilności finansowej czy też kryzysu finansowego jako stanu przeciwstawnego trudno definiowalnej stabilności. Podejście takie jednak tylko pozornie tworzy wartość dodaną. Wydaje się, że najprostszą i jednocześnie najlepiej oddającą istotę problemu definicją jest ta, zgodnie z którą stabilność finansowa to stan systemu finansowego, w którym system ten pełni swoje funkcje w sposób ciągły i efektywny. Często definicja ta jest rozbudowywana o uwagę dotyczącą ciągłości i efektywności nawet w przypadkach wystąpienia nieoczekiwanych i niekorzystnych zdarzeń, ale wydaje się, że jest to rozszerzenie nadmiarowe i logicznie nieuzasadnione. Koncepcja stabilnego systemu finansowego przewiduje również, że w przypadku wystąpienia poważnych zakłóceń system jest w stanie samodzielnie powracać do stanu równowagi bez interwencji z zewnątrz. Te modelowe założenia są permanentnie weryfikowane przez praktykę gospodarczą, co nie oznacza, że ich merytoryczny wymiar traci znaczenie. Stabilność systemu finansowego najczęściej jest charakteryzowana przez zestaw różnych miar ekonomicznych, odnoszących się głównie do polityki pieniężnej i fiskalnej, a także miar makroekonomicznych (Czechowska i in., 2020). Warto jednak podkreślić, że stabilność ta determinowana jest także przez czynniki nieekonomiczne, wśród których wymienia się najczęściej politykę, kwestie prawne, konflikty zbrojne, zmiany demograficzne, klimatyczne, ostatnio także uwarunkowania pandemiczne.

Niewątpliwie jednak czynnikiem nieekonomicznym o znaczeniu nadrzędnym jest cyfryzacja i jej wpływ na systemy wykorzystywane przez instytucje finansowe oraz ich użytkowników. Warto wspomnieć również społeczny aspekt omawianego zagadnienia. Zmiany technologiczne często utożsamia się ze zmianami społecznymi, a przecież ich dynamika jest zupełnie różna. Cyfryzacja jest dla pokolenia X czymś koniecznym – nierzadko trudnym, dla pokolenia Y czymś naturalnym – lecz niekoniecznie zrozumiałym, a pokolenie Z po prostu wzrastało razem z procesami cyfryzacji w różnych dziedzinach gospodarki – chociaż to wcale nie oznacza świadomości znaczenia tych procesów. Czynnikami sprawczymi cyfryzacji są nie tylko technologia, konkurencja czy reputacja. Wyniki badań ekonomicznych nie pozostawiają wątpliwości – podmioty ukierunkowane na rozwój zastosowań informatyki i podporządkowujące temu rozwojowi zmiany modeli biznesowych osiągają lepsze wyniki finansowe niż podmioty, które starają się tylko biernie nadążać za trendami (Iansiti i Lakhani, 2019).

Warunkiem realizacji procesów transformacji cyfrowej w sektorze finansowym jest implementacja rozwiązań informatycznych wspomagających wszystkie procesy biznesowe realizowane przez instytucje w tym sektorze funkcjonujące. Systemy informatyczne nie są już jedynie narzędziami, ale wręcz immanentnymi elementami każdego procesu, które nie tylko otwierają nowe możliwości, lecz warunkują poprawne funkcjonowanie świata finansów. Specyfika zastosowań informatyki nakazuje traktować te elementy jako odrębną i newralgiczną kategorię czynników wpływających na stabilność systemu finansowego. O specyfice tej decydują przede wszystkim następujące uwarunkowania:

- dynamiczny, nieliniowy i nieprzewidywalny rozwój technologii informatycznych oraz związany z nim nieprzewidywalny charakter i zakres zagrożeń bezpieczeństwa informatycznego,
- niesubstytucyjność większości systemów informatycznych wykorzystywanych przez instytucje finansowe,
- konieczność wspierania transformacji procesów biznesowych instytucji finansowych przez podmioty trzecie[15],
- nieznajomość konsekwencji wielu potencjalnych zdarzeń związanych z problemami bezpieczeństwa informatycznego,
- podatność większości systemów informatycznych na fizyczną destrukcję[16],
- niedostępność narzędzi zarządzania ryzykiem reputacyjnym,

---

[15] Konieczność taka wynika nie tylko z problemów natury merytorycznej, lecz także z wdrażania koncepcji *open banking*.

[16] Ten aspekt omawianego problemu nierzadko jest pomijany. Wprawdzie współczesna informatyka stworzyła wiele narzędzi ukierunkowanych na zachowanie ciągłości działania systemów, niemniej powszechna centralizacja przetwarzania danych determinuje istnienie kluczowego atrybutu systemów informatycznych, jakim jest podatność na zniszczenie. Nieprzypadkowo zatem olbrzymim zainteresowaniem sektora finansowego cieszy się każda innowacja, która ma potencjał wyeliminowania tego problemu (np. koncepcja *blockchain*).

- wyścig konkurencyjny pomiędzy uczestnikami systemu bankowego, ukierunkowany na szybkość i łatwość wykonywania operacji finansowych,
- brak praktycznej możliwości wykorzystania danych historycznych do budowy ilościowych modeli zarządzania ryzykiem informatycznym,
- paradoksalnie malejąca świadomość informatyczna użytkowników końcowych[17].

Wymienione determinanty mogą być oczywiście uznane za dyskusyjne. Niektóre z nich trudno zweryfikować, niemniej wydaje się, że przyjęcie założenia o ich poprawności może przynieść zdecydowanie więcej korzyści niż strat. Informatyzacja współczesnych finansów jest zatem katalizatorem rozwoju i jednocześnie czynnikiem, który w każdej chwili może zdestabilizować system finansowy. Poza tym możliwości przeciwdziałania tej destabilizacji są ograniczone, co jest naturalną konsekwencją wymienionych uwarunkowań. Mimo tej ograniczoności kluczowym aspektem zarządzania współczesnymi instytucjami finansowymi staje się zarządzanie cyberbezpieczeństwem. Cyberbezpieczeństwo zyskuje obecnie status filaru stabilności finansowej, na równi z tradycyjnymi elementami polityki monetarnej, fiskalnej czy działań nadzoru bankowego. Współczesne zagrożenia nie ograniczają się jedynie do oszustw lub kradzieży danych – mogą przyjmować formę ataków systemowych na infrastrukturę krytyczną sektora finansowego. W skrajnych przypadkach mają potencjał wywołania zakłóceń o charakterze systemowym, obejmujących nie tylko pojedyncze banki czy giełdy, ale także całe sektory lub regiony. Jak wskazuje Dugbartey (2025), zakłócenie w działaniu systemu hurtowych rozliczeń międzybankowych lub infrastruktury płatniczej może prowadzić do kryzysów płynności, efektu domina i destabilizacji sektora bankowego. W kontekście stabilności finansowej jednym z najbardziej wrażliwych elementów pozostaje zaufanie uczestników rynku do narzędzi informatycznych, które udostępniają im instytucje finansowe oraz integrującej je infrastruktury. W przypadku naruszenia danych, awarii systemu bankowego lub ujawnienia słabości infrastruktury może dojść do paniki rynkowej i masowego wycofywania środków, co w krótkim czasie przekłada się na realne zagrożenie dla stabilności instytucji finansowych. Zjawisko to nasila się w dobie automatyzacji i rozwoju technologii sztucznej inteligencji, która – choć oferuje nowe możliwości – zwiększa jednocześnie powierzchnię potencjalnego ataku. Zaffer i in. (2025) pokazują, że użytkownicy często nie mają pełnej świadomości cyberzagrożeń wynikających z wdrażania AI w sektorze finansowym, co dodatkowo potęguje ryzyko. Rozwój zdecentralizowanych systemów finansowych (DeFi), cyfrowych walut banków centralnych czy platform tradingowych opartych na technologii *blockchain* niesie ze sobą konieczność budowy zupełnie nowej architektury cyberbezpieczeństwa. Coraz częściej zwraca się uwagę na zjawisko tzw. *blended-security attacks*, czyli złożonych ataków łączących elementy fizyczne, cyfrowe oraz socjotechniczne, które mogą uderzyć w podstawy funkcjonowania DeFi oraz zdecentralizowanych giełd. Tego rodzaju zagrożenia wykraczają poza skalę jednostkową i mogą wywoływać skutki systemowe, porównywalne z klasycznymi kryzysami finansowymi.

[17] To subiektywna opinia autora, wymagająca pogłębionych badań.

W odpowiedzi na rosnące zagrożenia coraz więcej instytucji finansowych oraz banków centralnych wdraża specjalne scenariusze stres-testów zawierające komponenty informatyczne. Rozszerza się także definicję ryzyka systemowego o czynniki związane z cyberzagrożeniami. Jak pokazuje analiza S. Kima i in. (2025), integracja danych dotyczących ryzyka cybernetycznego z modelami makroekonomicznymi pozwala lepiej oszacować wpływ cyberataków na kondycję sektora finansowego i zachowanie uczestników rynku. Dzięki temu możliwe staje się wcześniejsze wykrywanie potencjalnych szoków oraz planowanie odpowiedzi regulacyjnej. Na poziomie geopolitycznym zwiększa się znaczenie cyberprzestrzeni jako pola rywalizacji międzynarodowej. Konflikty o charakterze informacyjnym, wojny hybrydowe oraz napięcia wokół technologii 5G, systemów rozliczeń międzynarodowych (jak np. SWIFT) czy infrastruktury chmurowej stają się istotnym czynnikiem wpływającym na stabilność finansową całych państw. Rizvi i in. (2025) podkreślają, że strategie transformacji cyfrowej i inwestycji technologicznych muszą być integrowane z polityką budowania odporności finansowej – w tym poprzez systematyczne wzmacnianie cyberbezpieczeństwa instytucji sektora publicznego i prywatnego. W nowoczesnej gospodarce nie da się już oddzielić cyberbezpieczeństwa od stabilności finansowej. Współczesne systemy finansowe, ewoluując pod wpływem transformacji cyfrowej, przeszły fundamentalną metamorfozę – z tradycyjnych struktur opartych głównie na instytucjach bankowych i regulatorach ekonomicznych w złożone, technologicznie zależne ekosystemy. Obecnie funkcjonowanie sektora finansowego nie jest możliwe bez ścisłej współpracy z ekspertami z obszarów bezpieczeństwa informacji, analizy danych oraz sztucznej inteligencji. Ta interdyscyplinarność wynika nie tylko z potrzeby zapewnienia efektywności i innowacyjności usług, ale przede wszystkim z konieczności ochrony stabilności całego systemu finansowego w obliczu nowych typów zagrożeń. Innowacje technologiczne, takie jak rozproszone rejestry, algorytmy uczenia maszynowego, rozwiązania chmurowe czy otwarta bankowość, zwiększają wydajność i dostępność usług finansowych, ale jednocześnie wprowadzają nowe klasy ryzyk, w tym: cyberzagrożenia, zawodność modeli algorytmicznych, niedeterministyczne efekty działania systemów opartych na AI oraz zwiększoną podatność na błędy propagujące się w złożonych łańcuchach zależności technologicznych (Arner i in., 2017, s. 371 i n.; Zetzsche i in., 2020, s. 273 i n.). Jak zauważa Financial Stability Board, dynamiczny rozwój technologii finansowych może generować zagrożenia o charakterze systemowym, szczególnie w sytuacjach braku odpowiednich mechanizmów nadzoru i regulacji (Financial Stability Board [FSB], 2017). W tym kontekście coraz większego znaczenia nabiera zintegrowane podejście do zarządzania, które obejmuje nie tylko ryzyka finansowe, lecz także ryzyka technologiczne, modelowe i reputacyjne. Kluczowe znaczenie mają tu również ramy regulacyjne, które kładą nacisk na rozwój cyberodporności i ciągłości działania w warunkach awarii systemów krytycznych. Nie można także pominąć roli międzynarodowej współpracy w zakresie standaryzacji podejść do oceny ryzyka technologicznego – przykładem może być zestaw wytycznych NIST (National Institute of Standards and Technology [NIST], 2022), które oferują holistyczne podejście do zarządzania zagrożeniami cyfrowymi w sektorze finansowym.

Analiza powyższych treści nakazuje zadać kluczowe – w kontekście tematu rozdziału – pytanie: czy realizacja zagrożeń bezpieczeństwa informatycznego jest w stanie przyczynić się bezpośrednio do powstania zjawisk o charakterze kryzysowym w systemie finansowym? Innymi słowy, czy ryzyko informatyczne w systemie finansowym ma potencjał kryzysotwórczy? Prosta odpowiedź, twierdząca lub przecząca, nie jest oczywiście wystarczająca. Złożoność relacji między informatyką a stabilnością finansową wymaga odpowiedzi szerszej, wzbogaconej o wskazanie tych obszarów, których potencjał kryzysotwórczy już dziś jest możliwy do zauważenia, oraz tych, które najprawdopodobniej taki potencjał będzie charakteryzował w przyszłości. Odpowiedź trudno jest przedstawić kompleksowo w ujęciu ilościowym. Głównym narzędziem analizy pozostaje jakościowy opis problemu. Opis ten powinien identyfikować te elementy ryzyka informatycznego, których potencjał systemowy – identyfikowany na podstawie dostępnych obserwacji oraz eksperckich przewidywań – jest największy. Częściowo dyskusję nad tym problemem kontynuuje rozdział drugi.

1.4. Podsumowanie

Utrzymanie stabilności systemu finansowego w warunkach postępującej technologizacji wymaga wielowarstwowego i interdyscyplinarnego podejścia, integrującego kompetencje technologiczne, analityczne, organizacyjne oraz regulacyjne. Współczesny sektor finansowy funkcjonuje w środowisku, w którym czynniki technologiczne stają się równorzędne – a niekiedy nadrzędne – wobec tradycyjnych determinant makroekonomicznych. Oznacza to, że przyszłość tego sektora będzie w coraz większym stopniu zależna od jakości i dojrzałości stosowanych narzędzi informatycznych, poziomu odporności systemów teleinformatycznych na zagrożenia, a także zdolności instytucji do adaptacji w kontekście dynamicznie ewoluującego ekosystemu cyfrowego. Wzrost znaczenia zaawansowanych technologii, w szczególności sztucznej inteligencji, nie tylko prowadzi do transformacji procesów operacyjnych i modelu świadczenia usług finansowych, lecz także inicjuje głębokie zmiany o charakterze społecznym, prawnym i regulacyjnym. Implementacja AI w sektorze finansowym wpływa na relacje instytucja–klient, przekształca rynek pracy poprzez automatyzację funkcji analitycznych, a także zmienia percepcję zaufania i odpowiedzialności w relacjach gospodarczych. Jednocześnie coraz większa rola algorytmów decyzyjnych rodzi potrzebę redefinicji ram prawnych dotyczących ochrony konsumentów, prywatności danych, odpowiedzialności za decyzje podejmowane przez systemy autonomiczne oraz transparentności procesów obliczeniowych. Zmiany technologiczne determinują również kierunki rozwoju regulacji międzynarodowych, które muszą odpowiadać na wyzwania takie jak transgraniczny charakter zagrożeń cybernetycznych, zróżnicowane standardy ochrony danych czy konieczność harmonizacji procedur raportowania incydentów. W rezultacie stabilność systemu finansowego staje się pochodną nie tylko efektywności mechanizmów zarządzania ryzykiem technologicznym, lecz także

zdolności sektora do elastycznego dostosowania się do ewolucji otoczenia prawnego i społecznego, w którym technologie, a zwłaszcza sztuczna inteligencja, odgrywają coraz bardziej centralną rolę.

Jak wskazują Czechowska i in. (2020), warto podejmować zintegrowane działania, których celem będzie zapobieganie zagrożeniom informatycznym, biorąc pod uwagę perspektywę mikroostrożnościową, która w ostatecznym rozrachunku łączy się z perspektywą makroostrożnościową, stabilnością systemu finansowego i jego bezpieczeństwem.

Coraz częściej spotykamy się z nieco prowokacyjną tezą, że któryś z kolejnych globalnych kryzysów finansowych będzie spowodowany przez technologię. Dotyczy to w szczególności przyszłych zastosowań sztucznej inteligencji (Danielsson i Uthemann, 2025). Trudno podejmować się jednoznacznej weryfikacji tego typu tezy, można jednak stwierdzić, że postrzeganie ryzyka technologicznego jako przyczyny przyszłych kryzysów finansowych jest racjonalne i dobrze ugruntowane w trendach. Nie jest to jednak przewidywanie falsyfikowalne – to strategiczne ostrzeżenie.

Rozdział 2
Cyberbezpieczeństwo i cyberryzyko

2.1. Podstawowe pojęcia

Obserwowany współcześnie rozwój technologii cyfrowych oraz postępująca transformacja cyfrowa sektora finansowego prowadzą do dynamicznego wzrostu znaczenia zagadnień związanych z cyberbezpieczeństwem i cyberryzykiem. W literaturze przedmiotu oraz praktyce zarządzania tymi obszarami obserwuje się jednak znaczne zróżnicowanie definicji i zakresów stosowanych pojęć. Brak jednoznacznego, powszechnie przyjętego słownictwa nie tylko sprzyja niespójności interpretacyjnej, lecz także może prowadzić do trudności w projektowaniu i wdrażaniu skutecznych strategii ochrony systemów informatycznych. Celem niniejszego rozdziału jest uporządkowanie i precyzyjne zdefiniowanie kluczowych terminów wykorzystywanych w analizach dotyczących cyberbezpieczeństwa oraz cyberryzyka, ze szczególnym uwzględnieniem ich zastosowań w sektorze finansowym. Wprowadzenie klarownej terminologii stanowi fundament dalszych rozważań teoretycznych i praktycznych.

Pojęcie cyberbezpieczeństwa nie jest pojęciem nowym i doczekało się już wielu definicji, mających oczywiście wspólny mianownik, odmiennych jednak w szczegółach oraz perspektywach postrzegania problemu. Ta terminologiczna ewolucja, będąca wynikiem dynamicznego rozwoju technologii teleinformatycznych, jest zrozumiała i chociaż nie wnosi wiele nowego do opisu zjawiska od strony teoretycznej, to stara się nadążać za specyfiką zmian w praktyce zastosowań tych technologii w gospodarce. Wydaje się jednak, że cyberbezpieczeństwo powinno być traktowane w kategoriach pojęcia podstawowego, którego definicja ma wyznaczać kierunki rozwoju dyscypliny, a nie wraz z tym rozwojem się zmieniać. Cyberbezpieczeństwo jest synonimem bezpieczeństwa informatycznego[18]. Na potrzeby niniejszego opraco-

[18] Stwierdzenie to wymaga komentarza. Podstawowa terminologia omawianego zagadnienia w większości polskojęzycznej literatury przedmiotu przedstawiana jest w bardzo dyskusyjny sposób. Wynika to m.in. z nieprawidłowych tłumaczeń terminów angielskich, takich jak np. *information security* czy *data security* (wyczerpująco problem ten opisał Wawrzyniak (2012, s. 38 i n.). Źródło to zawiera także obszerną dyskusję terminologiczną dotyczącą innych pojęć z zakresu bezpieczeństwa, wykorzystywanych w niniejszym rozdziale.) Konsekwencją tych nieprawidłowości są różne podejścia do kwestii terminologicznych dotyczących nowo powstających terminów. Wydawać by się zatem mogło, że rozwiązania problemu szukać należy w źródłach angielskojęzycznych. Wiele z nich stara się rozróżniać pojęcia *cybersecurity* oraz *information security* (lub *information technology security*). W większości przypadków rozróżnienie związane jest z przypisaniem terminowi *cybersecurity* znaczenia ochrony informacji i systemów przed atakami sieciowymi, a terminowi *information security* bardziej tradycyjnego (normatywnego) znaczenia zapewniania poufności, integralności, autentyczności i dostępności informacji. Niektóre podejścia doszukują się także różnic w postrze-

wania przyjęto definicję, zgodnie z którą bezpieczeństwem informatycznym jest stan systemu informatycznego, w którym poziom najważniejszych jego atrybutów jest akceptowalny przez podmiot dokonujący oceny bezpieczeństwa lub spełnia przyjęte w procesie oceny kryteria. Do atrybutów bezpieczeństwa zaliczamy:

- poufność – zapewniającą, że informacja nie jest udostępniana lub ujawniana nieuprawnionym osobom, podmiotom lub procesom,
- autentyczność – zapewniającą, że tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji; jest związana z badaniem, czy ktoś lub coś jest tym, za kogo lub za co się podaje;
- dostępność – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo,
- integralność danych – zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- integralność systemu – zapewniającą, że system realizuje swoje funkcje w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej,
- rozliczalność – zapewniającą, że działania podmiotu mogą być jednoznacznie przypisane tylko jemu,
- niezawodność – oznaczającą spójne, zamierzone i przewidywalne zachowanie i skutki.

Jest to zatem pojęcie względne, interpretowalne w sposób determinowany przyjętymi kryteriami oceny. Innymi słowy, w zależności od różnych aspektów oceny, takich jak wymagania podmiotu oceniającego, metody, cele, czas itp., bezpieczeństwo tego samego systemu może zostać ocenione w różny sposób. To ważne zastrzeżenie, gdyż pozwala uniknąć niepoprawnych oraz nieuprawnionych tez i sformułowań[19]. O bezpieczeństwie można mówić tylko w odniesieniu do przyjętych reguł i parametrów jego oceny. Wszelkie bezwzględne oceny bezpieczeństwa nie mogą być w żadnym wypadku uprawnione[20]. Cyberbezpieczeństwem jest zatem pewien stan systemu, zarządzaniem cyberbezpieczeństwem natomiast nazywamy zespół cyklicznych procesów ukierunkowanych na zidentyfikowanie, osiągnięcie i utrzymanie tego stanu, czyli założonego poziomu wymienionych atrybutów.

---

ganiu roli czynnika ludzkiego w problematyce bezpieczeństwa. Szczegółowa analiza uzasadnień wszystkich tych koncepcji terminologicznych wykazuje jednak ich niedociągnięcia oraz brak konsekwencji (von Solms i van Niekerk, 2013, s. 97 i n.). W rozdziale niniejszym – w celu uniknięcia terminologicznych dyskusji niewpływających w żaden sposób na zasadniczą treść wywodu – przyjęto założenie, zgodnie z którym pojęcia cyberbezpieczeństwa i bezpieczeństwa informatycznego są synonimami.

[19] Oczywiście względność pojęcia nie oznacza braku standardów i powszechnie akceptowanych norm. Pozwala jednak na uznaniowe podejście do omawianej problematyki, zależne od celów konkretnego procesu ewaluacyjnego.

[20] Warto zauważyć, że brak relatywizmu w omawianym obszarze jest *de facto* sam w sobie zagrożeniem bezpieczeństwa.

Wspomniana już niezmienność podstaw teoretycznych terminologicznego podejścia do omawianego zagadnienia nie oznacza jednak stagnacji w obszarze praktyki biznesowej. Nie da się bowiem nie dostrzec rozwijającego się od kilkunastu lat paradygmatu, zgodnie z którym współczesne instytucje – przede wszystkim finansowe – dostosowują się do funkcjonowania w ramach filozofii *to survive on a diet of poisoned fruit*[21], będącej następstwem dynamicznego rozwoju technologicznego skutkującego zapętlonym procesem współistnienia nowych szans i odpowiadającym im nowych zagrożeń. Innymi słowy, pomimo wymogu stabilizacji, leżącego u podstaw działalności finansowej, współczesne instytucje akceptują stan permanentnej niepewności, wynikającej z zagrożeń i podatności systemów informatycznych – zagrażający wręcz istnieniu tych instytucji – w zamian za nieocenione korzyści w obszarze jakości, szybkości, efektywności i konkurencyjności, dzięki którym mogą nadal funkcjonować na rynku usług finansowych oraz generować finansowe wartości dodane. Zjawisko to dostrzegano już ponad 20 lat temu, jednak jego natężenie stale się zwiększa (Winkler, 2002). Co więcej, zaczyna ono nabierać obserwowalnych cech paradoksu – zwanego paradoksem cyberbezpieczeństwa: nowe technologie informatyczne czynią instytucje silniejszymi i bardziej konkurencyjnymi, ale jednocześnie mniej bezpiecznymi i bardziej podatnymi na ryzyko operacyjne. Dotyczy to oczywiście wszelkich organizacji, jednak w kontekście instytucji systemu finansowego ma szczególne znaczenie.

Z pojęciem cyberbezpieczeństwa nierozerwalnie związane jest pojęcie ryzyka informatycznego. Terminologia tego zagadnienia również nie jest stabilna i charakteryzuje się wielością dość odmiennych definicji. Aby rozpocząć dyskusję nad pojęciem ryzyka informatycznego, należy przedstawić cztery kluczowe dla omawianego zagadnienia terminy: zasoby (aktywa), wrażliwość, zagrożenie i podatność (Wawrzyniak, 2012). Zasoby to wszystko, co dla instytucji ma wartość i co dla jej dobra należy chronić, aby mogła funkcjonować w sposób niezakłócony. Wrażliwość jest miarą ważności przypisaną do informacji przez jej autora lub dysponenta w celu wskazania konieczności oraz zasad jej ochrony. Zagrożeniami nazywamy potencjalne przyczyny niepożądanych zdarzeń, których skutkiem mogą być straty powstałe w systemie informatycznym, a w dalszej konsekwencji w instytucji. Podatność natomiast to słabość lub luka w systemie informatycznym mogąca być wykorzystana przez zagrożenia, powodując straty. Sam fakt istnienia zagrożeń jest immanentną cechą każdego systemu oraz jego otoczenia i nie jest jeszcze bezpośrednią przyczyną incydentów – zdarzeń negatywnie wpływających na bezpieczeństwo systemu. Na potrzeby niniejszego opracowania przyjęto, że ryzyko informatyczne, będące podobszarem ryzyka operacyjnego[22], to:

---

[21] To metaforyczne określenie coraz częściej jest przywoływane w kontekście niepewności, jaka jest związana z dynamiką rozwoju zastosowań rozwiązań informatycznych w instytucjach finansowych (Danzig, 2014).

[22] Ryzyko operacyjne jest pojęciem zdecydowanie szerszym niż ryzyko informatyczne. Obejmuje swoim zakresem działalność ludzi (pracowników, klientów), wadliwość procesów i przede wszystkim konieczność wykorzystywania nowoczesnych technologii. Triada ludzie-procesy-tech-

- w ujęciu jednostkowym – możliwość (prawdopodobieństwo), że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych[23],
- w ujęciu ogólnym – uogólniona matematycznie miara obrazująca możliwość (prawdopodobieństwo) zaistnienia incydentów bezpieczeństwa oraz uwzględniająca ich potencjalny, negatywny wpływ na funkcjonowanie instytucji.

Drugiej z zaproponowanych definicji należy się komentarz. Matematyczne uogólnienie wymaga zastosowania jakiegoś narzędzia ilościowego ukierunkowanego na syntetyczne spojrzenie na system lub jego podobszar. Tym narzędziem może być rozwiązanie dedykowane omawianemu zagadnieniu lub jedynie zaadaptowane na jego potrzeby. W zależności od wybranego narzędzia miara ryzyka informatycznego w ujęciu ogólnym może dostarczać informacji o różnym charakterze[24]. Ryzyko informatyczne jest problemem interdyscyplinarnym i niełatwo poddaje się uogólnieniom, szczególnie w warstwie ewaluacyjnej. Dualizm terminologiczny ryzyka informatycznego komplikuje także konstrukcję definicji zarządzania ryzykiem informatycznym, niemniej na potrzeby niniejszego rozdziału można przyjąć, że przez pojęcie to rozumiemy kompleksowy proces identyfikowania, monitorowania oraz eliminowania lub minimalizowania wartości iloczynu prawdopodobieństw realizacji zagrożeń bezpieczeństwa oraz ich skutków.

Relacja między pojęciami cyberbezpieczeństwa i cyberryzyka powoduje niejednoznaczności na gruncie zarówno teorii, jak i praktyki zarządzania bezpieczeństwem informatycznym. Choć formalne definicje jednoznacznie rozdzielają oba te terminy – wskazując, iż cyberbezpieczeństwo odnosi się przede wszystkim do stanu ochrony systemów informatycznych przed zagrożeniami, cyberryzyko zaś do prawdopodobieństwa oraz potencjalnych konsekwencji wystąpienia zdarzeń o charakterze niepożądanym – w literaturze przedmiotu powszechnie obserwuje się elastyczne podejście do stosowania tych pojęć. Nie tylko bywają one używane zamiennie, lecz nierzadko także definicje jednego są nieświadomie przenoszone na drugie. W niniejszej książce przyjęto założenie, iż pojęcie ryzyka informatycznego stanowi ramowy, nadrzędny koncept analityczny. W jego obrębie bezpieczeństwo informatyczne (cyberbezpieczeństwo) stanowi jedno z kluczowych, choć niewyczerpujących, pól badawczych. Fundamentami dla takiego podejścia są:

- istotne różnice w ontologicznym i epistemologicznym znaczeniu obu pojęć – ryzyko zakłada element niepewności i modelowania probabilistycznego, podczas

---

nologie koresponduje oczywiście z definicją bazylejską (Bank for International Settlements, 2020), chociaż warto podkreślić, że Komitet Bazylejski widzi w ramach ryzyka operacyjnego ryzyko prawne, a wyklucza poza nawias ryzyka operacyjnego ryzyko reputacyjne.

[23] Zastąpienie prawdopodobieństwa możliwością zostało przedyskutowane przez Wawrzyniaka (2016, s. 145 i n.).

[24] Miarą może być pojedyncza wielkość, lecz także zbiór wartości, np. opis ryzyka wykorzystujący aparat macierzowy. Warto również podkreślić, że relacja pomiędzy narzędziami oceny bezpieczeństwa a narzędziami szacowania ryzyka jest płynna i zależy od specyfiki danego przypadku. Wyczerpująco opisał to zagadnienie Wawrzyniak (2012).

gdy bezpieczeństwo jest koncepcyjnie związane ze stanem względnej ochrony lub jej brakiem,
- rosnąca waga zarządzania ryzykiem w szerokim ujęciu działalności finansowej, co przekłada się na zwiększoną rolę zarządzania ryzykiem informatycznym jako istotnym komponentem ryzyka operacyjnego,
- znaczenie ram regulacyjnych w sektorze finansowym, które formalnie sytuują ryzyko cybernetyczne w strukturze ogólnego zarządzania ryzykiem (EBA, 2025).

Jednocześnie warto poddać krytycznej refleksji dominujący w literaturze trend normatywny, który skłania się ku integracji podejścia do zarządzania ryzykiem z zarządzaniem bezpieczeństwem. Taka integracja, choć teoretycznie atrakcyjna, bywa w praktyce problematyczna, prowadzi bowiem do rozmycia granicy między narzędziami prewencji a mechanizmami oceny i modelowania ryzyka (Kshetri, 2025). W niniejszej książce pojęciem wiodącym pozostaje cyberbezpieczeństwo – nie tylko ze względu na centralne znaczenie dla stabilności finansowej systemów finansowych, ale również dlatego, że determinantą zmian w poziomie stabilności są w istocie obserwowane stany, a nie wyłącznie probabilistyczna estymacja przyszłych zdarzeń. Z tego względu, chociaż zarządzanie ryzykiem pozostaje fundamentem działalności finansowej jako całości, na potrzeby niniejszego opracowania operacyjnie priorytetowe znaczenie przypisano praktyce i strategiom zapewnienia cyberbezpieczeństwa.

Terminologia omawianego zagadnienia jest nierzadko uzupełniana jeszcze jednym pojęciem. Jest nim cyberodporność (*cyber-resilience*)[25]. Wielu ekspertów zauważa istotną różnicę między zdefiniowanym powyżej zarządzaniem ryzykiem a odpornością. Ta druga nie dotyczy bowiem oceny i analizy, w tym szacowania ryzyka oraz rekomendowania działań minimalizujących jego poziom, lecz ukierunkowana jest na tworzenie planów reagowania na zdarzenia kryzysowe, których wcześniejsza predykcja nie była możliwa, brak predykcji wynikał z błędów procedur zarządzania ryzykiem lub prawdopodobieństwo wystąpienia tych zdarzeń musiało być – zgodnie z zaakceptowanymi modelami – określone na skrajnie niskim poziomie (Danzig, 2014). Definicje proponowane przez praktyków wskazują cel nadrzędny procesu osiągania odporności, jakim jest ciągłość funkcjonowania organizacji w przypadkach realizacji zagrożeń bezpieczeństwa (European Systemic Risk Board, 2020). Jest to istotnie ważny element, który nakazuje przypisywać cyberodporności walory samodzielnego pojęcia o specyficznych dla siebie atrybutach. Co więcej, ukierunkowanie na ciągłość funkcjonowania w przypadkach krytycznych, a nie na bieżącą analizę i ocenę w okresach stabilnych, zbliża pojęcie cyberodporności do problematyki wpływu rozwoju technologicznego na stabilność systemu finansowego. Odporność jako koncepcja

[25] Warto zauważyć, że pojęcie cyberodporności nie stoi na najwyższym szczeblu w hierarchii terminologicznej. Coraz częściej w regulacjach europejskich, a w konsekwencji w literaturze przedmiotu pojawia się koncepcja suwerenności cyfrowej, ogólnie utożsamianej ze zdolnością państw do kształtowania swojego środowiska teleinformatycznego zgodnie z własnymi potrzebami (Wrzosek, 2023).

ogólna ma długą historię, obejmującą różne dyscypliny, od inżynierii materiałowej po psychologię, ekologię, urbanistykę i informatykę, aby wymienić najważniejsze. Chociaż identyfikacja atrybutów odporności w różnych dyscyplinach ma pewne cechy wspólne, to jednak brak wyraźnego rozgraniczania odmienności znaczeniowej zależnej od dyscypliny prowadzi do uproszczeń i błędów interpretacji. Rozpoznanie tych różnic zapobiega próbom przeniesienia metod analitycznych, które okazały się bardzo przydatne w określonej dziedzinie, ale mogą nie mieć znaczenia dla cyberbezpieczeństwa. W kontekście cyberbezpieczeństwa należy wskazać przede wszystkim jeden z wymiarów odporności organizacji, jakim jest dynamika[26]. Odporność wymaga bowiem procesowego podejścia, obejmującego działania przed szokiem lub incydentem katastroficznym, w ich trakcie i po nich. Oznacza to, że odporność można osiągnąć jedynie poprzez stały, cykliczny proces, w ramach którego organizacja przygotowuje się do stawienia czoła różnorodnym zagrożeniom o różnym nasileniu i częstotliwości, wdraża technologie i polityki ochronne, które mogą zmniejszyć podatności, wdraża protokoły wykrywania i reagowania, które mogą zagwarantować ciągłość funkcjonowania i złagodzić negatywne skutki zdarzeń niepożądanych oraz dostosowywać systemy i procedury do przyszłych, nieoczekiwanych zdarzeń.

Koncepcja odporności organizacyjnej oraz związanych z nią mechanizmów implementacji rozwiązań wspierających tę odporność ma teoretyczne uzasadnienie w analogii do klasycznego podejścia do klasyfikacji zdarzeń ryzyka operacyjnego – w tym również ryzyka o charakterze informatycznym. U podstaw tej analogii leży powszechnie przyjęte w literaturze przedmiotu rozróżnienie kategorii zdarzeń ryzyka operacyjnego w oparciu o dwa kluczowe wymiary: częstotliwość występowania danego zdarzenia oraz skalę jego potencjalnych negatywnych skutków, często określaną mianem szkodliwości (*severity*). Przyjęcie takiego dwuwymiarowego podejścia nie tylko umożliwia skuteczniejsze profilowanie ryzyk i priorytetyzację działań prewencyjnych, lecz także ułatwia projektowanie adekwatnych mechanizmów odpornościowych – zarówno technologicznych, jak i proceduralnych – w ramach systemu bezpieczeństwa organizacji. W kontekście cyberbezpieczeństwa oraz szerzej – odporności cyfrowej – taka klasyfikacja pozwala lepiej zrozumieć, które typy zagrożeń wymagają inwestycji w prewencję i detekcję, a które w odbudowę i zarządzanie skutkami. Na tej podstawie, w obrębie tak zdefiniowanego pola analitycznego, wyróżnia się cztery podstawowe kategorie zdarzeń ryzyka, różnicowane w zależności od kombinacji ich częstości i szkodliwości:

- kategorię 1 – zdarzenia wysokiej częstości i niskiej szkodliwości wymagające automatyzacji procesów detekcji i reakcji,
- kategorię 2 – zdarzenia niskiej częstości i niskiej szkodliwości generujące akceptowalny poziom ryzyka, zarządzane głównie przez monitoring i standardowe procedury operacyjne,

[26] Zob. (Dupont, 2019). Autor wymienia i charakteryzuje pięć wymiarów odporności (dynamikę, sieciowość, stałość praktyk biznesowych, zdolność adaptacji i podatność na kwestionowanie).

- kategorię 3 – zdarzenia wysokiej częstości i wysokiej szkodliwości, stosunkowo rzadkie, potencjalnie tworzące kluczowy obszar dla wdrażania mechanizmów odpornościowych, takich jak redundancja, segmentacja sieci, zaawansowane systemy detekcji anomalii,
- kategorię 4 – zdarzenia niskiej częstości, lecz bardzo wysokiej szkodliwości, generujące ryzyka katastroficzne, którymi zarządzanie wymaga zaawansowanego planowania ciągłości działania oraz mechanizmów transferu ryzyka (np. poprzez ubezpieczenia cybernetyczne).

Tego typu klasyfikacja ma szerokie zastosowanie zarówno w standardach zarządzania ryzykiem, jak i w praktycznych modelach budowania odporności cyfrowej w sektorze finansowym[27]. Kategorie 1 oraz 2 są informatyczną codziennością i można nimi skutecznie zarządzać, w tym także oceniać z wykorzystaniem standardowych narzędzi ilościowych. Kategorii 3 na razie nie obserwujemy w praktyce, chociaż to właśnie ona będzie najprawdopodobniej kluczowym czynnikiem determinującym powodzenie biznesu w przyszłości. Kategoria 4 natomiast to problem dzisiejszy. Do kategorii tej należą zdarzenia ekstremalnie mało prawdopodobne, lecz o katastrofalnych następstwach, zagrażających ciągłości funkcjonowania instytucji. Szczególną cechą kategorii 4 jest to, że zarówno prawdopodobieństwa wystąpienia zdarzeń, jak i ich negatywny skutek są praktycznie niewyznaczalne. Można jedynie zgrubnie je szacować, niemniej szacunki takie nie mają żadnej wartości decyzyjnej[28]. Ważniejsze od szacowania tych wielkości jest przygotowanie planu działania na wypadek zaistnienia zdarzenia mało prawdopodobnego o katastrofalnych następstwach. Opisana odporność będzie zatem ukierunkowana na zarządzanie głównie tą właśnie kategorią. Ograniczenie rozważań do jednej tylko kategorii nie jest bynajmniej wadą, gdyż to właśnie tego typu zjawisk instytucje finansowe obawiają się dziś najbardziej i te zjawiska mają potencjał kryzysotwórczy, zagrażający stabilności finansowej.

Ryzyko informatyczne w systemie finansowym podlega stałym zmianom. Jego ewolucja rozpoczęła się jeszcze przed upowszechnieniem się technologii informatycznych, jednak era globalnej sieci ewolucję tę zdecydowanie przyspieszyła. Specyficznym atrybutem tego ryzyka oraz związanych z nim ataków na systemy informatyczne jest swego rodzaju paradoks przejawiający się tym, że pomimo wzrostu poziomu złożoności technologicznej narzędzi ataków wiedza wymagana do korzystania z nich maleje. Oczywiście relację tę cechują zmienność w czasie i przestrzeni oraz pewne uproszczenie, niemniej wskazuje ona powagę zjawiska oraz jego przyszłe atrybuty[29].

---

[27] Wśród norm ISO dotyczących omawianego zagadnienia na szczególną uwagę zasługują normy z rodziny ISO/IEC 27000 oraz 31000.

[28] Nawet przy założeniu poprawnie przeprowadzonego procesu analitycznego (co w przypadku zdarzeń skrajnie mało prawdopodobnych jest dyskusyjne) wynikiem szacowania ryzyka będzie iloczyn liczby bardzo małej oraz bardzo dużej. Jakakolwiek próba interpretacji takiej wartości wynikowej nie ma sensu biznesowego.

[29] O uproszczeniu w tym wypadku można mówić z powodu dyskusyjności określenia „wymagana wiedza". Poziom tego czynnika maleje, ale jest to związane nie tyle z malejącymi wymaganiami kompetencyjnymi, ile z rosnącą dostępnością informacji.

Podsumowując, należy podkreślić, że ryzyko informatyczne jest funkcją wielu zmiennych, wśród których dwie najważniejsze to prawdopodobieństwo wystąpienia incydentu bezpieczeństwa oraz jego potencjalny skutek, warto jednak w krytyczny sposób postrzegać szczególnie pierwszą z tych zmiennych. W ogólnym przypadku nie poddaje się ona bowiem standardowej analizie statystycznej, a jej wadliwa predykcja może stać się przyczyną zjawisk o wymiarze katastrofalnym.

2.2. Zagrożenia cyberbezpieczeństwa systemu finansowego

2.2.1. Wprowadzenie

Jak już wspomniano, współczesny system finansowy podlega dynamicznym zmianom determinowanym przez wiele czynników, zarówno związanych z uwarunkowaniami natury biznesowej i regulacyjnej, jak i tych, których źródeł doszukiwać się należy poza światem finansów. Jednym z nich – być może o największym znaczeniu – jest dynamiczny i trudno przewidywalny rozwój informatyki oraz obszaru jej zastosowań w gospodarce. Obiektywna obserwacja zmian, jakie zaszły w ciągu ostatnich 20 lat na rynku produktów i usług finansowych, nie pozostawia wątpliwości. Kluczowy udział w kreowaniu tych zmian miały implementacje nowych rozwiązań informatycznych. Ten swego rodzaju znak czasów ma zarówno dobre, jak i złe konotacje. Wśród tych pierwszych znajdują się oczywiście bezdyskusyjne korzyści wynikające z procesów cyfryzacji różnych obszarów systemu finansowego. Wśród tych drugich należy podkreślić permanentny wzrost liczby zagrożeń bezpieczeństwa systemów informatycznych w instytucjach finansowych oraz – zasygnalizowany wcześniej – malejący poziom świadomości informatycznej użytkowników tych systemów. Specyfika zastosowań informatyki w instytucjach finansowych jednoznacznie bowiem określa zwrot wektora zmian: szybciej, łatwiej i wygodniej musi oznaczać mniej bezpiecznie. To właśnie zjawisko – znajdujące się w centrum zarządzania ryzykiem operacyjnym – w większym niż kiedykolwiek stopniu zagraża dziś stabilności systemu finansowego. Nieprzypadkowe jest w tym kontekście olbrzymie zainteresowanie, jakim cieszyły się w ostatnich latach nowo powstające rozwiązania informatyczne, nierzadko mianowane innowacjami, wykorzystujące m.in. koncepcję łańcucha bloków. Koncepcja ta miała się stać swego rodzaju panaceum na wszelkie problemy związane z bezpieczeństwem informatycznym w finansach. Wydaje się jednak, że do kompletnego panaceum nam jeszcze daleko, a informatyka – poprzez dynamikę jej zastosowań – będzie w coraz większym stopniu wpływać na stabilność finansową, w ujęciu zarówno lokalnym, jak i globalnym.

Tradycyjne podejście do problematyki zagrożeń systemów informatycznych w instytucjach finansowych zakłada współistnienie zbioru zagrożeń wynikających z przyczyn środowiskowych oraz działalności człowieka, którą można z kolei podzielić na

działalność przypadkową i celową (Wawrzyniak, 2012). Pierwsze tego typu podziały definiowane były już na początku lat osiemdziesiątych i do tej pory nie straciły aktualności (Robling Denning, 1992). Nie oznacza to oczywiście, że dynamiczny rozwój zastosowań informatyki nie wpłynął w żaden sposób na postrzeganie problematyki zagrożeń bezpieczeństwa systemów informatycznych w instytucjach finansowych. Wręcz przeciwnie, wpływ ten jest znaczny i stale się zwiększa, a kontekst stabilności systemu finansowego staje się obecnie szczególnie widoczny. Obawy przed zakłóceniem tej stabilności w naturalny sposób uwypuklają pewne kategorie zagrożeń, o których wiadomo od dawna, jednak ich destrukcyjny potencjał przybiera na sile w związku ze wspomnianą już specyfiką zastosowań informatyki we współczesnych finansach. Bieżące analizy omawianej problematyki oraz projekcje przyszłych trendów na pierwszy plan wysuwają następujące kategorie zagrożeń bezpieczeństwa informatycznego:

- *phishing*, wykorzystujący nieprawidłowe reakcje i postawy użytkowników systemów informatycznych, najczęściej ukierunkowany na zainfekowanie systemu złośliwym oprogramowaniem lub pozyskanie poufnych danych,
- *malware* – wszelkiego rodzaju szkodliwe oprogramowanie,
- *ransomware*, czyli rodzaj złośliwego oprogramowania, które uniemożliwia dostęp do zaatakowanego systemu komputerowego albo odczyt zapisanych w tym systemie danych, żądając jednocześnie opłacenia okupu za odblokowanie tego dostępu (nierzadko ataki tego typu są poprzedzane atakiem phishingowym),
- ataki typu *distributed denial of service*, ukierunkowane na ograniczenie lub zablokowanie dostępności systemów informatycznych,
- potencjalnie negatywny wpływ współpracy z podmiotami trzecimi, których systemy łączą się z systemami instytucji finansowych (w szczególności usługi *cloud computing*),
- problemy implementacji wielopoziomowego uwierzytelnienia w systemach bankowości internetowej i mobilnej,
- zagrożenia związane z niewłaściwymi praktykami zarządzania hasłami dostępu do systemów informatycznych,
- zaawansowane kampanie cyberprzestępcze (*advanced persistent threat*),
- wady szybko zmieniającego się oprogramowania aplikacyjnego, przede wszystkim aplikacji mobilnych,
- trudno przewidywalne zmiany, jakie wprowadzają do systemu finansowego innowacje technologiczne i finansowe,
- złośliwe oprogramowanie ukierunkowane na terminale płatnicze i bankomaty (*ATM malware*) – infekowanie urządzeń służących do obsługi gotówki i płatności w celu kradzieży środków lub danych kart,
- wycieki danych wynikające z błędów w konfiguracji chmury obliczeniowej – nieprawidłowo zabezpieczone zasoby chmurowe mogą prowadzić do ujawnienia danych klientów i transakcji,

- inżynierię społeczną poza phishingiem – wykorzystanie technik manipulacji interpersonalnej (telefonicznej, bezpośredniej) w celu wyłudzenia danych uwierzytelniających lub nakłonienia pracowników do działań na rzecz cyberprzestępców,
- podatności w technologiach z zakresu sztucznej inteligencji i automatyzacji,
- ataki *deepfake* oraz *voice spoofing* – wykorzystanie fałszywego obrazu lub głosu w celu oszukania procedur weryfikacji tożsamości, np. w bankowości telefonicznej,
- ataki typu *credential stuffing* – będące pochodnymi udanych przejęć parametrów dostępu,
- ataki na łańcuchy dostaw oprogramowania.

Wyszczególnienie to nie wyczerpuje oczywiście problemu, niemniej wskazuje te kategorie zagrożeń, których potencjalny negatywny wpływ na funkcjonowanie systemów informatycznych stale ewoluuje i zarówno przez praktyków, jak i przez teoretyków jest postrzegany jako czynnik o charakterze newralgicznym, potencjalnie kryzysogennym. Dalej zaprezentowano krótką charakterystykę wybranych kategorii zagrożeń.

2.2.2. *Phishing*

Phishing to ogólna nazwa wszelkiego rodzaju ataków ukierunkowanych na podszywanie się pod inną osobę lub instytucję w celu nakłonienia atakowanego do wykonania określonego działania. Co sprawia, że ten pozornie trywialny mechanizm ataku jest tak istotny dla instytucji finansowych? Jest to atak wykorzystujący najtrudniejszą do wyeliminowania podatność, jaką jest postawa człowieka (użytkownika systemu), będąca wypadkową kilku elementów, takich jak: intencje, przewidywania, kompetencje i emocje (Wawrzyniak, 2012). Wśród skutków ataków phishingowych, których potencjał systemowy jest największy, należy wymienić:

- zainfekowanie systemu informatycznego instytucji finansowej szkodliwym oprogramowaniem, negatywnie wpływającym na jeden lub więcej atrybutów bezpieczeństwa informatycznego (w tym ograniczenie dostępności systemu czy danych),
- masową utratę poufności lub integralności danych,
- uzyskanie nieautoryzowanych dostępów do systemów informatycznych.

Wszystkie tego typu skutki są w stanie zakłócić funkcjonowanie instytucji do tego stopnia, że mogą stać się bezpośrednią przyczyną zjawisk o charakterze systemowym. *Phishing* może być stosowany jako bezpośrednia metoda nakłaniania do wykonania określonego działania, ale również jako pośrednie narzędzie, ukierunkowane na infekowanie atakowanego systemu złośliwym oprogramowaniem, czego następstwem mogą być np. próby wymuszania okupu. *Phishing* w połączeniu z *ransomware* staje się więc zagrożeniem systemowym. Wykorzystując powszechną, związaną z czynnikiem ludzkim, słabość każdego systemu i każdej instytucji, ma potencjał przerywania ciągłości funkcjonowania. Ogólny schemat ataku phishingowego składa się z następujących etapów (Warburton, 2020):

- wyboru celu ataku (cele poprzednich ataków, wyniki analizy struktury organizacyjnej i technicznej atakowanej instytucji, wyniki analizy mediów społecznościowych),
- dostarczenia mechanizmu (takiego jak e-mail, media społecznościowe, SMS, Voice Mail),
- ominięcia środków ochrony (załączniki, które nie są blokowane przez systemy antywirusowe, skracanie adresów internetowych, inne),
- realizacji (atakowany wykonuje oczekiwaną czynność),
- wykorzystania udanego ataku (aktywacja *malware*),
- uzyskania korzyści (nieograniczone możliwości wykorzystania poufnych danych, szyfrowanie zawartości dysków, niszczenie danych, inne).

Phishing wyewoluował w ciągu ostatnich lat z prostego ataku mailowego do rozbudowanego procesu, realizowanego przez zorganizowane grupy, wykorzystującego dane o pracownikach oraz procedurach wewnętrznych instytucji. Co więcej, w procesach wyłudzania danych oraz wykorzystywania skompromitowanych informacji poufnych coraz częściej stosowane są specjalistyczne narzędzia informatyczne, dla których przeszkodą nie jest nawet silne uwierzytelnienie klienta[30]. Analiza aktualnych danych statystycznych dotyczących incydentów związanych z cyberbezpieczeństwem na poziomie globalnym jednoznacznie wskazuje, iż ataki typu phishingowego pozostają – i według prognoz będą w nadchodzących latach nadal pozostawać – najczęściej wykorzystywaną formą ataku sieciowego. Wzrost liczby takich incydentów jest bezpośrednio powiązany z niskim progiem wejścia dla cyberprzestępców, skutecznością socjotechniczną tego typu ataków oraz ciągle rosnącą powierzchnią ataku wynikającą z powszechnej cyfryzacji usług finansowych (Federal Bureau of Investigation, 2024; Verizon, 2024). Atak phishingowy może stanowić zarówno bezpośrednią metodę wyłudzania danych, jak i narzędzie pośrednie służące np. do uruchomienia *ransomware*. W tym kontekście *phishing* staje się zagrożeniem o charakterze hybrydowym – łączącym elementy socjotechniki, inżynierii społecznej i technologicznego zaawansowania.

Współczesny *phishing* nie jest zjawiskiem jednorodnym. Można wyróżnić kilka głównych typów ataków, które różnią się poziomem zaawansowania oraz zakresem celów:

- *phishing* ogólny (*mass phishing*) – szeroko rozpowszechniane e-maile z fałszywymi linkami i załącznikami, często o charakterze promocyjnym lub alarmującym (np. fałszywa informacja o zablokowanym koncie bankowym),
- *spear phishing* – atak ukierunkowany na konkretnego pracownika lub dział instytucji, poprzedzony analizą danych ofiary, np. z mediów społecznościowych,
- *whaling* – atak na osoby zajmujące kluczowe stanowiska kierownicze, często wiążący się z próbą zmanipulowania przelewów finansowych,
- *smishing* – atak realizowany za pomocą wiadomości SMS,

[30] Mechanizmem tego typu jest np. *Real Time Phishing Proxy*.

- *vishing* – oszustwo głosowe (np. fałszywe telefony od pracowników banku lub policji),
- *clone phishing* – wykorzystanie wcześniej wysłanej legalnej wiadomości e-mail, która zostaje podmieniona na złośliwą wersję i ponownie wysłana z zaufanego źródła,
- *pharming* – przekierowywanie użytkownika na fałszywe strony internetowe za pomocą manipulacji w systemie DNS.

W skutecznym phishingu absolutnie kluczową rolę odgrywa psychologia. Przestępcy bazują na klasycznych zasadach perswazji opisanych przez Cialdiniego (2023). Są nimi: społeczny dowód słuszności, autorytet, niedobór oraz wzajemność. Zasady te, pierwotnie opisywane w kontekście marketingu i wpływu społecznego, niezwykle skutecznie zastosowano w cyberprzestępczości. Ich moc polega na uruchamianiu automatycznych mechanizmów poznawczych u ofiar – decyzje podejmowane są często bezrefleksyjnie, w odpowiedzi na presję sytuacyjną. Badania Taiba i in. (2019), które opierały się na dużej symulacji z udziałem ponad 56 000 uczestników, jednoznacznie wykazały, że najskuteczniejsze były techniki wywołujące emocje i poczucie pilności. Elementy takie jak „Twoje konto zostanie zablokowane w ciągu 24 godzin" lub „Masz ostatnią szansę na uniknięcie kary" skutecznie prowokowały reakcje impulsywne. Przestępcy często konstruują komunikaty tak, aby odbiorca poczuł się zaniepokojony lub odpowiedzialny za szybkie podjęcie działania. W warunkach stresu system przetwarzania poznawczego ulega ograniczeniu i dominuje szybkie, automatyczne rozumowanie – znane jako „System 1" w teorii Kahnemana (2023)[31]. W phishingu istotną rolę odgrywa również zjawisko heurystyki dostępności – użytkownicy, którzy niedawno słyszeli o atakach hakerskich lub doświadczyli problemów z kontem bankowym, są bardziej podatni na sugestie zawarte w fałszywych wiadomościach[32]. Psychologiczna dostępność pewnych scenariuszy zwiększa podatność ofiar na manipulacje. Zjawisko to było szczególnie widoczne w czasie pandemii COVID-19, gdy wiele osób doświadczało niepewności finansowej i technologicznej, co ułatwiało cyberprzestępcom tworzenie realistycznych kampanii phishingowych opartych na tematach związanych ze zdrowiem, pomocą finansową i bezpieczeństwem danych (Abdajabar i Idbeaa, 2024). Warto także zwrócić uwagę na wykorzystanie tzw. modelu socjotechnicznego wpływu, który opisuje sześć głównych taktyk manipulacyjnych stosowanych przez cyberprzestępców:

- wzbudzanie zaufania,
- kreowanie presji czasu,
- wykorzystywanie autorytetu,

[31] Zob. także (Gasparski, 2016, s. 115 i n.).

[32] Heurystyka dostępności to uproszczona reguła myślenia, według której ludzie oceniają prawdopodobieństwo lub częstość występowania danego zjawiska na podstawie tego, jak łatwo mogą przywołać je z pamięci. Im łatwiej coś sobie przypomnieć, tym bardziej wydaje się nam to prawdopodobne, częste lub typowe – nawet jeśli obiektywnie nie jest. Paradoksalnie, ta łatwość przywołania czegoś z pamięci zwiększa podatność na ataki phishingowe.

- imitowanie zaufanych źródeł,
- wzbudzanie ciekawości,
- tworzenie fałszywego zagrożenia.

Każda z tych technik została potwierdzona w badaniach jako skuteczna w prowadzeniu użytkownika do nieświadomego wykonania żądanej czynności, np. kliknięcia linku czy podania hasła (Hadnagy, 2011). Zmiany w treści wiadomości phishingowych w ostatnich latach jednoznacznie pokazują, że cyberprzestępcy stale pogłębiają swoją wiedzę psychologiczną. Coraz częściej wiadomości są personalizowane i dostosowane do kontekstu działania ofiary – np. zawierają nazwisko pracownika, nazwę działu, a nawet aktualne procedury obowiązujące w danej organizacji. Według badań Jagatica i in. (2007) spersonalizowane e-maile phishingowe mają wskaźnik skuteczności nawet czterokrotnie wyższy niż anonimowe wiadomości masowe. Przykładami skutecznych strategii psychologicznych mogą być także komunikaty sugerujące dostęp do ekskluzywnej oferty („Masz dostęp do specjalnej oferty inwestycyjnej tylko dziś!") – wykorzystujące zasadę niedoboru, lub wiadomości sugerujące zaufanie nadawcy („Zgodnie z wcześniejszą rozmową – załączam dokument") – aktywujące mechanizm wzajemności. Wszystkie te techniki działają na poziomie automatycznych reakcji emocjonalnych, zanim jeszcze zostanie uruchomiona logiczna analiza sytuacji. Zdolność do wykorzystania naturalnych skrótów poznawczych i emocji ofiar czyni omawiane zagrożenie jednym z najbardziej efektywnych narzędzi w arsenale cyberprzestępców. Co więcej, w dobie rozwoju sztucznej inteligencji i przetwarzania języka naturalnego możliwe staje się tworzenie coraz bardziej przekonujących komunikatów generowanych automatycznie na podstawie analizy danych osobowych dostępnych w sieci (Heiding i in., 2024). Współczesne instytucje finansowe, jeśli mają skutecznie przeciwdziałać tego rodzaju zagrożeniom, muszą więc inwestować nie tylko w technologie bezpieczeństwa, ale przede wszystkim w szkolenia z zakresu psychologii oszustwa cyfrowego, budowanie świadomości poznawczej oraz rozwijanie kompetencji użytkowników w rozpoznawaniu manipulacji.

Phishing nie jest już wyłącznie kwestią indywidualnych błędów użytkowników. W kontekście instytucji finansowych jego skutki mogą zakłócić płynność działania, wpłynąć na rynek finansowy, a nawet uruchomić efekt domina wśród instytucji współpracujących. W połączeniu z *ransomware* staje się zagrożeniem o charakterze systemowym – prowadzącym do złośliwego szyfrowania danych, blokowania dostępu, wymuszeń finansowych, a w konsekwencji do potencjalnego przerwania ciągłości operacyjnej. *Phishing* stanowi obecnie jedno z najbardziej destrukcyjnych zagrożeń dla sektora finansowego, a jego konsekwencje wykraczają daleko poza incydentalne naruszenia bezpieczeństwa. Choć często rozpoczyna się od pojedynczego e-maila lub wiadomości SMS, skutki ataku mogą być głębokie, systemowe i długotrwałe. Jedną z pierwszych i najbardziej bezpośrednich konsekwencji udanego ataku phishingowego jest infekcja systemów instytucji finansowych złośliwym oprogramowaniem. Tego typu oprogramowanie często działa w tle, niezauważone przez standardowe opro-

gramowanie antywirusowe, i może zostać aktywowane po długim czasie „uśpienia", co utrudnia wykrycie źródła naruszenia. W ślad za infekcją technologiczną idzie utrata poufności oraz integralności danych – zarówno klientowskich (np. numery kont, dane osobowe, historie transakcji), jak i operacyjnych (np. logi systemowe, wartości funkcji skrótu dla haseł, schematy działania systemów finansowych). Kolejnym niebezpiecznym skutkiem może być przejęcie kont użytkowników oraz uzyskanie nieautoryzowanego dostępu do systemów wewnętrznych, w tym systemów transakcyjnych czy zarządzania ryzykiem. Taka eskalacja może prowadzić do pełnej kompromitacji infrastruktury cyfrowej instytucji – umożliwiając np. wykonanie nieautoryzowanych przelewów, zmianę ustawień systemowych czy wprowadzanie dalszych mechanizmów ukierunkowanych na przyszłe ataki. Długofalowo najpoważniejszą konsekwencją jest paraliż procesów operacyjnych. W przypadku dużych instytucji finansowych nawet kilkugodzinne zatrzymanie systemów może prowadzić do poważnych strat finansowych i reputacyjnych – nie tylko z powodu przerwania działalności, lecz także w związku z natychmiastową reakcją rynku i spadkiem wartości akcji. W artykule Oesta i in. (2020) podkreślono, że utrata dostępności systemów często prowadzi do fali wycofywania środków przez klientów, masowych reklamacji, a nawet ryzyka runu na bank. Na poziomie społecznym i rynkowym skutkiem phishingu może być także spadek zaufania klientów do instytucji finansowych. Jak wynika z raportu Ponemon Institute (2021), aż 59% klientów po incydencie bezpieczeństwa zmienia swoją instytucję finansową, a 65% deklaruje obniżenie zaufania do cyfrowych kanałów obsługi. Reputacyjne skutki ataku są często trudniejsze do naprawienia niż straty finansowe – odbudowa zaufania może trwać miesiącami, a niekiedy latami.

Konsekwencje phishingu w sektorze finansowym są wielopoziomowe i wzajemnie się wzmacniają. Od technicznych infekcji, przez utratę danych i kompromitację kont, aż po strategiczne skutki dla funkcjonowania całej instytucji – *phishing* to nie tylko kwestia bezpieczeństwa, ale także kluczowy problem zarządzania ryzykiem operacyjnym i reputacyjnym. Dane z raportów potwierdzają, że *phishing* stanowi obecnie najczęstszy typ ataku na instytucje finansowe. Technologie stosowane w nowoczesnych kampaniach obejmują coraz nowsze zdobycze informatyki, także z obszaru biometrii. Coraz większa liczba ataków ukierunkowanych na kadrę zarządzającą w instytucjach finansowych obejmuje wykorzystanie technologii syntezy mowy, umożliwiającej realistyczne odwzorowanie głosu znanych osób. Zjawisko to istotnie zwiększa skuteczność socjotechniczną ataków, co zostało potwierdzone w badaniach nad wpływem sztucznej inteligencji na bezpieczeństwo sektora bankowego (Johora i in., 2024). Kolejnym trendem jest *phishing* za pośrednictwem platform społecznościowych i aplikacji mobilnych. Zaawansowane kampanie coraz częściej są również wspierane przez tzw. *Phishing-as-a-Service* (PhaaS). Na czarnym rynku dostępnych jest już kilkaset zestawów narzędzi tego typu, które umożliwiają mniej doświadczonym cyberprzestępcom prowadzenie wysoce profesjonalnych ataków (Group-IB, 2025). Niepokojące jest również to, że coraz więcej takich kampanii jest zautomatyzowanych za pomocą botów AI, co pozwala atakującym rozwijać działania na niespotykaną dotąd

skalę. W kontekście sektora finansowego trzeba zauważyć, że skuteczność zaawansowanych kampanii phishingowych przekłada się bezpośrednio na straty finansowe. Według danych Federal Bureau of Investigation (2024) różne formy phishingu odpowiadały w 2023 r. za straty przekraczające 10 mld USD.

W związku z dynamicznym rozwojem omawianych technik organizacje finansowe intensyfikują swoje działania w zakresie bezpieczeństwa, wprowadzając wielopoziomowe mechanizmy uwierzytelniania, zaawansowane systemy wykrywania oparte na sztucznej inteligencji oraz kompleksowe programy szkoleniowe dla pracowników. Nawet najlepsze technologie nie są jednak w stanie całkowicie wyeliminować ryzyka, jeśli czynnik ludzki pozostaje najsłabszym ogniwem w łańcuchu bezpieczeństwa. Dlatego też kluczowym elementem w walce z zaawansowanymi kampaniami phishingowymi pozostaje nie tylko inwestycja w nowe technologie, lecz także nieustanne podnoszenie świadomości zagrożeń wśród użytkowników końcowych.

2.2.3. *Malware*

Phishing stanowi obecnie jedno z najczęściej wykorzystywanych i najniebezpieczniejszych narzędzi w arsenale cyberprzestępców. Jego skuteczność nie wynika jednak wyłącznie z manipulacyjnych technik socjotechnicznych, lecz przede wszystkim z synergii, jaką tworzy z innymi formami zagrożeń – w szczególności z infekcjami szkodliwym oprogramowaniem (*malware*). Współczesne kampanie phishingowe rzadko kończą się jedynie na pozyskaniu danych logowania – znacznie częściej są wektorem dostarczania złośliwego kodu. To właśnie zintegrowane działanie phishingu i *malware* odpowiada za najbardziej destrukcyjne incydenty bezpieczeństwa, prowadzące nie tylko do wycieku danych, lecz także do całkowitego zakłócenia działalności organizacji. W rezultacie skutki takich ataków mają charakter wielowymiarowy – obejmując zarówno aspekt techniczny, jak i finansowy oraz reputacyjny.

Termin *malware*, będący skrótem od *malicious software*, odnosi się do każdego rodzaju oprogramowania, które zostało celowo zaprojektowane w sposób szkodliwy wobec użytkownika, jego systemu komputerowego, danych lub infrastruktury sieciowej. W definicji przedstawionej przez National Institute of Standards and Technology *malware* to każdy program komputerowy zaprojektowany w celu zakłócenia, uszkodzenia lub uzyskania nieautoryzowanego dostępu do systemu komputerowego (Souppaya i Scarfone, 2013). Podobną definicję przyjmuje Europejska Agencja ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity – ENISA), która kładzie nacisk na funkcjonalność złośliwego kodu, wskazując, że *malware* to program komputerowy wykorzystywany do złośliwego działania wobec systemu, sieci lub użytkownika, najczęściej bez jego wiedzy i zgody (ENISA, 2025). Wspólną cechą wszystkich form *malware* jest ich działanie bez zgody użytkownika i w sposób ukryty oraz intencjonalne naruszenie integralności, poufności lub dostępności zasobów informatycznych. *Malware* może realizować funkcje kradzieży danych, szyfrowania plików w celu wymuszenia okupu (*ransomware*), przejmowania kontroli nad systemem

lub zakłócania funkcjonowania infrastruktury. Z punktu widzenia klasyfikacji prawnej i normatywnej *malware* wpisuje się w szerszy kontekst przestępczości komputerowej, określanej w konwencji budapeszteńskiej jako *cybercrime*.

Choć dziś *malware* kojarzy się głównie z *ransomware* i atakami hakerskimi, jego historia sięga początków informatyki i rozwoju sieci komputerowych. W 1949 r. John von Neumann jako pierwszy sformułował teoretyczne podstawy programów zdolnych do samoreplikacji, co jest uznawane za koncepcyjny fundament dla rozwoju przyszłych wirusów komputerowych (von Neumann, 1966). Obecnie *malware* jest stosowane nie tylko przez przestępców indywidualnych, lecz także przez zorganizowane grupy, działające często w interesie geopolitycznym (Crowdstrike, 2025). Raporty ENISA oraz producentów oprogramowania antywirusowego potwierdzają, że *malware* jest najczęściej stosowanym narzędziem w kampaniach phishingowych, atakach na infrastrukturę krytyczną oraz oszustwach finansowych[33]. Ze względu na ogromne zróżnicowanie technik i celów działania szkodliwe oprogramowanie jest klasyfikowane według różnych kryteriów. Najczęściej przyjmuje się podział ze względu na sposób działania, technikę infekcji oraz cel ataku. W literaturze przedmiotu oraz dokumentach standaryzujących spotyka się typologię *malware* uwzględniającą następujące kategorie:

- wirusy komputerowe – najstarsza i najbardziej znana forma szkodliwego oprogramowania. Działają poprzez samoczynne kopiowanie się do innych plików lub sektorów systemu, aktywując się przy ich uruchomieniu. Zazwyczaj wymagają interakcji użytkownika,
- robaki – w odróżnieniu od wirusów, nie potrzebują pliku nosiciela ani interwencji użytkownika, rozprzestrzeniają się automatycznie przez sieć, często wykorzystując luki w protokołach lub aplikacjach,
- konie trojańskie podszywające się pod legalne oprogramowanie w celu uzyskania dostępu do systemu,
- oprogramowanie szpiegujące działające w tle, zbierające informacje o użytkowniku: dane logowania, aktywność w przeglądarce, a nawet naciskane klawisze,
- *information stealers* – rozwiązania podobne do oprogramowania szpiegującego, ale bardziej wyspecjalizowane – ukierunkowane na kradzież konkretnych danych,
- oprogramowanie reklamowe generujące niechciane reklamy, często w zamian za pozornie darmowe funkcje,
- *ransomware* – jedna z najbardziej szkodliwych form *malware*, szyfrująca pliki lub całe systemy, a następnie żądająca okupu za ich odszyfrowanie. Szczególnie niebezpieczne są odmiany typu *double extortion*, w których dane są dodatkowo wykradane i grozi się ich ujawnieniem,
- *rootkits* – oprogramowanie pozwalające atakującemu na ukrycie obecności innych komponentów *malware* w systemie,

[33] Problem ten zostanie rozwinięty w dalszej części.

- botnety i *malware* sieciowe – *botnet* to sieć komputerów zainfekowanych *malware*, które są zdalnie kontrolowane przez cyberprzestępców. Urządzenia stają się częścią zautomatyzowanej infrastruktury używanej m.in. do ataków DDoS, rozsyłania spamu, kopania kryptowalut i oszustw finansowych,
- *droppers* – rodzaj złośliwego oprogramowania zaprojektowanego w celu zainstalowania innych typów *malware* na docelowym systemie,
- mechanizmy *backdoor* – zazwyczaj ukryte i nieautoryzowane, umożliwiające obejście standardowych procedur uwierzytelniania lub zabezpieczeń systemu komputerowego, aplikacji, serwera lub sieci,
- *malware* hybrydowy i zautomatyzowany – coraz częściej obserwuje się formy *malware* hybrydowego, łączącego funkcje różnych typów (np. *trojan-ransomware-spyware*). Równocześnie rozwija się *malware* wspomagany przez AI, który potrafi adaptować się do środowiska, omijać zabezpieczenia i wykrywać najlepsze wektory ataku w czasie rzeczywistym.

W tabeli 2 przedstawiono uproszczoną klasyfikację głównych typów szkodliwego oprogramowania.

Tabela 2. Cechy charakterystyczne głównych typów szkodliwego oprogramowania

Typ *malware*	**Cechy charakterystyczne**	**Wymaga interakcji?**	**Najczęstszy cel ataku**
Wirus	replikacja przez pliki	tak	zakłócenie działania systemu
Robak	samoczynne rozprzestrzenianie się	nie	rozprzestrzenianie i niszczenie
Trojan	udawanie legalnego oprogramowania	tak	kradzież, dostęp zdalny
Spyware/Adware	śledzenie, reklamy	nie	dane osobowe
Ransomware	szyfrowanie pamięci stałej i wymuszanie okupu	tak	zysk finansowy
Rootkit	ukrywanie obecności atakującego	nie	trwała kontrola
Botnet	przejęcie kontroli nad urządzeniami	nie	DDoS, spam

Źródło: opracowanie własne.

W sektorze finansowym kluczowym aspektem omawianego zagadnienia jest zrozumienie źródeł infekcji oraz wektorów ataku. Złośliwe oprogramowanie coraz częściej wykorzystuje zaawansowane techniki dystrybucji, które adaptują się dynamicznie do środowiska ofiary (Bustos-Tabernero i in., 2024). Do najpowszechniejszych źródeł infekcji należy zaliczyć następujące[34]:

[34] Na podstawie zbioru raportów dotyczących cyberbezpieczeństwa przedstawionego w następnym rozdziale.

- *phishing* i *spear phishing* – pozostające podstawowym źródłem infekcji systemów finansowych. Kampanie phishingowe dostarczają zainfekowane załączniki lub linki do złośliwych stron WWW, które instalują *malware* po kliknięciu. Skuteczność tych działań wzrasta, gdy są personalizowane (*spear phishing*), co szczególnie zagraża pracownikom sektora bankowego,
- *exploit kits* i luki typu *zero-day* – wektor ten opiera się na wykorzystaniu niezałatanych podatności w oprogramowaniu serwerów bankowych, aplikacji mobilnych i systemów operacyjnych. Ataki z użyciem *exploit kits* często prowadzą do „cichej" infekcji bez wiedzy użytkownika,
- złośliwe oprogramowanie dostarczane przez strony internetowe – infekcja może nastąpić przez odwiedzenie zainfekowanej strony, bez konieczności aktywnego pobrania pliku przez użytkownika. Zjawisko to jest szczególnie groźne dla klientów bankowości elektronicznej korzystających z nieaktualizowanych przeglądarek,
- podszywanie się pod aktualizacje systemowe lub aplikacyjne – fałszywe komunikaty o konieczności aktualizacji oprogramowania są jednym z bardziej podstępnych źródeł infekcji. Atakujący mogą modyfikować kanały dystrybucji lub wysyłać spreparowane wiadomości w imieniu znanych dostawców,
- nośniki fizyczne i ataki insiderskie – choć rzadziej omawiane, infekcje przez zainfekowane nośniki USB lub celowe działanie osób wewnątrz organizacji nadal stanowią poważne zagrożenie, szczególnie w systemach o ograniczonym dostępie do Internetu.

Rozwój szkodliwego oprogramowania wykazuje tendencję do coraz większej specjalizacji i automatyzacji, czemu sprzyja łatwa dostępność gotowych zestawów *exploit*, infrastruktury oraz zaawansowanych narzędzi opartych na sztucznej inteligencji. Współczesny *malware* coraz częściej działa w sposób wysoce wyrafinowany, potrafi unikać detekcji za pomocą technik polimorficznych i korzysta z kanałów szyfrowanych, co utrudnia klasyczne monitorowanie ruchu sieciowego. Należy się spodziewać dalszej ewolucji szkodliwego oprogramowania w stronę ataków autonomicznych, opartych na algorytmach samouczących się, a także prób wykorzystania luk w systemach IoT i rozwiązań chmurowych. Taka dynamika rozwoju stawia przed sektorem finansowym poważne wyzwania związane z koniecznością wdrażania proaktywnych, adaptacyjnych mechanizmów obrony.

2.2.4. *Denial of Service*

Wśród szerokiego spektrum zagrożeń cybernetycznych, jakie dotykają współczesne instytucje finansowe, szczególne miejsce zajmują ataki typu *Denial of Service* (DoS) oraz ich rozproszone warianty określane mianem *Distributed Denial of Service* (DDoS). Zjawisko to jest definiowane jako celowe przeciążenie zasobów infrastrukturalnych lub aplikacyjnych danej jednostki, prowadzące do utraty dostępności usług dla uprawnionych użytkowników (Mirkovic i Reiher, 2004). W kontekście sektora finansowego, którego funkcjonowanie opiera się na ciągłości operacji i nieprzerwanym

dostępie do usług cyfrowych, skutki takich incydentów mogą przybrać postać poważnych strat finansowych, degradacji reputacji marki oraz zakłócenia integralności systemów. Ataki DoS realizowane są przez generowanie nadmiernego ruchu sieciowego – wysyłanie milionów zapytań lub pakietów danych – w celu wyczerpania zasobów atakowanego systemu, takich jak pasmo sieciowe, moc obliczeniowa serwerów czy limity aplikacji. Ataki typu odmowy usługi stanowią kategorię cyberataków ukierunkowanych na konkretne aplikacje lub serwisy internetowe, których celem jest wyczerpanie zasobów systemowych ofiary. W rezultacie prowadzi to do niedostępności lub nieosiągalności zaatakowanego systemu, skutecznie uniemożliwiając prawidłowy dostęp do usługi przez uprawnionych użytkowników. Mimo że ataki DoS mogą przyjmować wiele form, w literaturze przedmiotu najczęściej wyróżnia się trzy następujące typy (S. Kumar i in., 2022):

- przeciążenie zasobów sieciowych, które polega na wykorzystaniu wszelkich dostępnych zasobów sprzętowych, programowych lub przepustowości sieciowej w celu ataku. W przypadku bezpośredniego przeciążenia zasobów sieciowych sprawca cyberataku doprowadza do przeciążenia przez działania takie jak eksploatacja luk w zabezpieczeniach serwera lub masowe przesyłanie dużej liczby żądań. W przypadku ataku refleksyjno-amplifikacyjnego napastnik wykorzystuje serwery pośredniczące („reflektory"), aby zwielokrotnić wolumen ruchu sieciowego kierowanego na cel. Atak polega na przesyłaniu żądań do serwerów trzecich, z podszytym adresem IP ofiary, co powoduje, że odpowiedzi serwerów są automatycznie przekazywane na adres celu, prowadząc do przeciążenia jego infrastruktury,
- przeciążenie zasobów protokołów komunikacyjnych – polega na wykorzystaniu wszystkich dostępnych zasobów sesji lub połączeń w infrastrukturze ofiary, co skutecznie blokuje możliwość nawiązywania nowych połączeń przez prawidłowych użytkowników,
- przeciążenie zasobów aplikacyjnych – obejmuje eksploatację zasobów obliczeniowych lub pamięciowych aplikacji poprzez generowanie żądań, które prowadzą do wyczerpania możliwości przetwarzania danych lub przechowywania informacji przez system docelowy.

W klasycznym modelu DoS źródłem ataku jest pojedyncze urządzenie lub ograniczona liczba punktów ataku. Jednak znacznie bardziej niebezpieczną formą są ataki rozproszone (DDoS), w których ruch jest sztucznie generowany równocześnie z wielu lokalizacji, z wykorzystaniem botnetów – sieci zainfekowanych urządzeń, takich jak komputery osobiste, serwery, routery, a nawet urządzenia IoT (Kolias i in., 2017). *Botnets* wykorzystywane do przeprowadzania ataków DDoS są często wynikiem działalności zorganizowanych grup cyberprzestępczych, a ich liczebność może sięgać milionów zainfekowanych urządzeń. Charakterystyka ataków DDoS obejmuje dziś szeroki wachlarz technik, w tym ataki wolumetryczne, ataki na poziomie protokołów oraz ataki aplikacyjne, co czyni je jednym z najtrudniejszych do przeciwdziałania typów zagrożeń.

Znaczenie problematyki DoS/DDoS w sektorze finansowym jest wielokrotnie podkreślane w literaturze przedmiotu. Jak zauważają Mahjabin i in. (2017), instytucje finansowe, jako elementy infrastruktury krytycznej, są szczególnie narażone na ataki motywowane względami ekonomicznymi, politycznymi, a nawet ideologicznymi. Skuteczność ataków DDoS w tym sektorze wynika m.in. z wysokiej wartości transakcyjnej operacji finansowych, co powoduje, że nawet krótkotrwała niedostępność usług może generować gigantyczne straty. Instytucje finansowe stanowią atrakcyjny cel dla sprawców ataków z kilku kluczowych powodów:

- dużej wartości transakcji finansowych w krótkim czasie (Singh i Behal, 2020),
- dużej wrażliwości klientów na przerwy w dostępie do usług (Hovav i D'Arcy, 2003),
- wymogów regulacyjnych dotyczących nieprzerwanej dostępności i ochrony danych (Mahjabin i in., 2017).

W XXI w. techniki ataków DDoS ewoluowały w sposób dynamiczny. W latach 2000-2010 dominowały proste ataki floodowe (UDP Flood, SYN Flood) (Hovav i D'Arcy, 2003). W latach 2010-2020 nastąpił rozwój technik refleksji i amplifikacji z wykorzystaniem serwerów DNS, NTP i SSDP. Obecnie obserwuje się wzrost znaczenia ataków wielowektorowych oraz wykorzystania sztucznej inteligencji do dynamicznej modyfikacji schematów ataku. W szczególności ataki amplifikacyjne, które pozwalają na zwiększenie siły ataku nawet 50-krotnie, stały się istotnym zagrożeniem (Antonakakis i in., 2017).

W odpowiedzi na coraz większe zagrożenie ze strony ataków typu DoS oraz ich rozproszonych wariantów, instytucje finansowe intensyfikują wysiłki w zakresie implementacji zaawansowanych technologii ochrony infrastruktury krytycznej. Środki te nie ograniczają się jedynie do tradycyjnych mechanizmów zabezpieczających, lecz obejmują wielowarstwowe strategie oparte na nowoczesnych narzędziach analitycznych i predykcyjnych. Kluczowymi rozwiązaniami w tym obszarze są systemy wykrywania anomalii (*Anomaly Detection Systems*). Nowoczesne systemy tego typu są oparte na analizie danych sieciowych w czasie rzeczywistym, wykorzystując zaawansowane algorytmy uczenia maszynowego, takie jak głębokie sieci neuronowe czy modele klasyfikacyjne typu *Random Forest* (Farnaaz i Jabbar, 2016). Głównym celem tych systemów jest identyfikacja nietypowych wzorców ruchu, które mogą wskazywać na próbę przeprowadzenia ataku DDoS, zanim spowoduje on zakłócenie usług (Singh i Behal, 2020). Przewaga takich systemów polega na ich zdolności do adaptacji do dynamicznie zmieniającego się środowiska sieciowego oraz wykrywania tzw. ataków typu *zero-day*, które nie mają jeszcze zdefiniowanych sygnatur.

Innym rozwiązaniem przeciwdziałającym DoS są rozproszone systemy *load balancing* (*Distributed Load Balancing Systems*). W celu ograniczenia wpływu ataków wolumetrycznych instytucje finansowe stosują rozproszone systemy równoważenia obciążenia, które automatycznie dystrybuują ruch sieciowy pomiędzy wiele centrów danych lub węzłów serwerowych (Hovav i D'Arcy, 2003). *Load balancers* umożliwiają nie tylko zwiększenie wydolności infrastruktury, ale również redukcję ryzyka pojedyn-

czego punktu awarii (*single point of failure*), co znacznie poprawia odporność systemu na ataki przeciążeniowe.

Systemy klasy *Intrusion Detection/Prevention* (IDS/IPS) stanowią natomiast fundament wczesnego ostrzegania przed zagrożeniami. IDS analizują ruch sieciowy pod kątem znanych sygnatur ataków lub anomalnych zachowań, IPS idą jeszcze krok dalej – są w stanie automatycznie blokować podejrzany ruch w czasie rzeczywistym, zanim osiągnie docelowe zasoby (Mahjabin i in., 2017). W kontekście ochrony przed atakami DDoS, IDS/IPS pełnią funkcję filtrów wstępnych, umożliwiając eliminację niepożądanego ruchu, zanim przeciąży on zasoby aplikacyjne lub sieciowe.

Współczesne strategie obronne coraz częściej integrują komponenty analizy wywiadu o zagrożeniach (*Cyber Threat Intelligence*), które polegają na systematycznym gromadzeniu, analizowaniu oraz korelowaniu informacji o bieżących i przyszłych zagrożeniach cybernetycznych. W kontekście przeciwdziałania atakom DDoS, CTI umożliwia wcześniejsze rozpoznawanie schematów kampanii ataków, identyfikację źródeł zagrożeń oraz dynamiczne dostosowywanie polityk bezpieczeństwa do aktualnych trendów w cyberprzestępczości. Wdrażanie wymienionych rozwiązań w sposób kompleksowy, zintegrowany i wielowarstwowy znacznie zwiększa odporność instytucji finansowych na incydenty typu DoS i DDoS, jednocześnie podnosząc ogólny poziom cyberbezpieczeństwa infrastruktury krytycznej.

Ekonomiczne konsekwencje ataków typu *Distributed Denial of Service* cechują się znaczną złożonością i wielowymiarowością, obejmując zarówno bezpośrednie straty materialne, jak i długofalowe skutki wpływające na funkcjonowanie organizacji w wymiarze finansowym, operacyjnym oraz reputacyjnym (Mirkovic i Reiher, 2004). Skuteczność ataków DDoS w generowaniu strat wynika nie tylko z ich natychmiastowego wpływu na ciągłość operacyjną instytucji finansowych, lecz także z efektów ubocznych, które mogą się materializować w dłuższym horyzoncie czasowym. Główne kategorie strat związanych z incydentami DDoS obejmują:

- straty finansowe bezpośrednie,
- koszty naprawcze i rekonfiguracyjne,
- utratę reputacji i zaufania klientów,
- kary regulacyjne i odpowiedzialność prawną.

Skalę zagrożenia związanego z atakami typu *Distributed Denial of Service* doskonale ilustrują najnowsze dane, zgodnie z którymi globalne koszty wynikające z takich incydentów w 2025 r. przekroczą wartość 25 mld USD (Sunna i in., 2025). Trend ten jednoznacznie wskazuje, iż zagrożenia DDoS należy postrzegać nie wyłącznie w kategoriach problemów technologicznych, lecz jako poważne wyzwanie strategiczne, wymagające kompleksowego przygotowania organizacyjnego oraz adekwatnych inwestycji w zwiększenie odporności infrastruktury cyfrowej.

2.2.5. Zagrożenia *cloud computing*

Kolejną istotną kategorią zagrożeń o charakterze systemowym jest szeroko rozumiany outsourcing usług informatycznych, który w aktualnych uwarunkowaniach technologicznych wyraża się przede wszystkim w rozwiązaniach chmurowych (*cloud computing*). Rozwiązania te, mimo licznych zalet funkcjonalnych i kosztowych, wprowadzają nowe typologie ryzyka, zwłaszcza w kontekście zewnętrznej kontroli nad infrastrukturą oraz przetwarzanymi danymi. Outsourcing – definiowany jako delegowanie odpowiedzialności za zarządzanie zasobami informatycznymi podmiotom trzecim – stanowi odpowiedź na rosnącą presję organizacyjną na ograniczanie kosztów operacyjnych i minimalizację ryzyk związanych z wewnętrzną eksploatacją systemów. W tym sensie, z perspektywy zarządczej, migracja do chmury może być postrzegana jako strategia racjonalizacji zasobów i koncentracji na kluczowych kompetencjach organizacji, jednakże, z punktu widzenia analizy systemowej oraz ewaluacyjnej, rosnące uzależnienie od rozwiązań typu *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) czy *Software-as-a-Service* (SaaS) prowadzi do przesunięcia wektora odpowiedzialności za bezpieczeństwo poza organizację macierzystą. Paradoksalnie, choć *cloud computing* rozwiązuje wiele problemów związanych z redundancją, skalowalnością i ciągłością działania, jednocześnie generuje nowe płaszczyzny podatności – zarówno na poziomie architektury technicznej, jak i w zakresie zgodności z regulacjami. Przetwarzanie w chmurze koresponduje ze stale rosnącą potrzebą minimalizowania ryzyka informatycznego przez eliminowanie własnych systemów i zastępowania ich rozwiązaniami zarządzanymi zewnętrznie. Z ewaluacyjnego oraz systemowego punktu widzenia *cloud computing* – rozwiązując oczywiście część problemów zarządzania cyberbezpieczeństwem – w ujęciu globalnym paradoksalnie podwyższa poziom ryzyka informatycznego[35]. Sam w sobie nie jest zagrożeniem *sensu stricto*, ale jego powszechne zastosowania potęgują ryzyko realizacji praktycznie wszystkich znanych zagrożeń bezpieczeństwa (Sen, 2013). W kontekście instytucji finansowych jest to zjawisko szczególnie ważne, gdyż dotyczy danych objętych zarówno tajemnicą bankową, jak i przepisami dotyczącymi ochrony danych osobowych oraz warunkujących efektywne funkcjonowanie instytucji na rynku. Z problematyką outsourcingu usług informatycznych koresponduje także filozofia *open banking*. Nie jest oczywiście tożsama z outsourcingiem, jednak w podobny sposób umiejscawia w systemie finansowym tzw. podmioty trzecie, czyli instytucje niezwiązane bezpośrednio z finansami i systemem rozliczeniowym, oferujące jednak narzędzia i interfejsy wspomagające ten system. *Open banking* to koncepcja wdrożona już w Unii Europejskiej przez dyrektywę PSD2 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366…). Otwiera ona zupełnie nowe możliwości funkcjonowania firmom z szeroko rozumianego obszaru fintech w procesach dotychczas zarezerwowanych

[35] To być może kontrowersyjne stwierdzenie wymaga komentarza. *Cloud computing* stał się standardem organizacyjno-technologicznym, który przetransferował z outsourcingu wybranych usług informatycznych do holistycznego podejścia ukierunkowanego na mitygowanie.

dla banków i innych instytucji tworzących systemy rozliczeniowe. Podobnie jak w przypadku *cloud computing* trudno krytykować samą koncepcję – jest jednak wielką niewiadomą, w jaki sposób jej powszechne implementacje wpłyną na ryzyko informatyczne w skali globalnej.

2.2.6. *Advanced Persistent Threat*

Stosunkowo nową kategorią zagrożeń wśród uprzednio wymienionych są ataki typu *Advanced Persistent Threat* (APT). Termin ten odnosi się do kompleksowych działań organizacyjnych, których autorstwo przypisuje się zazwyczaj dużym grupom przestępczym, organizacjom o wysokim poziomie profesjonalizacji, a nawet państwom prowadzącym długofalowe kampanie ukierunkowane na uzyskanie nieautoryzowanego dostępu do krytycznych zasobów informatycznych i ich niezauważalne wykorzystywanie przez długi czas. APT stanowią dziś rzeczywisty przykład strategii cyberoperacji o potencjalnie paramilitarnym charakterze, w których dochodzi do precyzyjnego planowania działań, stosowania wyrafinowanych technik inżynierii społecznej (np. *spear phishing*), a także wykorzystania rozproszonych sieci agentów i narzędzi do długoterminowej eksfiltracji danych. APT wyróżniają się wyższym niż w przypadku tradycyjnych ataków poziomem wyrafinowania, zdolnością szybkiej koordynacji działań oraz coraz bardziej sformalizowanymi strukturami współpracy, umożliwiającymi skuteczne pokonanie zaawansowanych mechanizmów bezpieczeństwa – często przez przejęcie przyczółków w infrastrukturze organizacji i eskalację uprawnień od wewnątrz. Motywacje intruzów w przypadku APT są ukierunkowane zarówno na cele polityczne czy militarne, jak i na długoterminowe korzyści finansowe. Kluczowymi cechami tego rodzaju przedsięwzięć pozostają wytrwałość, umiejętność ukrywania się w środowisku ofiary oraz konsekwencja w osiąganiu założonych celów strategicznych. Interdyscyplinarny charakter ataków APT, integrujący wiedzę z zakresu technologii, socjotechniki oraz inżynierii bezpieczeństwa, powoduje, że zagrożenia te są szczególnie trudne do wykrycia i neutralizacji, nawet przy zastosowaniu zaawansowanych systemów wykrywania włamań i procedur reagowania na incydenty (Ahmad i in., 2019).

2.2.7. Zagrożenia związane ze sztuczną inteligencją

Dynamiczny rozwój zastosowań sztucznej inteligencji jest jednym z najbardziej przełomowych zjawisk współczesnej transformacji cyfrowej, oferując znaczne usprawnienia w zakresie automatyzacji procesów ochrony infrastruktury teleinformatycznej, w tym systemów detekcji anomalii, analizy ryzyka czy predykcji zagrożeń. Niemniej należy zauważyć, że równolegle z potencjałem wspierania cyberbezpieczeństwa technologie AI wprowadzają nowe wyzwania i zagrożenia, których skala oraz dynamika wymykają się często tradycyjnym mechanizmom kontroli. Szczególnie istotne jest ryzyko związane z tym, że sztuczna inteligencja może zostać wykorzystana w spo-

sób złośliwy, wzmacniając skuteczność ataków cybernetycznych, zwiększając ich automatyzację oraz poziom precyzji. W literaturze przedmiotu wskazuje się, że AI może umożliwiać przeciwnikom szybkie i elastyczne dostosowanie się do zabezpieczeń ofiary, przy jednoczesnym ograniczeniu kosztów prowadzenia ataków (Brundage i in., 2024). Ponadto algorytmy uczenia maszynowego mogą być instrumentalizowane do generowania wysoce wiarygodnych treści fałszywych, przełamywania zabezpieczeń biometrycznych[36], a także do kamuflowania i rekonfiguracji szkodliwego oprogramowania w sposób utrudniający jego wykrycie. W konsekwencji sztuczna inteligencja jawi się nie tylko jako narzędzie wzmacniające potencjał obronny, lecz także jako czynnik mogący destabilizować środowisko bezpieczeństwa informatycznego, tworząc nowe wektory ataku oraz podważając zaufanie do tradycyjnych mechanizmów ochronnych. Najważniejsze zagrożenia wynikające z zastosowań technologii AI w cyberprzestrzeni wymieniono poniżej.

- Automatyzacja ataków – algorytmy uczenia maszynowego mogą zostać wykorzystane przez cyberprzestępców do błyskawicznego rozpoznawania słabości systemów obronnych oraz do generowania precyzyjnych kampanii phishingowych czy *ransomware*. Badania wskazują, że algorytmy AI mogą optymalizować proces rekonesansu i eskalacji uprawnień w infrastrukturze sieciowej (Brundage i in., 2024).
- Generowanie złośliwych treści (*deepfake*) – sztuczna inteligencja umożliwia tworzenie syntetycznych materiałów wideo i audio, które mogą posłużyć do ataków socjotechnicznych na bezprecedensową skalę. *Deepfake* może skutecznie podważać zaufanie do kanałów komunikacji elektronicznej, a także być wykorzystywany w atakach na kadry zarządzające w instytucjach finansowych (Mirsky i Lee, 2021).
- Przełamywanie zabezpieczeń biometrycznych – algorytmy generatywne, np. GAN (*Generative Adversarial Networks*), mogą produkować syntetyczne obrazy odcisków palców czy twarzy w celu obejścia mechanizmów uwierzytelniania biometrycznego (Sharif i in., 2019).
- Automatyczne tworzenie i ukrywanie szkodliwego oprogramowania – AI jest w stanie wspierać tworzenie polimorficznych wariantów *malware*, trudnych do wykrycia tradycyjnymi systemami antywirusowymi, dzięki czemu złośliwy kod może adaptować się do zmian w środowisku i unikać detekcji (Rigaki i Garcia, 2018).
- Ataki na modele AI (AI vs AI) – coraz częściej wskazuje się, że systemy sztucznej inteligencji same w sobie mogą być celem ataków, np. poprzez *adversarial examples*, które wprowadzają niewielkie modyfikacje danych wejściowych, skutkujące błędną klasyfikacją w modelach wykrywających zagrożenia (Biggio i Roli, 2018).

[36] Ten aspekt omawianego zagadnienia wydaje się szczególnie istotny. Metody biometryczne, pozornie bardzo dobrze nadające się do wykorzystania w procesach uwierzytelnienia, są najbardziej narażone na zagrożenia związane z generowaniem fałszywych obrazów, filmów, dźwięków. Rozwój narzędzi AI w tym obszarze stawia duży znak zapytania przy problemie powszechnej efektywności metod biometrycznych.

- Zwiększenie skuteczności inżynierii społecznej – modele językowe mogą generować spersonalizowane wiadomości w języku naturalnym, pozbawione błędów, dostosowane do profilu ofiary (np. na podstawie jej aktywności w mediach społecznościowych), co radykalnie podnosi efektywność phishingu, spear-phishingu i BEC (*Business Email Compromise*).
- Cyberataki w czasie rzeczywistym i adaptacyjne kampanie ofensywne – dzięki zdolności uczenia się na bieżąco systemy AI mogą modyfikować parametry ataku w odpowiedzi na zachowanie systemu obronnego ofiary, co utrudnia ich neutralizację i skraca czas potrzebny na obejście zabezpieczeń.

Poza oczywistymi konsekwencjami wymienionymi powyżej istnieje jeszcze jedno, być może najpoważniejsze zagrożenie. Jest nim utrata zaufania do systemów i procesów cyfrowych. To szczególnie niebezpieczne zjawisko. Bardzo szybko przybiera na sile, korzystając nie tylko z technologii, ale także z malejącego poziomu świadomości informatycznej użytkowników końcowych. Erozja zaufania do komunikacji i instytucji, zwłaszcza finansowych, jest przejawem stosunkowo nowego zjawiska, jakim jest tzw. paradoks zaufania do AI. Z jednej strony bowiem modele generatywne produkują treści o dużej wierności, przez co użytkownikom coraz trudniej jest ocenić, co jest prawdziwe, a co syntetyczne; z drugiej – naturalna atrakcyjność takich komunikatów sprzyja ich bezkrytycznemu przyjmowaniu jako autentycznych. Badania tego bardzo młodego zjawiska już wykazują, że sztucznie generowane treści rozprzestrzeniane w mediach społecznościowych mogą nie tylko sprowokować pojedyncze decyzje odbiorców, lecz także przyczynić się nawet do zjawisk masowych, w tym wycofywania depozytów bankowych. Według szacunków już 10 GBP wydanych na reklamy może skutkować wycofaniem aż miliona GBP depozytów[37].

Według raportu Deloitte (2024a) niemal 26% kadry kierowniczej doświadczyło incydentów z użyciem *deepfake*, a 92% firm poniosło straty finansowe w związku z ich skutkami. W literaturze wskazuje się zatem nowy, poważny czynnik ryzyka reputacyjnego, ponieważ dezinformacja i *deepfake* mogą znacznie nadwyrężyć wiarygodność instytucji finansowej oraz zmniejszyć zaufanie klientów (Mustak i in., 2023). Jednocześnie badania psychologiczne dostarczają dalszych wniosków: eksperymenty przeprowadzone w USA i Singapurze wykazały, że ekspozycja na *deepfake* przedstawiający katastrofy infrastrukturalne (np. zawalenie mostu) istotnie podnosi poziom nieufności wobec rządu, szczególnie wśród osób o niższym poziomie wykształcenia (Ahmed i in., 2025). Z kolei badania nad wyjaśnieniami generowanymi przez AI wykazały, że nawet fałszywe, lecz logicznie brzmiące uzasadnienia wygenerowane przez LLM silniej wzmacniają wiarę w nieprawdziwe wiadomości niż zwykłe błędne klasyfikacje, co podkreśla potrzebę wzmacniania kompetencji logicznego rozumowania i krytycznego myślenia w społeczeństwie (Danry i in., 2024).

[37] To oczywiście bardzo ogólny szacunek, niemniej skala zjawiska nakazuje traktować je w kategoriach kluczowego zagrożenia dla ryzyka działalności bankowej; zob. np. (Howcroft, 2025).

Podsumowując, można stwierdzić, że sztuczna inteligencja jawi się jako klasyczny przykład technologii o charakterze „miecza obosiecznego" (*dual-use technology*) – te same jej mechanizmy mogą służyć zarówno wzmacnianiu, jak i osłabianiu odporności cybernetycznej organizacji. Rozwiązania oparte na AI, takie jak zaawansowane systemy wykrywania anomalii, predykcja zagrożeń czy adaptacyjne mechanizmy reagowania, istotnie podnoszą skuteczność obrony przed atakami w cyberprzestrzeni, skracając czas detekcji incydentów i umożliwiając proaktywne zarządzanie ryzykiem. Jednakże te same algorytmy w rękach podmiotów przestępczych mogą zostać zaadaptowane w celu automatyzacji działań ofensywnych, precyzyjnego omijania systemów obronnych oraz skalowania ataków z minimalnym udziałem czynnika ludzkiego (ENISA, 2020). W literaturze przedmiotu podkreśla się, że kluczowe wyzwania związane z omawianą technologią obejmują przede wszystkim potrzebę zwiększenia przejrzystości modeli AI, umożliwiającej audyt, weryfikację oraz zrozumienie procesów decyzyjnych w kontekście bezpieczeństwa (*explainable AI* – XAI). Równolegle konieczne jest wdrażanie metod odpornościowych na ataki przeciwnika, takich jak techniki *adversarial training*, detekcja danych zmanipulowanych czy mechanizmy kontroli integralności modelu. Istotnym aspektem jest także opracowanie i egzekwowanie międzynarodowych standardów etycznych oraz regulacyjnych, które będą przeciwdziałać niekontrolowanemu wykorzystaniu AI w cyberprzestępczości i cyberwojnie. Przyszłość zastosowań sztucznej inteligencji w cyberbezpieczeństwie będzie zależeć od zdolności społeczności naukowej, przemysłu i regulatorów do wypracowania równowagi między innowacyjnością a bezpieczeństwem, tak aby potencjał tej technologii mógł być w pełni wykorzystany w działaniach defensywnych, przy jednoczesnym minimalizowaniu ryzyka jej destrukcyjnego zastosowania.

2.2.8. Studia przypadków

Podrozdział niniejszy przybliża wybrane, upublicznione wydarzenia będące skutkami ataków na systemy instytucji finansowych na świecie. Źródłem wiedzy na temat tych wydarzeń są różne serwisy internetowe, warto jednak pamiętać, że pełna wiarygodność tego typu informacji jest dyskusyjna. Mimo to można przyjąć, że zakres upubliczniannych informacji na temat skutków ataków na systemy informatyczne jest co najmniej równy ich rzeczywistym zakresom. Atakowane instytucje – szczególnie finansowe – starają się bowiem za wszelką cenę ograniczać dostępność potwierdzonych informacji związanych z cyberbezpieczeństwem, które mogłyby negatywnie wpływać na ich reputację.

W latach 2015-2016 doszło do serii spektakularnych ataków wymierzonych w banki korzystające z globalnej sieci SWIFT (Society for Worldwide Interbank Financial Telecommunication). Hakerzy uzyskali dostęp do uprawnień operatorów bankowych, co pozwoliło im na wysyłkę fałszywych instrukcji przelewów SWIFT, wyglądających autentycznie dla systemów odbiorczych. Najbardziej znanym przypadkiem zastosowania tej techniki jest atak na rachunek Centralnego Banku Ban-

gladeszu w lutym 2016 r., kiedy to cyberprzestępcy przesłali 35 zleceń przelewu na kwotę prawie 1 mld USD, z czego pięć zostało zrealizowanych. W rezultacie skradziono ok. 101 mln USD (Wikipedia, b.d.). Ataki nie ograniczały się jedynie do Bangladeszu. Już w 2015 r. Banco del Austro w Ekwadorze stracił 12,2 mln USD, a w Wietnamie hakerzy zdołali wytransferować 1,36 mln USD – wszystko na skutek kompromitacji lokalnego środowiska informatycznego, umożliwiającej wysyłanie autoryzowanych zleceń SWIFT z wykorzystaniem prawdziwych poświadczeń bankowych. Kluczowym elementem tych ataków była instalacja niestandardowego *malware* w systemie bankowym, pozwalającego na wygenerowanie i wysłanie fałszywych komunikatów SWIFT, a jednocześnie na ukrycie ich poprzez modyfikację raportów systemowych.

Równie wielką skalą ataku charakteryzowała się operacja Carbanak. Była jedną z najbardziej spektakularnych kampanii cyberprzestępczych wymierzonych bezpośrednio w banki. Rozpoczęta pod koniec 2013 r., skierowana była przeciwko instytucjom finansowym w ponad 30 krajach, obejmując ok. 100 celów i generując straty sięgające od 2,5 do 10 mln USD na bank, a łącznie szacowane na ok. 1 mld USD (Securelist, 2015). Metodyka działania grupy cyberprzestępców była wysoce zaawansowana. Ataki zaczynały się od spreparowanych spear-phishingowych maili skierowanych do pracowników banków, zawierających zainfekowane załączniki (.doc, .cpl), które wykorzystywały luki w Microsoft Office do instalacji backdoora Carbanak. Zainfekowane systemy umożliwiały cyberprzestępcom uzyskanie pełnej kontroli nad siecią banku – m.in. dostęp do kamer monitoringu, urządzeń ATM, systemów Oracle i środowisk bankowości online. Atakująca grupa przeprowadzała fazę manualnego rozpoznania i podsłuchu, rejestrując dane wprowadzane z klawiatur, zrzuty ekranowe i wideonagrania aktywności pracowników, co pozwalało odtworzyć wzorce ich pracy i produkować fałszywe, wiarygodne transakcje. W zależności od strategii środki wyprowadzano na dwa sposoby: przez nadpisanie sald kont i natychmiastowy transfer „nadwyżki" do kont przestępców oraz manipulację bankomatami, które wydawały gotówkę o określonych godzinach. Wynajęci pośrednicy (*mules*) podejmowali gotówkę w imieniu atakujących. Operacja Carbanak stanowiła swego rodzaju przełom w historii cyberprzestępczości finansowej. Była skoordynowana, długoterminowa i nastawiona na bezpośrednie wykradanie gotówki, co wyróżnia ją spośród dotychczasowych ataków wymierzonych przede wszystkim w dane klientów. Wymusiła także międzynarodową współpracę służb ścigania i zainicjowała zmiany w podejściu instytucji finansowych do monitoringu, segmentacji sieci i edukacji pracowników.

Innym bardzo znanym incydentem o charakterze masowym był atak wykorzystujący błąd logiczny w konstrukcji strony internetowej First American Financial Corp, który umożliwił publiczny dostęp do informacji (w tym danych o kredytach hipotecznych) dzięki brakowi mechanizmu weryfikacji dostępu. Ten tzw. *Business Logic Flaw* spowodował wyciek aż 885 mln rekordów zawierających dane osobowe i finansowe (Kost, 2025). To ujawnienie nie zostało zainicjowane przez hakera. Podatność, która umożliwiła dostęp do wrażliwych danych, była wynikiem błędu wewnętrznego – zda-

rzenia znanego jako *data leaks*. Choć *data leaks* i *data breaches* to dwa różne typy incydentów, oba niosą ze sobą ten sam potencjalny skutek – przedostanie się wrażliwych informacji klientów w ręce cyberprzestępców.

Wśród najnowszych incydentów cyberbezpieczeństwa nie można nie wspomnieć o globalnej awarii znanej jako *CrowdStrike Falcon*. 19 lipca 2024 r. firma CrowdStrike – dostawca zaawansowanego oprogramowania zabezpieczającego klasy Endpoint Detection and Response (EDR), znanego jako Falcon Sensor – przypadkowo wywołała największą w historii globalną awarię informatyczną. W rezultacie wadliwej aktualizacji mechanizmu odpowiedzialnego za obsługę komunikacji międzyprocesowej wystąpił błąd związany z odczytem pamięci poza dozwolonym zakresem, co spowodowało nagłe awarie systemu oraz niekiedy wejście urządzeń w pętlę startową lub tryb odzyskiwania. Według szacunków Microsoftu aktualizacja wpłynęła na ok. 8,5 mln urządzeń z systemem Windows (mniej niż 1% wszystkich aktywnych komputerów), lecz objęła kluczową infrastrukturę przedsiębiorstw i instytucji. Skala zakłóceń była bezprecedensowa: dotknięte zostały sektory transportu lotniczego, mediów, systemy bankowe, szpitale, centra ratunkowe i administracja publiczna, co doprowadziło do globalnych opóźnień, odwołanych lotów, przerw w udzielaniu usług oraz strat ekonomicznych szacowanych na co najmniej 10 mld USD. W odpowiedzi na awarię CrowdStrike opublikował poprawkę i współpracował ze służbami, choć wiele systemów wymagało ręcznej interwencji. Całe zdarzenie podkreśliło potrzebę rygorystycznych testów i procedur wdrożeniowych w środowiskach krytycznej infrastruktury cyfrowej.

W lutym 2025 r. odnotowano incydent o istotnym znaczeniu dla dyskusji nad wpływem technologii *deepfake* na bezpieczeństwo sektora finansowego, związany z próbą oszustwa inwestycyjnego z wykorzystaniem wizerunku znanego brytyjskiego menedżera funduszy inwestycyjnych Anthony'ego Boltona. Jak poinformował portal *Financial News*, cyberprzestępcy opublikowali w mediach społecznościowych materiał wideo wygenerowany przy użyciu technologii generatywnej sztucznej inteligencji (GAN), w którym syntetyczna wersja Boltona zachęcała odbiorców do dołączenia do rzekomej grupy inwestycyjnej w aplikacji WhatsApp, oferującej atrakcyjne warunki lokowania kapitału. Analiza incydentu wskazuje, że tego typu ataki wykorzystują efekt autorytetu oraz wysoką wiarygodność generowanych treści w celu przeprowadzenia socjotechnicznych kampanii wyłudzających dane osobowe i środki finansowe od inwestorów detalicznych. Według raportów branżowych wolumen przypadków oszustw inwestycyjnych z użyciem *deepfake* gwałtownie rośnie – liczba zgłoszeń w tym segmencie wzrosła w 2024 r. o ponad 2000% w stosunku do roku poprzedniego (Deloitte, 2024b). Incydent z wykorzystaniem wizerunku Boltona stanowi przykład nowej klasy zagrożeń, w której granica między autentycznym a syntetycznym przekazem zostaje zatarta, co w konsekwencji może prowadzić do erozji zaufania do komunikacji elektronicznej oraz instytucji finansowych jako takich.

Jak już wspomniano, wiele incydentów jest ukrywanych przez instytucje lub informacje na ich temat są niepełne. Skutków niektórych zdarzeń nie da się jednak

ukryć, gdyż wpływają bezpośrednio na rozwiązania informatyczne oferowane użytkownikom końcowym. Jednym z takich przypadków jest atak na firmę Garmin – producenta m.in. urządzeń GPS oraz zegarków sportowych. Według zgromadzonych raportów i analiz, w lipcu 2020 r. firma Garmin padła ofiarą ataku typu *ransomware* wykorzystującego oprogramowanie WastedLocker. Zaszyfrowane zostały systemy wewnętrzne, co spowodowało poważne zakłócenia usług, m.in. Garmin Connect, flyGarmin oraz serwisów wsparcia technicznego. Choć Garmin oficjalnie tych informacji nie potwierdził, przypuszcza się, że firma zapłaciła okup – rzekomo w wysokości ok. 10 mln USD – by uzyskać klucz deszyfrujący i przywrócić normalną pracę systemów (Olenick, 2020).

Analizując studia przypadków, nie sposób pominąć narastającej skali zjawiska rozproszonych ataków typu odmowy usługi (*Distributed Denial of Service*), które stanowią istotny element współczesnego krajobrazu zagrożeń dla sektora finansowego. W warunkach polskich, według danych branżowych i raportów instytucji zajmujących się bezpieczeństwem teleinformatycznym, banki komercyjne oraz instytucje płatnicze odnotowują obecnie nawet kilka tysięcy prób ataków DDoS miesięcznie (Pasławski, 2024). Chociaż zdecydowana większość z nich kończy się niepowodzeniem dzięki stosowanym mechanizmom ochronnym, ich skala, zróżnicowanie wektorów ataku oraz rosnący stopień zaawansowania technicznego wymuszają nieustanny rozwój i optymalizację architektury cyberbezpieczeństwa. Ataki te charakteryzują się dużą zmiennością parametrów – począwszy od wolumetrycznych kampanii generujących ruch rzędu setek gigabitów na sekundę, a skończywszy na atakach aplikacyjnych ukierunkowanych na konkretne funkcjonalności systemów bankowości elektronicznej. Coraz częściej obserwuje się również wykorzystywanie technik hybrydowych, łączących elementy DDoS z innymi wektorami ataku, takimi jak próby włamania czy wstrzykiwanie złośliwego kodu, co dodatkowo komplikuje proces detekcji i przeciwdziałania. Ponadto postęp w obszarze botnetów opartych na urządzeniach IoT oraz możliwość wynajęcia infrastruktury atakującej w modelu *DDoS-as-a-Service* powodują, że bariera wejścia dla potencjalnych sprawców znacznie się obniża. W tym kontekście strategia obrony wymaga podejścia wielowarstwowego, obejmującego zarówno rozwiązania prewencyjne, jak i zaawansowane mechanizmy detekcji w czasie rzeczywistym, wspierane przez sztuczną inteligencję i analizę behawioralną ruchu sieciowego. Kluczowym aspektem jest także adaptacyjność systemów ochronnych, umożliwiająca dynamiczne dostosowanie reguł filtracji i priorytetów ruchu w odpowiedzi na zmieniające się charakterystyki ataku.

Rozwinięciem tematu rozdziału jest prezentacja statystyk realizacji zagrożeń cyberbezpieczeństwa przedstawiona w rozdziale trzecim.

2.3. Cyberpodatności systemu finansowego

Analizując przestrzeń zagrożeń bezpieczeństwa informatycznego, warto także zidentyfikować najważniejsze podatności, które determinują trendy rozwojowe zagrożeń systemów informatycznych w instytucjach finansowych[38], w szczególności zagrożeń, które mają potencjał zakłócania stabilności finansowej. Podatności te będą bowiem w najbliższej przyszłości stanowić tak samo ważny obszar zarządzania instytucjami finansowymi jak obszary *stricte* finansowe.

Jak już wspomniano, pomimo terminologicznej odmienności pojęć zagrożenia i podatności oba pojęcia przenikają się i nierzadko jednoznaczne przypisanie określonego zjawiska do zbioru zagrożeń lub podatności nie jest możliwe. Podrozdział niniejszy jest próbą bliższego spojrzenia na podatności obserwowane w wymiarze systemowym, czyli te, które nie są cechą konkretnego systemu zabezpieczeń, ale raczej pewnym atrybutem wspólnym dla wszystkich współczesnych systemów. Do podatności tego typu należy zaliczyć:

- malejący poziom świadomości informatycznej użytkowników systemów informatycznych,
- otwartość systemów informatycznych wykorzystywanych przez instytucje finansowe (zarówno technologiczną, jak i determinowaną przez regulacje),
- scentralizowany charakter przetwarzania danych w systemach informatycznych instytucji finansowych,
- brak substytucyjności systemów informatycznych.

Cechą wspólną tych podatności jest praktyczna niemożność ich eliminowania. Swego rodzaju paradoksem jest wręcz predykcja ich trendu rozwojowego, zgodnie z którym ich negatywny wpływ będzie coraz większy, pomimo pełnej wiedzy na temat źródeł i determinant ich powstawania.

Świadomość informatyczną społeczeństwa można definiować jako pewien zbiór umiejętności oraz zasobów wiedzy, który pozwala nam świadomie pozyskiwać, przetwarzać oraz wykorzystywać do różnych celów informacje[39]. Świadomość in-

[38] Różnica między zagrożeniem a podatnością jest dyskusyjna. Współczesna informatyka definiuje podatność jako słabość zasobu lub systemu przetwarzania danych. Wydaje się zatem, że jest to pojęcie znacząco różne od pojęcia zagrożenia, jednak analiza konkretnych przykładów zagrożeń i podatności pozwala kwestionować tę odmienność. Na potrzeby niniejszej publikacji przyjęto, że zagrożenie – jako potencjalna przyczyna zdarzeń niekorzystnych z punktu widzenia bezpieczeństwa informatycznego – zawsze jest niepożądane, podczas gdy wiele podatności jest jak najbardziej pożądanych i tworzących wartość dodaną. Przykładem podatności, która jednocześnie generuje zagrożenia, jest np. otwartość systemów informatycznych.

[39] Pojęcie informacji jest pojęciem abstrakcyjnym, trudnym do jednoznacznego zdefiniowania. Próbę jego terminologicznej analizy podjął m.in. Wawrzyniak (2012, s. 36 i n.). Ważnym głosem w dyskusji nad problematyką świadomości informatycznej jest także tekst Marciszewskiego (2011). Jego autor wyróżnia trzy warstwy świadomości informatycznej: poznawczą, aksjologiczną

formatyczna użytkowników systemów informatycznych jest pochodną zarówno procesów edukacyjnych i realizowania obowiązków służbowych, jak i postaw oraz nawyków. Obserwowany obecnie rozwój zastosowań informatyki jest tak dynamiczny, że nie da się już analizować problemu świadomości informatycznej w kontekście jedynie edukacji podstawowej, średniej czy wyższej. Konsekwencją tego zjawiska jest nienadążanie za rozwojem technologicznym, w tym także za zmianami w obszarze bezpieczeństwa informatycznego. Paradoksalnie zatem, ludzie młodzi wcale nie będą lepiej przygotowani do funkcjonowania w środowisku pełnym zagrożeń bezpieczeństwa informatycznego od ludzi starszych. Ta konstatacja – jakkolwiek dyskusyjna – niewątpliwie stanowi o wadze problematyki kreowania właściwych postaw oraz budowania świadomości informatycznej. Jak pokazują badania, problem świadomości informatycznej nie dotyczy jedynie użytkowników końcowych – klientów instytucji finansowych. Równie poważnie należy postrzegać go w kontekście postaw i zachowań pracowników tych instytucji. Szczegółową dyskusję nad tym niezwykle ważnym zagadnieniem przedstawiono w dalszych częściach pracy.

Otwartość systemów informatycznych jest jednym z większych osiągnięć informatyki. Umożliwia bowiem rozszerzanie systemów o nowe funkcje oraz łączenie ich z systemami zewnętrznymi. Innymi słowy, jest to kluczowa cecha współczesnych rozwiązań informatycznych, pozwalająca na dostosowywanie ich do zmieniających się wymagań funkcjonalnych i technicznych. Zalety otwartości są bezdyskusyjne. Dzięki niej stało się możliwe chociażby upowszechnienie bankowości internetowej i mobilnej. Co więcej, otwartość nie jest jedynie atrybutem technicznym, jest to także główny motyw filozofii rozwoju systemu bankowego w Europie. *Open banking* jest niczym innym, jak skierowaniem procesów rozwojowych na styku bankowości i informatyki w stronę nieograniczonych możliwości integracji systemów bankowych z systemami zewnętrznymi. *Open banking* jest w naturalny sposób powiązane z rozwojem sektora fintech. Nie jest to oczywiście zjawisko nowe – istniało praktycznie od początku zastosowań informatyki w działalności finansowej, jednak dynamika jego rozwoju oraz wpływu na system finansowy zdecydowanie nasiliła się w ostatnich latach. Próby klasyfikacji działalności podmiotów z grupy fintech ukierunkowane są na identyfikację ich funkcji w systemie finansowym. Najczęściej stosowany podział wyróżnia takie segmenty, jak:

- płatności i infrastruktura płatnicza,
- działalność operacyjna i zarządzanie ryzykiem,
- bezpieczeństwo i monetyzacja danych,
- komunikacja z klientami,
- ekonomia współdzielenia.

---

oraz prakseologiczną, podkreślając jednak, że znaczenie tej pierwszej, związanej z wiedzą na temat pozyskiwania, przechowywania, przekazywania, przetwarzania i pomiaru informacji, a także jej zastosowań jest zdecydowanie największe.

Tak szeroki merytorycznie zakres obszarów, w których funkcjonuje dzisiaj fintech, integrując się z mechanizmami systemu finansowego, generuje niespotykany dotąd poziom ryzyka informatycznego o potencjale systemowym. Wprawdzie fintech tworzy w wielu przypadkach wartość dodaną, zarówno dla instytucji finansowych, jak i dla ich klientów, ale wpływ tego zjawiska na stabilność finansową nie jest jednoznaczny. Uzasadnione jest bowiem wykazywanie wpływu zarówno pozytywnego, jak i negatywnego. Według Financial Stability Board do najważniejszych korzyści wynikających z rozwoju fintech należy zaliczyć:

- decentralizację rynku i dywersyfikację usług,
- pojawienie się produktów i usług komplementarnych do już istniejących,
- wymuszenie większej konkurencyjności instytucji finansowych,
- obniżenie kosztów dla użytkownika końcowego.

Pozytywnym aspektom rozwoju omawianego zjawiska przeciwstawia się jednak nowe zagrożenia, których katalizatorem są spółki fintech oraz tworzone przez nie rozwiązania. Na plan pierwszy wysuwa się kwestia zwiększonego poziomu ryzyka informatycznego w systemie finansowym (FSB, 2019).

Istotną podatnością pozostaje także scentralizowany charakter przetwarzania danych w systemach informatycznych instytucji finansowych. Skupienie kluczowych funkcji przetwarzania, przechowywania i zarządzania danymi w ograniczonej liczbie węzłów infrastruktury zwiększa ryzyko pojedynczego punktu awarii oraz ułatwia potencjalnym atakującym przeprowadzenie skoordynowanego cyberataku o dużym zasięgu. Centralizacja danych sprzyja również powstawaniu tzw. *data silos*, które mogą ograniczać możliwości szybkiego reagowania na incydenty bezpieczeństwa i utrudniać ich wykrywanie. W przypadku udanego przełamania zabezpieczeń systemu centralnego atakujący zyskuje dostęp do szerokiego spektrum wrażliwych informacji, co może prowadzić do poważnych strat finansowych i utraty zaufania klientów. W perspektywie rozwoju architektur systemów finansowych coraz większe znaczenie będą mieć dystrybucja i segmentacja danych, które mogą ograniczyć skutki potencjalnych kompromitacji infrastruktury centralnej.

Brak substytucyjności systemów informatycznych jest rozumiany jako ograniczona możliwość szybkiego zastąpienia krytycznych komponentów infrastruktury w przypadku ich awarii lub kompromitacji. Uzależnienie od określonych, często monolitycznych rozwiązań technologicznych powoduje, że przerwa w działaniu jednego kluczowego systemu może prowadzić do paraliżu całego łańcucha procesów biznesowych. Brak substytucyjnych mechanizmów awaryjnych ogranicza natomiast elastyczność reagowania na incydenty bezpieczeństwa i utrudnia odtworzenie ciągłości działania w sytuacjach kryzysowych. W dłuższej perspektywie zwiększa to podatność systemu finansowego na eskalację zagrożeń oraz wpływa negatywnie na jego odporność i stabilność.

2.4. Transmisyjność zagrożeń cyberbezpieczeństwa

Historia globalnego systemu finansowego nie zna jeszcze przypadku kryzysu bezpośrednio wywołanego przez technologię. Jednocześnie liczba incydentów bezpieczeństwa w systemach instytucji finansowych na całym świecie jest ogromna i stale się zwiększa. Cyberataki na podmioty gospodarcze stają się coraz częstsze. Szacuje się, że bezpośredni koszt takich ataków dla gospodarki globalnej zbliża się do 10 bln USD rocznie i w najbliższych latach może istotnie wzrosnąć[40]. O wielu poważnych naruszeniach bezpieczeństwa informatycznego dowiadujemy się z raportów branżowych, jednak należy przyjąć, że jest to jedynie wierzchołek góry lodowej. Najprawdopodobniej ponad 90% incydentów bezpieczeństwa, szczególnie w systemach finansowych, nie jest przedmiotem ogólnodostępnych statystyk. Ryzyko informatyczne jest postrzegane przez ekspertów jako jedno z pięciu najważniejszych rodzajów ryzyka, które należy brać pod uwagę, zarządzając biznesem[41]. Jest wielce prawdopodobne, że tylko kwestią czasu jest przenoszenie się lokalnych zakłóceń na cały system finansowy. Ten punkt widzenia nakazuje więc identyfikować pomijany do tej pory aspekt transmisyjności problemów cyberbezpieczeństwa na stabilność obszaru systemu finansowego, którego te problemy dotyczą. W tym przypadku transmisyjność należy rozumieć jako potencjał powstawania kryzysów finansowych, których bezpośrednią przyczyną są problemy natury technologicznej.

Na problematykę zagrożeń bezpieczeństwa informatycznego współczesnego systemu finansowego należy patrzeć przez pryzmat co najmniej trzech perspektyw:

- perspektywy cyberbezpieczeństwa operacji wykonywanych przez użytkowników końcowych – klientów instytucji finansowych,
- perspektywy cyberbezpieczeństwa systemów informatycznych instytucji tworzących system finansowy,
- perspektywy cyberbezpieczeństwa interfejsów komunikacyjnych.

Pochodną identyfikacji tych perspektyw jest możliwość określenia kanałów transmisyjnych, których zakłócenia bezpieczeństwa informatycznego mogą wpływać na stabilność systemu bankowego. Źródłami istnienia tych kanałów będą zatem:

- niewłaściwe zachowania (postawy) klientów instytucji finansowych wykonujących operacje w systemach bankowości internetowej i mobilnej,

---

[40] Według raportu IBM *Cost of a Breach Data Report 2024* średni koszt pojedynczego naruszenia danych w sektorze finansowym na świecie wynosi obecnie 4,88 mln USD (IBM, 2024). Globalny koszt wszystkich form cyberprzestępczości osiągnął w 2024 r. wartość 9,5 bln USD (Experis, 2025).

[41] Według badania przeprowadzonego przez DTCC *cyberrisk* został wymieniony jako najpoważniejsze ryzyko w 2020 r. przez 22% respondentów, a aż 69% z nich umieściło to ryzyko w grupie pięciu najpoważniejszych. Warto jednak zauważyć, że wśród ryzyk opisanych w badaniu nie znalazło się ryzyko wystąpienia światowej pandemii (DTCC, 2019).

- niewłaściwe zachowania (postawy) użytkowników systemów informatycznych instytucji finansowych,
- ataki cybernetyczne na systemy informatyczne instytucji uczestniczących w systemie finansowym,
- zakłócenia ciągłości funkcjonowania interfejsów komunikacyjnych.

Można tym samym stwierdzić, że istnieją cztery podstawowe kanały transmisji zagrożeń cyberbezpieczeństwa na stabilność systemu bankowego:

- kanał użytkownika końcowego,
- kanał użytkownika wewnętrznego,
- kanał instytucjonalny,
- kanał telekomunikacyjny.

Kanał telekomunikacyjny jest związany z podstawą funkcjonowania globalnego systemu finansowego, jakim są globalne sieci komunikacyjne: Internet i sieć GSM. Obserwowane w ostatnich latach zmiany modeli biznesowych banków i innych instytucji determinowane są głównie czynnikami technologicznymi (Klimontowicz, 2020). Globalna sieć informatyczna stała się immanentną częścią systemu finansowego, w wielu obszarach będąc elementem o znaczeniu krytycznym. Bogata literatura przedmiotu, związana z problematyką bezpieczeństwa w sieci, dostrzega znaczenie tego bezpieczeństwa dla funkcjonowania globalnego systemu finansowego. Co ciekawe, jest to jeden z dwóch kanałów, którego atrybuty nie zależą w żadnym stopniu od uczestników systemu finansowego. Zagrożenia komunikacji internetowej stały się po prostu częścią zbioru zagrożeń systemów rozliczeniowych oraz transakcyjnych. Potencjał systemowy kanału telekomunikacyjnego jest olbrzymi. Globalna sieć komputerowa stanowi bowiem fundament funkcjonowania światowego systemu finansowego. Paradoksalnie ten system połączeń pomiędzy komputerami tworzy trwały fundament, mimo że nie jest niczyją własnością i nie jest centralnie zarządzany. Zakłócenie funkcjonowania sieci jest zagrożeniem o charakterze katastroficznym.

Oba kanały związane z działalnością legalnych użytkowników systemów informatycznych są trudne do jednoznacznej oceny. Trudność ta wynika z daleko posuniętego relatywizmu, z jakim podchodzi się do zagadnienia świadomości informatycznej użytkowników systemów informatycznych. Teoretycznie rzecz biorąc, poprawne – w sensie bezpieczeństwa – postawy świadomych i wyszkolonych użytkowników powinny eliminować zagrożenia, głównie phishingowe, w stu procentach. Nie jest to jednak zjawisko obserwowane w praktyce. Innymi słowy, to właśnie działalność użytkowników jest najpoważniejszym czynnikiem determinującym istnienie ryzyka informatycznego. Nie ma nic odkrywczego w tym stwierdzeniu, jednak wydaje się, że wątek behawioralny ciągle nie jest traktowany z należytą powagą. Wartym zauważenia elementem szeroko rozumianego ryzyka informatycznego w systemie bankowym, o stosunkowo dużym znaczeniu dla problematyki stabilności finansowej, jest także

perspektywa użytkownika końcowego, rozumiana jako poziom zaufania użytkowników systemów bankowości internetowej i mobilnej do oferowanych przez instytucje finansowe rozwiązań informatycznych. Jest to dość złożone zjawisko, rzadko będące przedmiotem badań naukowych[42]. Co ciekawe, nieczęsto zjawisko to jest kojarzone z reputacją banków, podczas gdy to właśnie ono powinno współcześnie o tej reputacji decydować. Masowa utrata zaufania do bankowości internetowej jest oczywiście trudno wyobrażalna, gdyż bez elektronicznego kanału dystrybucji usług bankowych gospodarka przestałaby funkcjonować, lecz warto pamiętać, że podobne założenia, takie jak *too big to fail* czy *too important to fail*, były akceptowane przez świat finansów jeszcze kilkanaście lat temu. Dziś nikt już o nich nie wspomina.

W kontekście rozważań nad kanałem użytkownika końcowego warto także wspomnieć o punkcie widzenia analogicznym do perspektywy depozytariusza banku komercyjnego. Podobnie jak w przypadku systemu gwarantowania depozytów, którego głównym zadaniem jest kreowanie przeświadczenia depozytariuszy o bezpieczeństwie ich depozytów, system finansowy, zwłaszcza bankowy, stara się zapewnić odpowiedni poziom przeświadczenia o bezpieczeństwie stosowanych w nim rozwiązań informatycznych. Nie istnieje wprawdzie dedykowana temu celowi instytucja, jednak można stwierdzić, że ogół przekazu medialnego generowanego przez system bankowy ma na celu informowanie o zagrożeniach z jednej strony, lecz także unikanie informowania o incydentach z drugiej[43].

Źródłami istnienia kanałów transmisyjnych są wszelkie zagrożenia bezpieczeństwa informatycznego występujące w systemie finansowym, niemniej istotne wydają się różnice pomiędzy atrybutami tych kanałów oraz ich negatywnym – z punktu widzenia stabilności finansowej – potencjałem. Każdy z kanałów transmisyjnych można opisać zestawem następujących atrybutów:

- potencjału systemowego, rozumianego jako zdolność do przekształcenia incydentów bezpieczeństwa w masowe zjawisko zagrażające funkcjonowaniu instytucji sektora bankowego,
- transparentności, rozumianej jako wysoki poziom zrozumienia mechanizmów odpowiadających za powstawanie incydentów bezpieczeństwa, czyli za realizację zagrożeń,

---

[42] Jednym z niewielu aktualnych badań na ten temat jest badanie reputacji sektora bankowego w Polsce przeprowadzone w 2019 r. Znamienne jest, że wśród kilkunastu pytań ankietowych tylko jedno dotyczyło bezpieczeństwa bankowości elektronicznej (Idzik i Gieorgica, 2019).

[43] To zjawisko można oceniać dwojako. Jego źródłem są dwa elementy: indywidualny, przejawiający się troską o wizerunek instytucji bankowych, oraz systemowy – ukierunkowany na unikanie elektronicznej wersji *bank run*. Dualizm ewaluacyjny w tym wypadku przejawia się w zestawieniu krytycznego spojrzenia na fakt niepełnej transparentności systemu bankowego z obiektywnym stwierdzeniem, zgodnie z którym celem nadrzędnym jest unikanie masowych, negatywnych reakcji końcowych użytkowników systemu.

- szybkości transmisji, rozumianej jako stosunkowo krótki czas potrzebny na przekształcenie się incydentów bezpieczeństwa w masowe zjawisko zagrażające funkcjonowaniu instytucji sektora bankowego,
- podatności na wpływ innowacji technologicznych, rozumianej jako słabość związana z bardzo dużym wpływem rozwoju technologii na dany kanał,
- podatności na wpływ czynnika ludzkiego, rozumianej jako słabość związana z bardzo dużym wpływem postaw użytkowników systemów informatycznych na dany kanał.

Tabela 3. Potencjał systemowy wybranych zagrożeń bezpieczeństwa informatycznego

Zagrożenie	**Cel ataku**	**Potencjalne negatywne skutki**	**Wymagany poziom zaawansowania atakującego / współistnienie z innymi zagrożeniami**	**Możliwości przeciwdziałania**	**Potencjał systemowy**
Phishing	nieokreślony; udany atak phishingowy może być przygotowaniem do osiągnięcia dowolnego celu, związanego z dowolnym z atrybutów bezpieczeństwa	nieograniczone, niemożliwe do oszacowania	bardzo niski; zagrożenia współistniejące: praktycznie wszystkie związane z wykorzystywaniem szkodliwego oprogramowania	średnie, związane głównie z działaniami organizacyjnymi ukierunkowanymi na kreowanie właściwych postaw użytkowników systemów informatycznych	wysoki – wynikający z nieznanego celu (skutku) udanego ataku
Distributed Denial of Service	zablokowanie dostępu do systemów informatycznych	bardzo duże, głównie w obszarze wizerunkowym	bardzo niski; brak współistniejących zagrożeń	wysokie poprzez stosowanie zaawansowanych narzędzi anty-DDoS	wysoki – wynikający z nieprzewidywalnych reakcji klientów banków na brak dostępu do systemów, głównie bankowości internetowej i mobilnej oraz systemów rozliczeniowych
APT	nieokreślony; udany atak typu APT może być przygotowaniem do osiągnięcia dowolnego celu, związanego z dowolnym z atrybutów bezpieczeństwa	nieograniczone, niemożliwe do oszacowania	bardzo niski; zagrożenia współistniejące: praktycznie wszystkie związane z wykorzystywaniem szkodliwego oprogramowania	bardzo niskie w kontekście otwartości współczesnych systemów oraz podatności czynnika ludzkiego	bardzo wysoki – wynikający z nieznanego celu (skutku) udanego ataku

Źródło: opracowanie własne.

Dokładna charakterystyka wymienionych atrybutów nie jest trywialna. Na przykład potencjał systemowy[44] scharakteryzowanych zagrożeń jest bardzo wysoki, niemniej występują pomiędzy nimi pewne różnice. W tabeli 3 przedstawiono próbę zestawienia niektórych z nich[45].

Globalny system finansowy i technologię informatyczną cechuje wieloaspektowa, symbiotyczna relacja. Dynamiczny rozwój technologii determinuje od wielu lat nie tylko rozwój produktów i usług finansowych, lecz także zmiany paradygmatów funkcjonowania banków i innych instytucji. Jednocześnie potrzeby systemu finansowego wielokrotnie były katalizatorami innowacji technologicznych. Dzisiaj tę relację często wiąże się z dyskutowanym już zjawiskiem fintech.

Rewolucja informatyczna wprowadziła do systemu finansowego nowe cechy usług finansowych, atrakcyjne zarówno dla kupujących, jak i dla sprzedających. Wraz z tymi cechami pojawiły się także efekty uboczne w postaci niespotykanych wcześniej zagrożeń bezpieczeństwa transakcji finansowych. Dziś można mówić wręcz o uzależnieniu się globalnego systemu finansowego od technologii. Uzależnienie to ma wymiar nie tylko *stricte* techniczny, lecz także organizacyjny i społeczny. Co więcej, dynamika rozwoju technologii informatycznych oraz rosnący poziom globalnego ryzyka informatycznego w największym stopniu wpływają właśnie na sektor finansowy, gdyż to on od zawsze był najatrakcyjniejszym celem działań cyberprzestępców. Współcześnie wyróżnia się wiele kategorii motywów, którymi kierują się cyberprzestępcy. Najważniejsze z nich to:

- cyberprzestępstwo (*cyber-crime*) – ukierunkowane głównie na uzyskanie korzyści finansowej,
- szpiegostwo komputerowe (*cyber espionage*) – związane z pozyskiwaniem informacji, m.in. w celach gospodarczych, wojskowych lub politycznych),
- wojna w cyberprzestrzeni (*cyber war*) – związana z zaangażowaniem struktur państwowych przeciwko innemu krajowi[46].

---

[44] Rozumiany jako potencjał przeniesienia negatywnych skutków realizacji zagrożeń bezpieczeństwa na funkcjonowanie całej instytucji, a w konsekwencji systemu finansowego.

[45] Tabele 3 i 4 przedstawiają jedynie wybrane zagrożenia i wybrane podatności. Nie stanowią kompleksowego ujęcia problemu, wskazują jednak te elementy, których znaczenie dla tematyki rozdziału jest kluczowe i są próbą uogólnienia omawianego zjawiska.

[46] *Cyber wars* to problem, który najprawdopodobniej już niedługo zdominuje dyskusje na temat cyberbezpieczeństwa. Jest to współczesny wymiar konfliktu zbrojnego i geopolitycznego, w którym państwa (także organizacje) wykorzystują zasoby cyfrowe do prowadzenia działań ofensywnych, destabilizacyjnych i wywiadowczych. Kluczowym komponentem współczesnych cyberwojen są operacje dezinformacyjne (*disinformation operations*), które mają na celu manipulowanie opinią publiczną, podważanie zaufania społecznego oraz destabilizację instytucji demokratycznych. Kampanie te często wykorzystują media społecznościowe, fałszywe konta oraz generowane przez AI treści (*deepfake*, *synthetic media*) jako narzędzie wpływu. Równolegle prowadzone są tzw. operacje wpływu (*influence operations*), których celem jest oddziaływanie na procesy decyzyjne w państwach przeciwnych, np. przez ingerencję w wybory czy wzniecanie napięć społecznych. Na poziomie technologicznym cyberwojny obejmują również użycie

Tabela 4 przedstawia motywacje i cele różnych kategorii cyberprzestępców.

Tabela 4. Motywacje i cele różnych kategorii cyberprzestępców

Kategoria	Motywacje	Cele	Przykładowe efekty działań
Struktury państwowe	geopolityka, ideologia	zakłócenie funkcjonowania systemu, fizyczne niszczenie, kradzież, szpiegostwo, korzyść finansowa	usunięcie danych, niszczenie sprzętu komputerowego, zakłócenia w zasilaniu, szpiegostwo, pranie brudnych pieniędzy
Cyberprzestępcy	wzbogacenie się	kradzież, korzyść finansowa	kradzież wartości, pranie brudnych pieniędzy, wymuszenia okupu
Terroryści, organizacje wykorzystujące haktywizm, sabotażyści	ideologia, niezadowolenie, żart, chęć zdobycia rozgłosu	zakłócenie funkcjonowania systemu/instytucji	wycieki danych, ataki DDoS, dezinformacja

Źródło: opracowanie własne.

Cele, o których mówi zestawienie w tabeli 4, osiągane są przede wszystkim z wykorzystaniem opisanych uprzednio narzędzi, takich jak *ransomware*, *phishing*, DDoS, ataki na centra *cloud computing* (CheckPoint, 2025). Zakłócenia stabilności finansowej będące następstwem cyberprzestępczości mogą mieć konsekwencje, które trudno obecnie przewidzieć. Wśród najczęściej wymienianych jako najpoważniejsze wskazuje się (Office of Financial Research, 2017):

- paraliż systemów bankowych związany z brakiem substytucyjności kluczowych elementów systemu bankowego, takich jak banki centralne czy instytucje rozliczeniowe,
- utratę zaufania do systemu w ujęciu lokalnym lub globalnym,
- utratę integralności danych przetwarzanych w systemie bankowym.

Te trzy cechy determinują konieczność postrzegania omawianej problematyki także z punktu widzenia ryzyka systemowego. W każdym bowiem z powyższych przypadków istnieje scenariusz prowadzący do realizacji ryzyka systemowego poprzez uprzednio opisane mechanizmy transmisyjne. Instytucje systemu bankowego oraz

destrukcyjnego oprogramowania złośliwego (*destructive malware*), które ma za zadanie fizycznie zniszczyć dane i uniemożliwić działanie systemów krytycznych. W przeciwieństwie do *ransomware* celem tych ataków jest nie zysk, lecz wywołanie paraliżu instytucjonalnego. Ostatnią ważną kategorią są działania określane jako przygotowanie zakłóceń (*disruption preparation*) polegające na długoterminowym rozpoznaniu infrastruktury krytycznej przeciwnika, zainstalowaniu backdoorów i pozostawieniu „cyfrowych ładunków" gotowych do aktywacji w momencie eskalacji konfliktu.

jego infrastruktura są szczególnie wrażliwe na zakłócenia powodowane realizacjami zagrożeń bezpieczeństwa informatycznego. Ta specyficzna dla systemu finansowego wrażliwość źródła ma przede wszystkim w (Narodowy Bank Polski, 2019, s. 124 i n.):

- ryzyku reputacyjnym, uwarunkowanym zaufaniem społecznym do instytucji i ich środowiska informatycznego,
- wysokim stopniu uzależnienia od poufności, integralności, autentyczności i dostępności informacji i systemów, a także niezawodności tych systemów i niezaprzeczalności transakcji,
- otwartości systemów wykorzystywanych przez instytucje finansowe,
- wysokim poziomie centralizacji systemu rozliczeniowego.

Uwarunkowania te nie są jedynie źródłami specyfiki zastosowań informatyki w systemie finansowym, lecz przede wszystkim determinują sposób postrzegania ryzyka operacyjnego i ryzyka reputacyjnego we współczesnych finansach. Reputacja jest bowiem nieprzypadkowo traktowana jako samodzielny problem, wykraczający nawet poza bardzo szerokie ramy ryzyka operacyjnego.

Wysoki stopień uzależnienia od atrybutów bezpieczeństwa jest kluczowym czynnikiem warunkującym niezakłócone funkcjonowanie instytucji finansowej, szczególnie w warunkach braku możliwości pełnego odizolowania systemów instytucji od sieci globalnej. Centralizacja natomiast, przejawiająca się m.in. istnieniem centralnych, międzybankowych systemów rozliczeniowych, tworzy nad obszarem zastosowań informatyki w finansach permanentny parasol niepewności związanej ze świadomością oparcia ciągłości funkcjonowania systemu na jednej instytucji. Wszystkie te elementy składają się na aktualny, niezbyt pozytywny obraz poziomu ryzyka informatycznego w działalności instytucji finansowych, który często jest charakteryzowany wręcz dramatycznie brzmiącymi porównaniami. Jedno z nich mówi, że technologia informatyczna w finansach oferuje swego rodzaju „pakt z diabłem" (*Faustian bargain*), udostępniając nieograniczone możliwości rozwoju, konkurencyjności i efektywności w zamian za permanentnie rosnący i ciągle wymykający się spod pełnej kontroli poziom ryzyka, graniczącego wręcz z permanentną niepewnością (Angelbeck, 2014). Te poetyckie nieco sformułowania nie są bynajmniej pozbawione podstaw merytorycznych. Współistnienie rozwoju technologii oraz odpowiadającego mu wzrostu poziomu ryzyka jest immanentną cechą współczesnego systemu finansowego. Stabilność finansowa jest więc nierozerwalnie związana z problematyką bezpieczeństwa systemów informatycznych instytucji tworzących ten system.

2.5. Środki ochrony

Współczesnym zagrożeniom cybernetycznym przeciwdziałają złożone mechanizmy ochronne, określane zbiorczo mianem środków bezpieczeństwa lub środków ochrony. W ujęciu tradycyjnym dzieli się je najczęściej według kryterium funkcjonalnego na:

- środki prawne – regulacje i akty normatywne kształtujące ramy prawne ochrony informacji, np. przepisy RODO, DORA, PSD2, ustawy o krajowym systemie cyberbezpieczeństwa,
- środki organizacyjne – polityki, procedury, systemy zarządzania bezpieczeństwem informacji, audyty i kontrole zgodności z regulacjami,
- środki techniczne – sprzętowe i programowe rozwiązania ochronne, takie jak zapory sieciowe, systemy IDS/IPS, mechanizmy szyfrowania czy wieloskładnikowe uwierzytelnianie,
- środki edukacyjne i prewencyjne – działania podnoszące świadomość pracowników i użytkowników, obejmujące m.in. szkolenia, kampanie informacyjne czy testy socjotechniczne.

Choć podział ten ma ugruntowaną pozycję w literaturze (Białas, 2006), jego ograniczeniem jest liniowe traktowanie komponentów, podczas gdy w praktyce bezpieczeństwo teleinformatyczne wymaga zintegrowanego i procesowego podejścia. Współczesne strategie cyberbezpieczeństwa, rekomendowane m.in. przez *Cybersecurity Framework*… (NIST, 2024) czy *Cybersecurity Culture Guidelines*… (ENISA, 2018), akcentują cykliczność działań ochronnych oraz ich powiązanie z fazami zarządzania ryzykiem i reagowania na incydenty. W tym kontekście zasadne jest wprowadzenie klasyfikacji środków ochrony ukierunkowanej na strategie cyberbezpieczeństwa, która lepiej odzwierciedla dynamikę zagrożeń i rolę poszczególnych komponentów w procesie budowania odporności systemów. NIST (2024) wyróżnia następujące kategorie:

- środki prewencyjne (*preventive controls*) – mające na celu minimalizację prawdopodobieństwa wystąpienia incydentu i obejmujące m.in. zastosowania kryptografii, kontrolę dostępu, konfigurację systemów, aktualizacje oprogramowania oraz programy szkoleniowe z zakresu świadomości bezpieczeństwa,
- środki detekcyjne (*detective controls*) – służące wczesnemu wykrywaniu anomalii, prób włamania lub naruszeń. Zaliczają się do nich systemy monitorowania bezpieczeństwa, mechanizmy analizy behawioralnej, systemy IDS, a także platformy *threat intelligence*,
- środki reakcyjne (*responsive controls*) – uruchamiane w momencie wykrycia incydentu w celu ograniczenia jego skutków, np. automatyczne izolowanie zainfekowanych segmentów sieci, systemy SOAR, plany reagowania na incydenty (IRP) oraz procedury zarządzania kryzysowego,
- środki odtworzeniowe (*recovery controls*) – skoncentrowane na przywróceniu pełnej funkcjonalności systemów po incydencie, w tym mechanizmy tworzenia i odtwarzania kopii zapasowych (*backup*/*restore*), usługi DRaaS (*Disaster Recovery as a Service*) oraz procedury zachowania ciągłości działania,
- środki adaptacyjne (*adaptive controls*) – oparte na analizie doświadczeń z przeszłych incydentów i uczeniu się organizacji, obejmujące aktualizację procedur, integrację nowych technologii ochronnych (np. AI do predykcji zagrożeń) oraz dostosowanie architektury bezpieczeństwa do zmieniającego się otoczenia.

Tak ujęta klasyfikacja pozwala traktować bezpieczeństwo nie jako zbiór statycznych narzędzi, lecz jako proces cykliczny, w którym środki techniczne, organizacyjne, prawne i edukacyjne są spójnie zintegrowane i przypisane do konkretnych funkcji w strategii cyberbezpieczeństwa. Podejście to ułatwia również ocenę dojrzałości organizacji w obszarze bezpieczeństwa oraz zapewnia lepsze dopasowanie środków ochrony do charakteru i profilu ryzyka instytucji finansowej. Szczegółowe omówienie wymienionych kategorii wykraczałoby poza ramy publikacji. Tabele 5-9 przedstawiają ogólne ujęcie systematyki współczesnych środków ochrony w kontekście ich zastosowań w sektorze finansowym.

Tabela 5. Prewencyjne środki ochrony

Kategoria	Zastosowanie w systemach instytucji finansowych
Mechanizmy zarządzania dostępem i tożsamością	ochrona dostępu do systemów, uwierzytelnianie pracowników i użytkowników bankowości internetowej i mobilnej, zarządzanie kontami uprzywilejowanymi w środowiskach krytycznych, interfejsy do systemów zewnętrznych
Narzędzia ochrony sieci i infrastruktury	zapobieganie nieautoryzowanemu dostępowi do zasobów, filtrowanie ruchu sieciowego, segmentacja sieci w centrach przetwarzania danych, bezpieczny dostęp zdalny dla pracowników i użytkowników bankowości internetowej i mobilnej, zapory sieciowe, systemy antywirusowe
Procedury twardej konfiguracji i zarządzania podatnościami	regularne łatanie podatności w systemach transakcyjnych, automatyzacja aktualizacji oprogramowania
Narzędzia ochrony punktów końcowych i urządzeń mobilnych	ochrona terminali kasjerskich, komputerów pracowników i urządzeń mobilnych z dostępem do systemów instytucji finansowych, zarządzanie bezpieczeństwem BYOD[(a)]
Protokoły i algorytmy kryptograficzne	szyfrowanie baz danych, szyfrowanie komunikacji wewnętrznej i zewnętrznej, zarządzanie hasłami, podpisy cyfrowe, sieci *blockchain*, wirtualne sieci prywatne
Narzędzia ochrony aplikacji i usług	ochrona aplikacji bankowości internetowej i mobilnej, zabezpieczenie API używanych do integracji z fintechami, testy penetracyjne aplikacji finansowych
Narzędzia ochrony poczty i komunikacji	ochrona przed phishingiem ukierunkowanym na klientów i pracowników, filtrowanie złośliwych załączników i linków
Procesy edukacyjne ukierunkowane na zwiększenie świadomości informatycznej	szkolenia wewnętrzne, testy reakcji pracowników na ataki symulowane, zwiększanie świadomości klientów w zakresie bezpiecznego korzystania z bankowości online
Narzędzia prewencji opartej na AI i analizie behawioralnej	wykrywanie anomalii w ruchu sieciowym, identyfikacja nietypowych działań użytkowników mogących wskazywać na przejęcie konta, predykcja zagrożeń na podstawie wzorców historycznych

[(a)] *Bring Your Own Device* – polityka, która pozwala pracownikom na używanie własnych urządzeń (takich jak laptopy, smartfony, tablety) do celów służbowych w pracy.

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Tabela 6. Detekcyjne środki ochrony

Kategoria	Zastosowanie w systemach instytucji finansowych
Systemy monitorowania bezpieczeństwa	centralizacja logów z systemów i serwerów aplikacyjnych; korelacja zdarzeń w celu identyfikacji prób ataku; generowanie alertów bezpieczeństwa
Systemy wykrywania włamań (IDS) i zapobiegania włamaniom (IPS)	analiza ruchu sieciowego pod kątem znanych sygnatur ataków i nietypowych wzorców, blokowanie podejrzanych połączeń w czasie rzeczywistym
Systemy analizy behawioralnej	wykrywanie nietypowych działań pracowników lub użytkowników bankowości internetowej i mobilnej, identyfikacja możliwych przejęć kont
Systemy monitorowania integralności plików	wykrywanie nieautoryzowanych zmian w plikach systemowych, aplikacjach lub konfiguracjach krytycznych dla działania instytucji
Platformy *Threat Intelligence*	zbieranie i analiza informacji o nowych zagrożeniach zewnętrznych, integracja danych o atakach z systemami obrony instytucji
Systemy monitorowania transakcji w czasie rzeczywistym	analiza operacji finansowych pod kątem wzorców oszustw, automatyczne oznaczanie podejrzanych transakcji w systemach bankowych
Systemy wykrywania *malware* w czasie rzeczywistym	skany pamięci i plików wykonywane w sposób ciągły, detekcja złośliwego oprogramowania w załącznikach poczty i pobieranych plikach
Systemy monitorowania bezpieczeństwa chmury	analiza konfiguracji usług chmurowych pod kątem błędów i luk, wykrywanie nieautoryzowanych zmian w środowiskach chmurowych

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Tabela 7. Reakcyjne środki ochrony

Kategoria	Zastosowanie w systemach instytucji finansowych
Plany reagowania na incydenty (IRP)	określenie procedur postępowania w przypadku wykrycia incydentu, koordynacja działań zespołów
Automatyczne systemy reakcji (SOAR)	orkiestracja i automatyzacja działań naprawczych, takich jak blokowanie kont, izolacja urządzeń czy aktualizacja reguł *firewall*
Izolacja segmentów sieci	natychmiastowe odcięcie zainfekowanej części infrastruktury od reszty sieci w celu ograniczenia rozprzestrzeniania się ataku
Zarządzanie komunikacją kryzysową	informowanie interesariuszy, klientów i regulatorów o incydencie w sposób zgodny z wymogami prawnymi i minimalizujący szkody reputacyjne
Dynamiczne modyfikowanie polityk bezpieczeństwa	aktualizacja reguł dostępu, reguł *firewall* i filtrów w odpowiedzi na wykryty wektor ataku

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Tabela 8. Odtworzeniowe środki ochrony

Kategoria	Zastosowanie w systemach instytucji finansowych
Systemy tworzenia i odtwarzania kopii zapasowych (*backup/restore*)	regularne tworzenie kopii zapasowych krytycznych danych i systemów, szybkie przywracanie po incydencie lub awarii
Usługi *Disaster Recovery as a Service* (DRaaS)	odtwarzanie środowisk informatycznych w infrastrukturze chmurowej dostawcy po awarii lub ataku *ransomware*
Plany ciągłości działania	zapewnienie ciągłości kluczowych procesów biznesowych podczas i po incydencie, minimalizacja przestojów
Replikacja danych w czasie rzeczywistym	synchronizacja danych pomiędzy ośrodkami zapasowymi w celu skrócenia czasu odtworzenia i minimalizacji utraty danych
Infrastruktura zapasowa	przygotowane lokalizacje lub środowiska gotowe do przejęcia operacji w przypadku awarii głównego centrum danych
Automatyzacja procesów odtworzeniowych	skrócenie czasu przywracania usług poprzez skrypty i narzędzia do automatycznego rekonfigurowania środowisk

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Tabela 9. Adaptacyjne środki ochrony

Kategoria	Zastosowanie w systemach instytucji finansowych
Aktualizacja procedur bezpieczeństwa	wprowadzanie zmian w politykach i procedurach na podstawie doświadczeń z incydentów oraz nowych wymagań regulacyjnych
Uczenie się na incydentach	analiza zdarzeń po ich wystąpieniu w celu identyfikacji luk w zabezpieczeniach i procesach oraz opracowanie działań naprawczych
Integracja nowych technologii ochronnych	wdrażanie innowacyjnych narzędzi, takich jak systemy oparte na sztucznej inteligencji do predykcji zagrożeń lub *blockchain* do zabezpieczania transakcji
Dostosowanie architektury bezpieczeństwa	modyfikacja topologii sieci, segmentacji i konfiguracji systemów w odpowiedzi na zmieniające się wektory ataku
Ciągła analiza ryzyka	dynamiczne dostosowywanie profilu ryzyka organizacji poprzez bieżące monitorowanie otoczenia i analizę trendów cyberzagrożeń

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Analiza środków i narzędzi cyberbezpieczeństwa w sektorze finansowym jednoznacznie wskazuje, że skuteczna ochrona teleinformatyczna wymaga wielowarstwowego i zintegrowanego podejścia, w którym rozwiązania prewencyjne, detekcyjne, reakcyjne, odtworzeniowe i adaptacyjne tworzą spójny ekosystem bezpieczeństwa. Poszczególne kategorie nie są jednak od siebie całkowicie odseparowane – wiele narzędzi pełni swoje funkcje w więcej niż jednej grupie, w zależności od kontekstu wdrożenia i konfiguracji. Przykładowo, nowoczesne platformy klasy EDR/XDR mogą

równocześnie pełnić funkcję środka detekcyjnego (monitorowanie i wykrywanie incydentów), reakcyjnego (izolowanie zainfekowanych urządzeń) oraz adaptacyjnego (uczenie się na podstawie wcześniejszych zdarzeń i aktualizacja reguł bezpieczeństwa). Podobnie systemy klasy SIEM (*Security Information and Event Management*) mogą jednocześnie realizować funkcje detekcji, reakcji oraz wspierać procesy adaptacyjne. Z uwagi na dynamiczny rozwój technologii, zmieniający się krajobraz zagrożeń oraz rosnącą dostępność rozwiązań bezpieczeństwa liczba dostępnych narzędzi i usług jest bardzo duża i stale się zwiększa. Obecnie rynek oferuje zarówno kompleksowe platformy bezpieczeństwa obejmujące wiele obszarów ochrony, jak i wysoko wyspecjalizowane narzędzia dedykowane konkretnym zadaniom, takim jak ochrona aplikacji mobilnych, analiza ruchu w chmurze czy weryfikacja tożsamości użytkowników. Wymienienie wszystkich dostępnych produktów, wraz z ich szczegółowymi parametrami, przekroczyłoby ramy niniejszej monografii i wymagałoby odrębnego opracowania o charakterze przeglądowym. Należy także podkreślić, że skuteczność wdrożonych środków ochrony nie zależy wyłącznie od wyboru odpowiedniej technologii, lecz od właściwej integracji elementów z różnych kategorii, dostosowania ich do profilu ryzyka organizacji oraz regularnej oceny ich efektywności w warunkach rzeczywistych. Strategia bezpieczeństwa powinna być traktowana jako proces ciągły, w którym technologia, procedury i kompetencje personelu są rozwijane równolegle, a wnioski z incydentów i audytów stanowią podstawę do wprowadzania zmian w architekturze zabezpieczeń. Takie holistyczne podejście, uwzględniające przenikanie się kategorii narzędzi oraz elastyczne dostosowanie strategii ochrony do zmieniającego się środowiska zagrożeń, jest kluczowe dla zapewnienia wysokiego poziomu odporności cybernetycznej w sektorze finansowym. W rozdziale trzecim opracowania omówione zostały wybrane środki cyberbezpieczeństwa, które – według autora i przeprowadzonej przez niego krytycznej analizy literatury przedmiotu – w najbliższej przyszłości będą determinować parametry omawianego zjawiska.

2.6. Podsumowanie

Problematyka wpływu bezpieczeństwa informatycznego na stabilność systemu finansowego jest obecnie jednym z głównych wątków prac analitycznych związanych z cyfryzacją współczesnych finansów. Wiele instytucji stara się robić wszystko, by scenariusz kryzysu finansowego wywołanego przez technologię nigdy się nie zrealizował. Międzynarodowy Fundusz Walutowy wskazuje np. konieczność tworzenia tzw. *cyber-maps* sektora finansowego, uwzględniających instytucje i systemy oraz interfejsy pomiędzy nimi. Takie mapowanie powinno pozwalać na dokładną identyfikację systemowo ważnych instytucji i połączeń między nimi oraz umożliwiać identyfikację słabych punktów i wąskich gardeł (Brauchle i in., 2020). Rozwinięciem koncepcji wizualizacji instytucjonalno-organizacyjnej infrastruktury systemu finansowego są

projekcje scenariuszy transmisji incydentów informatycznych na szoki systemu finansowego. Warto podkreślić, że ta pozornie mało naukowa koncepcja jest w praktyce jedynym racjonalnym narzędziem, które może wspierać procesy decyzyjne w omawianym obszarze. Identyfikacja kanałów transmisyjnych oraz ich potencjalnego wpływu na system jest daleko ważniejsza od jakichkolwiek prób analizy ryzyka. Analiza ta jest bowiem – jak już wspomniano – praktycznie niewykonalna, podczas gdy przygotowanie odpowiednich planów reakcji na ewentualne szoki wydaje się właściwym kierunkiem zarządzania stabilnością systemu finansowego.

Budowanie odporności na ryzyko cybernetyczne w usługach finansowych jest coraz większym priorytetem dla wszystkich zainteresowanych stron. Banki i inne instytucje robią wiele, aby poprawić swą zdolność radzenia sobie z zagrożeniami cybernetycznymi, stosując zarówno wewnętrzne polityki, jak i regulacje właściwych organów. Nowym trendem obserwowanym w działalności bankowej jest tzw. *cyber threat intelligence*, czyli skoordynowane działania ukierunkowane na permanentne monitorowanie otoczenia informatycznego oraz wyprzedzanie działań intruzów internetowych. Także instytucje europejskie bardzo aktywnie monitorują zmiany zachodzące w cyberprzestrzeni. Jedną z kluczowych instytucji o wymiarze europejskim w obszarze cyberbezpieczeństwa jest cytowana już ENISA – Agencja Unii Europejskiej ds. Bezpieczeństwa Cybernetycznego. Na podstawie ogłoszonego w 2019 r. Rozporządzenia Parlamentu Europejskiego i Rady UE dalej zwanego aktem o cyberbezpieczeństwie instytucja ta otrzymała nowe, większe niż dotychczas uprawnienia (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881…). Podstawowym zadaniem ENISA jest wspieranie spójnego wprowadzania odpowiednich ram prawnych, a w szczególności skutecznego wdrażania dyrektyw UE oraz stosownych instrumentów prawnych zawierających aspekty dotyczące cyberbezpieczeństwa, co ma kluczowe znaczenie dla zwiększenia cyberodporności. ENISA będzie odgrywać kluczową rolę w tworzeniu i utrzymywaniu europejskich ram certyfikacji cyberbezpieczeństwa przez przygotowanie podstaw technicznych dla określonych programów certyfikacji. ENISA jest upoważniona do zacieśnienia współpracy operacyjnej na szczeblu UE, pomagając państwom członkowskim UE, które chcą się o nią zwrócić, w rozwiązywaniu ich incydentów cybernetycznych oraz wspierając koordynację UE w przypadku transgranicznych cyberataków i kryzysów na dużą skalę. Będący kluczowym elementem wyżej wymienionego rozporządzenia Akt o cyberbezpieczeństwie to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług oraz procesów informatycznych. Akt ten tworzy również ramy certyfikacji dla produktów, usług i procesów cyberbezpieczeństwa w Unii Europejskiej. Jest to przełomowe osiągnięcie, ponieważ pierwszy raz w historii rynku wewnętrznego powstaje regulacja o tak dużym zasięgu merytorycznym. Akt o cyberbezpieczeństwie określa mechanizmy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty lub usługi spełniają określone wymogi bezpieczeństwa. Celem tych regu-

lacji jest doprowadzenie do sytuacji, w której konsument będzie miał świadomość, że wybiera produkt i usługę, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa.

Akt rozpoczyna się zestawem sentencji wprowadzających. Pierwsza z nich w doskonały sposób identyfikuje kluczowy problem:

„Sieci i systemy informatyczne oraz sieci i usługi łączności elektronicznej odgrywają kluczową rolę w społeczeństwie i stały się podstawą wzrostu gospodarczego. Technologie informacyjno-komunikacyjne stanowią podstawę złożonych systemów wspierających codzienne działania społeczne, zapewniają funkcjonowanie naszej gospodarki w kluczowych sektorach, takich jak opieka zdrowotna, energetyka, finanse i transport, a zwłaszcza wspomagają funkcjonowanie rynku wewnętrznego"[47].

Postanowienia aktu stanowią również wyzwanie dla tych państw członkowskich, które do tej pory nie posiadały infrastruktury do testowania sprzętu i oprogramowania. Akt zwiększy pewność obywateli UE, że rozwiązania, z których korzystają, zostały sprawdzone pod kątem bezpieczeństwa przez niezależny i kompetentny podmiot.

Era cyfrowa, ku której niewątpliwie zmierza światowy system finansowy, będzie kierować światową gospodarkę w stronę coraz rzadszego wykorzystania nieelektronicznych narzędzi i metod rozliczeniowych. Transformacja ta będzie jednak permanentnie zwiększać liczbę i wielorakość zagrożeń bezpieczeństwa elektronicznych operacji finansowych. Innymi słowy, poziom ryzyka informatycznego w systemie finansowym przyrównać można już dziś do interpretacji pojęcia entropii w znaczeniu fizycznym. Ryzyko to będzie już wyłącznie rosło. Obecnie wśród najpowszechniejszych przejawów i determinant tego wzrostu wymienia się (Adelman i in, 2020):

- powszechnie stosowany i akceptowany transfer finansowych procesów biznesowych do podmiotów spoza systemu finansowego,
- upowszechnianie się rozwiązań wykorzystujących *cloud computing*,
- zanikanie tradycyjnych, nieelektronicznych kanałów dostępu do systemów instytucji finansowych,
- coraz częstsze wykorzystanie robotyki i algorytmów sztucznej inteligencji do automatyzacji procesów finansowych,
- zwiększające się zainteresowanie walutami wirtualnymi.

Co więcej, omawiana problematyka nigdy nie będzie się cechowała żadną oznaką stabilizacji. Rozwój zastosowań informatyki kreuje nowe możliwości, które bardzo szybko stają się już nie tylko wizjami, lecz realnymi projektami. Obecnie do tego typu zjawisk zaliczyć należy m.in.:

---

[47] Warto zauważyć – w kontekście krótkiej dyskusji terminologicznej z początku rozdziału – że dokument definiuje *cybersecurity* jako środki i działania związane z ochroną sieci i systemów informatycznych oraz ich użytkowników (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881…, Art. 2 – Definitions). W tym kontekście odpowiednikiem *cybersecurity* w języku polskim powinna być „ochrona danych i systemów", a nie „bezpieczeństwo".

- dynamicznie rozwijające zakres swoich usług instytucje pieniądza elektronicznego,
- pieniądz cyfrowy banków centralnych,
- kryptowaluty,
- procesy tokenizacji aktywów finansowych.

Istotnym elementem problemu wpływu technologii na stabilność systemu finansowego jest także trudność szacowania ryzyka informatycznego. Powszechnie rekomendowane narzędzia ilościowe nie dają żadnej odpowiedzi na pytania dotyczące potencjalnych skutków realizacji zagrożeń typu 3 i 4 przedstawionych w rozdziale drugim. Ten aspekt omawianej problematyki należy uznać za jeden z kluczowych. To właśnie zdarzenia niezwykle rzadkie i o nieprzewidywalnych skutkach mają potencjał systemowy, umożliwiający transmisję pojedynczych incydentów na cały system, skutkującą problemami natury zarówno technicznej, jak i organizacyjnej oraz reputacyjnej.

Rozdział 3

Determinanty cyberbezpieczeństwa systemu finansowego

3.1. Wprowadzenie

Współczesne podejście do zarządzania cyberbezpieczeństwem zakłada konieczność systematycznego identyfikowania i analizy determinant bezpieczeństwa – czynników warunkujących zdolność organizacji, systemów informatycznych oraz całych sektorów do przeciwdziałania zagrożeniom, ograniczania skutków incydentów oraz skutecznego reagowania na ataki. Determinanty te nie mają wyłącznie charakteru technicznego, lecz obejmują również aspekty organizacyjne, regulacyjne, ludzkie i środowiskowe, co odzwierciedla wielowymiarowość zjawiska cyberbezpieczeństwa. Ich identyfikacja możliwa jest zarówno poprzez systematyczne obserwacje praktyk organizacyjnych i incydentów bezpieczeństwa, jak i na podstawie wiedzy eksperckiej gromadzonej m.in. w raportach branżowych, analizach sektorowych, normach technicznych oraz badaniach akademickich. Tak zdefiniowane determinanty stanowią punkt wyjścia do budowy modeli odporności cyfrowej, oceny ryzyka oraz projektowania strategii zarządzania bezpieczeństwem informacji. W niniejszym rozdziale podjęto próbę klasyfikacji najważniejszych determinant cyberbezpieczeństwa z uwzględnieniem ich źródeł, powiązań funkcjonalnych oraz znaczenia dla sektora finansowego.

Interdyscyplinarność analizowanego zagadnienia w naturalny sposób utrudnia jego systematyczne ujęcie. Istnieje szereg uwarunkowań, których charakterystyka ma istotne znaczenie dla zrozumienia dynamicznych procesów adaptacyjnych w obrębie ekosystemów bezpieczeństwa cyfrowego. Przede wszystkim należy wskazać:

- intensyfikację rozwoju technologii informatycznych, która prowadzi do nieustannego pojawiania się nowych architektur systemowych, protokołów komunikacyjnych oraz rozwiązań chmurowych, stwarzających zarówno szanse rozwoju, jak i nowe zagrożenia bezpieczeństwa,
- eskalację zaawansowania technik i metod ataków cybernetycznych, głównie związanych z szeroko rozumianym phishingiem, w tym także opartym na sztucznej inteligencji,
- automatyzację procesów, nie tylko w obszarze działalności operacyjnej, ale również w strukturach zarządzania ryzykiem informatycznym, co generuje nowe potrzeby w zakresie bezpieczeństwa systemów autonomicznych oraz podejmowania decyzji w czasie rzeczywistym,

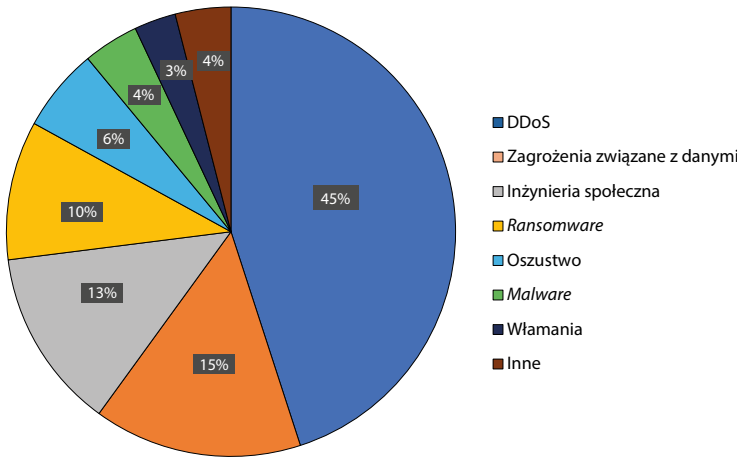
- zachodzące przemiany społeczne, obejmujące m.in. cyfryzację codziennych interakcji, upowszechnienie pracy zdalnej oraz zwiększoną podatność użytkowników końcowych na manipulacje informacyjne i socjotechniczne,
- rygorystyczne wymagania w zakresie zarządzania ryzykiem operacyjnym, które wymuszają wdrażanie zaawansowanych strategii oceny ryzyka, zgodności regulacyjnej oraz planowania ciągłości działania,
- wzrost dostępnej mocy obliczeniowej, co umożliwia zarówno intensyfikację analiz predykcyjnych i stosowanie algorytmów uczenia maszynowego w detekcji zagrożeń, jak i rozwój cyberprzestępczości wykorzystującej zaawansowane narzędzia analityczne,
- rozszerzające się ramy regulacyjne i zwiększające się znaczenie współpracy międzynarodowej, obejmujące inicjatywy legislacyjne oraz działania koordynacyjne w ramach unijnych, międzykontynentalnych i międzysektorowych platform wymiany informacji o incydentach i podatnościach.

Charakterystyka tych problemów wskazuje jednoznacznie ich interdyscyplinarny charakter – obejmujący aspekty technologiczne, społeczne, organizacyjne oraz prawne – co uniemożliwia ich uproszczoną systematyzację lub klasyfikację według jednorodnych kryteriów. Analiza ich współzależności wymaga stosowania metod badawczych integrujących nauki techniczne, zarządzanie, prawo oraz socjologię technologii[48], co stanowi wyzwanie zarówno dla środowiska akademickiego, jak i dla praktyków zarządzania cyberbezpieczeństwem w instytucjach finansowych. Ważne jest także ciągłe śledzenie statystyk i danych liczbowych obrazujących skalę i dynamikę zmian w obszarze bezpieczeństwa. Dane takie zawsze będą jedynie cząstkowym, wybiórczym obrazem rzeczywistości, niemniej ich systematyczne zestawianie może być podstawą poprawnych wniosków. Na przykład raport wspomnianej już organizacji ENISA (2025) prezentuje statystykę zidentyfikowanych realizacji zagrożeń bezpieczeństwa w sektorze finansowym w Europie (rys. 1)[49].

---

[48] Socjologia technologii, zwana także cybersocjologią, to dziedzina zajmująca się poszukiwaniem odpowiedzi na pytanie, jak technologie cyfrowe wpływają na strukturę społeczną, tożsamość jednostki, wzorce komunikacyjne, formy uczestnictwa obywatelskiego oraz dynamikę władzy i kontroli. Analizuje również, w jaki sposób społeczne potrzeby, normy i instytucje kształtują rozwój i zastosowanie tych technologii. Cybersocjologia obejmuje problemy tożsamości cyfrowej, społeczności wirtualnych, cyfrowej nierówności, cyberkultury i memetyki, relacji władzy w sieci oraz cyberprzemocy i cyberprzestępczości (Graham i Dutton, 2019).

[49] Jak zaznaczają autorzy raportu, incydent może zostać zaklasyfikowany do więcej niż jednej kategorii zagrożeń, co oznacza, że łączny procent zagrożeń przedstawionych na rysunku przekracza 100. Przykładowo, wektor ataku użyty do uzyskania początkowego dostępu może obejmować kampanię phishingową o tematyce finansowej (inżynieria społeczna), po której następuje kompromitacja systemu za pomocą oprogramowania *ransomware*, która może – choć nie musi – prowadzić do wycieku danych (zagrożenia związane z danymi). Podobnie incydenty obejmujące atak na dostawcę lub usługodawcę zostały sklasyfikowane zarówno jako ataki na łańcuch dostaw (*supply chain*), jak i jako konkretny typ ataku wykorzystany do naruszenia bezpieczeństwa.



Rys. 1. Statystyka zagrożeń cyberbezpieczeństwa w sektorze finansowym w Europie (styczeń 2023 – czerwiec 2024)

Źródło: (ENISA, 2025).

Analiza statystyki przedstawionej na rys. 1 prowadzi do konstatacji, zgodnie z którą w wymiarze ilościowym dominują dwa rodzaje zagrożeń: ataki typu DDoS i wszelkiego rodzaju negatywne skutki phishingu oraz innych metod ukierunkowanych na nieautoryzowany dostęp do systemów, kradzież poufnych danych, oszustwa. Podobny w swojej wymowie jest raport firmy Cisco (2024), z którego wynika, że najczęściej identyfikowanym w 2024 r. zagrożeniem było oprogramowanie typu *information stealer* (246 mln przypadków). Następne w kolejności były: trojany (175 mln), *ransomware* (154 mln), RAT (*Remote Access Trojan* – 46 mln), APT (40 mln), *botnet* (31 mln), *dropper* (20 mln), *backdoor* (14 mln).

W raporcie CheckPoint (2025) zwrócono natomiast uwagę na najbardziej dynamicznie rozwijające się typy zagrożeń. Wyróżniono przede wszystkim: *ransomware*, *information stealers*, zagrożenia *cloud computing*, problemy bezpieczeństwa urządzeń brzegowych oraz wskazano na rosnące znaczenie szerszego kontekstu cyberbezpieczeństwa, jakim są wspomniane już *cyber wars*.

Raport Armis (2025) skupia się na coraz częściej eksponowanym – zasygnalizowanym w poprzednich rozdziałach – problemie *AI as a double egded sword*. Wśród aspektów negatywnych wymienia:

- zautomatyzowane tworzenie złośliwego oprogramowania – złośliwy kod generowany przez AI może dynamicznie modyfikować swoją strukturę, aby unikać wykrycia przez systemy zabezpieczeń,
- *phishing* wspomagany sztuczną inteligencją – wiadomości generowane maszynowo zwiększają skuteczność ataków socjotechnicznych, czyniąc je bardziej realistycznymi i personalizowanymi,

- dezinformację przy użyciu *deepfake* – treści multimedialne tworzone przez AI manipulują opinią publiczną oraz podważają zaufanie do autentyczności cyfrowej komunikacji,
- autonomiczne ataki sieciowe – narzędzia oparte na sztucznej inteligencji nieprzerwanie skanują infrastrukturę w poszukiwaniu podatności i przeprowadzają ataki bez udziału człowieka,
- rekomendacje celów ataku przez AI – systemy analityczne wspierane AI identyfikują obszary najbardziej podatne na atak, które jednocześnie są pozbawione odpowiednich mechanizmów detekcji.

Po stronie pozytywów odnajdujemy natomiast:

- analizę behawioralną – sztuczna inteligencja wykrywa odchylenia od normalnej aktywności użytkownika, identyfikując potencjalne próby wtargnięcia,
- zautomatyzowane wyszukiwanie zagrożeń – AI nieustannie skanuje środowisko w poszukiwaniu nowych wektorów ataku, wskaźników aktywności ofensywnych oraz oznak naruszenia bezpieczeństwa,
- adaptacyjne mechanizmy obronne – sztuczna inteligencja umożliwia dynamiczną rekonfigurację ustawień zabezpieczeń w czasie rzeczywistym, dostosowując je do pojawiających się zagrożeń,
- wykrywanie eksploatacji podatności – modele uczenia maszynowego identyfikują przypadki aktywnego wykorzystywania luk w oprogramowaniu,
- rekomendacje obronne – AI może generować plany przeciwdziałania na podstawie wykrytego zagrożenia oraz dostępnych środków ochrony, dostosowanych do specyfiki środowiska.

Raport CrowdStrike (2025) wskazuje natomiast następujące kluczowe problemy współczesnego cyberbezpieczeństwa: *social engineering* ze szczególnym uwzględnieniem vishingu, połączenie sztucznej inteligencji i inżynierii społecznej, zagrożenia przetwarzania w chmurze, w szczególności SaaS. Raport porusza także problem rosnącego, holistycznego zagrożenia ze strony jednego z państw[50].

Krajowy raport CERT (2025) podkreśla znaczenie *ransomware*, wycieków danych, działań grup APT, oszustw reklamowych oraz *malware* mobilnego. Raport jak zwykle promuje także edukację informatyczną.

Synteza wspomnianych treści wskazuje ogólny zbiór problemów, które w najbliższej przyszłości determinować będą światowe cyberbezpieczeństwo. Należą do nich:

[50] W raporcie odnajdujemy obszerną analizę zdolności Chin w zakresie cyberwywiadu i zbierania informacji, które – według autorów – osiągnęły w 2024 r. punkt zwrotny w porównaniu z latami poprzednimi. Oprócz intensywnych i szeroko nagłaśnianych działań szpiegowskich w cyberprzestrzeni, podmioty powiązane z Chinami oraz szeroko rozumiany ekosystem wspierający ich operacje wykazały znaczny wzrost zarówno skali działania, jak i w zakresie kompetencji.

- inżynieria społeczna i narzędzia jej eksploatacji,
- szkodliwe oprogramowanie ukierunkowane głównie na kompromitację parametrów dostępu do systemów,
- zastosowania sztucznej inteligencji.

W kontekście systemów finansowych należy również zwrócić uwagę na zjawisko, które ma istotne znaczenie prognostyczne, mimo że pozostaje jeszcze poza głównym nurtem raportów branżowych oraz systematycznych analiz technologicznych. Mowa o potencjalnych zastosowaniach nowoczesnej kryptografii oraz wpływie, jaki rozwój technologii obliczeń kwantowych może wywrzeć na obecne modele zabezpieczeń kryptograficznych. Choć zagadnienie to ma wciąż charakter przyszłościowy, wiele wskazuje na to, że jego znaczenie stanie się krytyczne znacznie szybciej, niż zakładają obecne scenariusze strategiczne. Postępy w dziedzinie komputerów kwantowych mogą bowiem prowadzić do fundamentalnego przełomu w zdolności łamania współczesnych nam algorytmów szyfrowania, co ma istotne implikacje dla integralności, poufności oraz niezaprzeczalności danych w systemach finansowych.

Podsumowując, można wskazać, że obszarami, których rozwój będzie decydował w najbliższej przyszłości o szeroko rozumianym cyberbezpieczeństwie sektora finansowego, są:

- silne uwierzytelnienie klienta i jego poprawna, powszechna implementacja,
- świadomość informatyczna użytkowników końcowych, w szczególności użytkowników systemów bankowości internetowej i mobilnej,
- wzrost dostępnej mocy obliczeniowej komputerów, związany głównie z koncepcją komputera kwantowego,
- zastosowania rozwiązań wykorzystujących sztuczną inteligencję, głównie w obszarze systemów wykrywania anomalii.

Każda konstatacja tego typu będzie zawsze obarczona wadą subiektywności. Wieloletnia analiza rozwoju omawianej problematyki musi jednak prowadzić do takich wniosków. W dalszej części rozdziału przedstawiono, w ujęciu zarówno teoretycznym, jak i praktycznym, zarys wymienionych problemów.

3.2. Silne uwierzytelnienie

3.2.1. Uwagi wstępne

Pojęcie silnego uwierzytelnienia (*strong authentication*) po raz pierwszy zostało formalnie zdefiniowane i wprowadzone do praktyki w dokumentach normatywnych oraz międzynarodowych standardach technicznych na początku lat dziewięćdziesiątych XX w.[51] Początkowo koncepcja ta stanowiła opozycję względem tzw. prostej autoryza-

[51] Jedną z pierwszych norm definiujących to pojęcia była ITU-T: Recommendation X.800: Security Architecture for Open Systems – norma międzynarodowa, określająca architekturę bezpieczeństwa dla otwartych systemów komunikacyjnych, opublikowana w 1991 r. (ITU, 1991).

cji (*simple authentication*), która opierała się wyłącznie na zastosowaniu tradycyjnego mechanizmu identyfikacyjnego opartego na parze identyfikator użytkownika i hasło statyczne. Tego rodzaju uwierzytelnienie, choć powszechne i łatwe w implementacji, wykazywało znaczne słabości z perspektywy bezpieczeństwa informacyjnego, w szczególności w kontekście rosnącego zagrożenia cyberatakami. Wraz z dynamicznym rozwojem infrastruktury klucza publicznego koncepcja silnego uwierzytelniania zaczęła ewoluować w kierunku bardziej złożonych modeli uwierzytelniających, opartych na wieloskładnikowości oraz kryptografii asymetrycznej. W tym kontekście silne uwierzytelnienie zaczęto definiować jako proces, który wymaga od użytkownika przedstawienia co najmniej dwóch niezależnych elementów uwierzytelniających, pochodzących z różnych kategorii: wiedzy, posiadania oraz cech biometrycznych.

Współcześnie silne uwierzytelnienie stanowi jedno z kluczowych zagadnień w obszarze bezpieczeństwa systemów informatycznych i cyberbezpieczeństwa jako całości. Znaczenie tego pojęcia zostało dodatkowo wzmocnione przez wdrożenie dyrektywy znanej jako PSD2 (Payment Services Directive 2), która wymusza implementację silnego uwierzytelnienia klienta (SCA – *Strong Customer Authentication*) w usługach płatniczych świadczonych drogą elektroniczną (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366…). Regulacja ta miała na celu nie tylko podniesienie poziomu ochrony konsumenta, lecz także zwiększenie zaufania do rozwiązań finansowych online. Silne uwierzytelnienie należy także rozpatrywać jako integralny komponent szerszego paradygmatu bezpieczeństwa informatycznego, jakim jest kontrola dostępu (*access control*). Umożliwia ona nie tylko weryfikację tożsamości użytkownika, ale również zapewnienie, że dostęp do zasobów systemowych uzyskują wyłącznie uprawnione podmioty, zgodnie z określoną polityką bezpieczeństwa organizacji.

3.2.2. Kontrola dostępu

Kontrola dostępu stanowi jeden z podstawowych filarów bezpieczeństwa systemów informatycznych, odpowiadający za ograniczanie dostępu do zasobów wyłącznie dla podmiotów uprawnionych. Kontrolę dostępu zdefiniować można jako ogół mechanizmów, mających na celu zagwarantowanie, że tylko upoważnione osoby lub systemy mają możliwość dostępu do określonych zasobów informacyjnych. W ujęciu ogólnym dostęp użytkownika do określonego zasobu jest definiowany jako zestaw przysługujących mu praw operacyjnych, obejmujących odczyt, zapis oraz wykonywanie (*read, write, execute*) danego obiektu systemowego. Mechanizmy kontroli dostępu dzieli się na trzy główne kategorie:

- kontrolę dyskrecjonalną (*Discretionary Access Control*, DAC),
- kontrolę obowiązkową (*Mandatory Access Control*, MAC),
- kontrolę opartą na rolach (*Role-Based Access Control*, RBAC) (Wawrzyniak, 2012, s. 155 i n.).

Dyskrecjonalna kontrola dostępu opiera się na zasadzie, według której właściciel zasobu lub podmiot uprawniony decyduje, którzy użytkownicy mogą uzyskać dostęp do danego obiektu i w jakim zakresie. Mechanizm ten jest oparty na sprawdzeniu uprawnień przypisanych użytkownikowi względem konkretnego obiektu systemowego. Dostęp może być rozpatrywany na dwa sposoby:

- użytkownik uzyskuje dostęp, jeśli system udziela jednoznacznej odpowiedzi pozytywnej,
- użytkownik uzyskuje dostęp, o ile system nie wygeneruje odpowiedzi negatywnej (model domniemanej zgody).

Większość nowoczesnych systemów informatycznych implementuje model pozytywnej kontroli dostępu, w którym dostęp jest przyznawany wyłącznie na podstawie wyraźnie zdefiniowanych uprawnień. W przeciwieństwie do tego model negatywny umożliwia domyślny dostęp do danych wszystkim użytkownikom, z wyjątkiem zasobów objętych mechanizmami bezpieczeństwa. Choć DAC umożliwia elastyczne zarządzanie uprawnieniami – m.in. przez tworzenie grup użytkowników o identycznych przywilejach – to jednocześnie cechuje się ograniczoną możliwością kontroli propagacji informacji oraz brakiem mechanizmów klasyfikacji zasobów według poziomu tajności.

Model obowiązkowej kontroli dostępu wprowadza rygorystyczną politykę bezpieczeństwa, w której zarówno użytkownicy, jak i obiekty systemowe przyporządkowani są określonym poziomom klasyfikacji (np. *poufne*, *tajne*, *ściśle tajne*). Dostęp do zasobów określany jest zgodnie z zasadami:

- „czytania w dół" (*no read up*) – użytkownik może odczytywać dane, których poziom klasyfikacji nie przekracza jego uprawnień,
- „pisania w górę" (*no write down*) – użytkownik może zapisywać dane jedynie do obiektów o równym lub wyższym poziomie klasyfikacji.

Model MAC minimalizuje ryzyko nieautoryzowanego ujawnienia informacji i zapewnia wysoki poziom ochrony przed niekontrolowanym przepływem danych, zgodnie z klasycznymi zasadami opisanymi już ponad 50 lat temu (Bell i LaPadula, 1973).

Kontrola dostępu oparta na rolach stanowi kompromis między elastycznością DAC a rygorem MAC, integrując ich najważniejsze zalety. W tym modelu dostęp do zasobów jest determinowany przez przynależność użytkownika do określonych ról, które z kolei są powiązane z zestawami uprawnień niezbędnych do realizacji przypisanych zadań. Proces kontroli przebiega dwuetapowo przez tworzenie ról odpowiadających funkcjom organizacyjnym lub operacyjnym w systemie oraz przypisanie użytkownika do jednej lub więcej ról, co pośrednio skutkuje nadaniem mu dostępu do właściwych zasobów. RBAC upraszcza zarządzanie uprawnieniami w systemach o dużej liczbie użytkowników oraz umożliwia łatwiejsze egzekwowanie zasad bezpieczeństwa zgodnych z polityką organizacyjną (Sandhu i in., 1996). Rozszerzenie możliwości RBAC oferują modele typu ABAC (*Attribute-Based Access Control*) umożliwiające wprowadzenie decyzji kontekstowych opartych na atrybutach:

- podmiotu (np. roli, lokalizacji),
- zasobu (np. typie danych),
- środowiskowych (np. godzinie, adresie IP),
- działań (np. operacji odczytu).

Dzięki temu ABAC umożliwia formułowanie bardziej złożonych i adaptacyjnych polityk dostępu. ABAC jest obecnie szeroko wykorzystywana w systemach opartych na chmurze oraz w rozwiązaniach klasy *Policy Enforcement Point* (PEP) i *Policy Decision Point* (PDP) (Arshad i in., 2022).

Klasyczne podejścia do projektowania bezpiecznych systemów informacyjnych można scharakteryzować dwojako: funkcjonalnie – poprzez zbiór zasad projektowych, oraz formalnie – poprzez modele matematyczne wyrażające polityki bezpieczeństwa. Kluczowymi publikacjami rozwijającymi te podejścia są prace Saltzera i Schroedera (1975) oraz Bella i LaPaduli (1973). Saltzer i Schroeder przedstawili osiem fundamentalnych zasad, które powinny kierować projektowaniem bezpiecznych systemów. Wśród nich szczególne znaczenie dla kontroli dostępu mają:

- zasada najmniejszego uprzywilejowania (*principle of least privilege*) – użytkownik powinien mieć wyłącznie te uprawnienia, które są niezbędne do wykonania danej czynności,
- zasada kompletności mediacji (*complete mediation*) – każda próba dostępu do obiektu powinna być weryfikowana przez mechanizm kontroli,
- zasada otwartości projektu (*open design*) – bezpieczeństwo systemu nie powinno opierać się na tajności jego struktury, lecz na poufności kluczy i innych danych wrażliwych,
- zasada ekonomii mechanizmów (*economy of mechanism*) – mechanizmy kontroli dostępu powinny być możliwie proste, zrozumiałe i możliwe do audytu.

Te zasady stały się podstawą konstrukcji i oceny nowoczesnych systemów kontroli dostępu, na poziomie zarówno operacyjnym (np. systemy operacyjne), jak i aplikacyjnym (np. systemy bankowe, chmury obliczeniowe). Z kolei formalne ujęcie problemu kontroli dostępu rozwinięto w modelu Bella i LaPaduli. Model ten skupia się na ochronie poufności danych i jest szczególnie użyteczny w systemach przetwarzających informacje sklasyfikowane, jak np. systemy wojskowe. Opiera się on na dwóch zasadach:

- zasadzie *no read up* (*simple security property*) – użytkownik nie może odczytać danych z poziomu bezpieczeństwa wyższego niż ten, do którego ma dostęp,
- zasadzie *no write down* (*-property) – użytkownik nie może zapisywać danych na poziomie niższym niż jego własny, co zapobiega nieautoryzowanemu przekazywaniu informacji do niższych klas zaufania.

Podejścia wymienionych naukowców pokazują wspólnie, że skuteczna kontrola dostępu wymaga zarówno przemyślanych zasad projektowych, jak i rygorystycznych modeli matematycznych, dostosowanych do charakteru chronionych danych i środo-

wiska operacyjnego. Ich znaczenie nie maleje mimo upływu lat, gdyż wiele współczesnych systemów – w tym nowoczesne modele uwierzytelniania oparte na tożsamości (*Identity-Based Access Control*, IBAC) czy rolach (RBAC) – opiera się na tych klasycznych fundamentach.

Klasyczne podejścia do kontroli dostępu stanowiły podstawę rozwoju praktycznych, skalowalnych systemów zabezpieczeń w środowiskach informatycznych. Wraz z postępującą cyfryzacją usług oraz migracją do środowisk chmurowych i rozproszonych konieczne stało się opracowanie bardziej elastycznych, dynamicznych metod zarządzania dostępem. W odpowiedzi na te potrzeby wykształciły się trzy dominujące modele współczesne: kontrola dostępu oparta na rolach, kontrola dostępu oparta na atrybutach oraz architektura *Zero Trust* – filozofia bezpieczeństwa zakładająca, że żaden podmiot, ani wewnętrzny, ani zewnętrzny, nie jest domyślnie zaufany. W modelu tym:

- każda próba dostępu wymaga uwierzytelnienia i autoryzacji w czasie rzeczywistym,
- decyzje opierają się na danych kontekstowych i bieżącej analizie ryzyka,
- wdrożone są mechanizmy ciągłej weryfikacji i mikrosegmentacji.

Model bezpieczeństwa *Zero Trust* (ZT) stanowi przełomowe podejście do ochrony systemów informatycznych w erze rosnących zagrożeń cybernetycznych oraz upowszechnienia pracy zdalnej i środowisk chmurowych. W przeciwieństwie do tradycyjnych modeli opartych na zaufaniu w obrębie sieci ZT zakłada zasadę „nigdy nie ufaj, zawsze weryfikuj", zgodnie z którą żadna jednostka ani zasób – niezależnie od położenia w sieci – nie może być domyślnie uznana za bezpieczną bez uprzedniego sprawdzenia. ZT koncentruje się na szczegółowej kontroli dostępu, uwierzytelnianiu tożsamości użytkowników i urządzeń, segmentacji sieci oraz ciągłym monitoringu zachowań. Na przykład Chawda i Parmar (2025) zaprezentowali hybrydowy model oparty na ZT i technologii *blockchain*, umożliwiający inteligentne zarządzanie dostępem do danych w środowiskach o wysokim poziomie ryzyka, takich jak infrastruktura krytyczna. Jednym z istotnych zastosowań ZT jest ochrona małych i średnich przedsiębiorstw, dla których tradycyjne zabezpieczenia bywają niewystarczające. Femighty i in. (2022) opisali wdrożenie ZT w chmurze jako skuteczne narzędzie zabezpieczające dane i aplikacje MŚP przed nieautoryzowanym dostępem. Również R. Kumar (2022) podkreśla konieczność stosowania architektury ZT w kontekście zmiennych zagrożeń dla systemów chmurowych i hybrydowych. Współczesne badania wskazują na dynamiczny rozwój modelu ZT w połączeniu z uczeniem maszynowym, federacyjnym uczeniem oraz biometrią behawioralną. Ogunmolu (2025) wykazał, że takie połączenia mogą wzmocnić architekturę ZT, szczególnie w sektorze ochrony zdrowia, który wymaga zarówno wysokiego poziomu bezpieczeństwa, jak i zgodności z przepisami o ochronie danych. Wdrożenie *Zero Trust* nie jest jednak pozbawione wyzwań. Pigola i de Spouza Meirelles (2025) identyfikują najważniejsze bariery organizacyjne, takie jak brak świadomości technologicznej, opór kulturowy czy wysokie koszty implementacji. W związku z tym sukces wdrożenia ZT zależy w dużej mierze od kompleksowego

planowania, integracji z istniejącą infrastrukturą oraz szkoleń personelu. Podsumowując, należy podkreślić, że model *Zero Trust* stanowi obecnie fundament nowoczesnego cyberbezpieczeństwa. Jego rola będzie rosła wraz ze wzrostem liczby zagrożeń wewnętrznych i zewnętrznych, a także rozwojem technologii opartych na danych i rozproszonych środowisk pracy.

3.2.3. Uwierzytelnienie użytkownika

Kontrola dostępu w klasycznym ujęciu stanowi fundamentalny mechanizm bezpieczeństwa informacyjnego, obejmujący zintegrowany proces identyfikacji, uwierzytelnienia oraz autoryzacji użytkowników i systemów. Identyfikacja polega na jednoznacznym określeniu tożsamości podmiotu próbującego uzyskać dostęp do zasobów informatycznych. Na kolejnym etapie – uwierzytelnienia – następuje weryfikacja przedstawionej tożsamości na podstawie dostarczonych danych uwierzytelniających (np. hasła, tokenu lub cech biometrycznych). Dopiero po pozytywnej weryfikacji możliwe jest przeprowadzenie autoryzacji, czyli przyznania odpowiedniego poziomu uprawnień do określonych zasobów, zgodnie z obowiązującymi politykami bezpieczeństwa oraz zasadą najmniejszych uprawnień. Cały ten proces jest realizowany w sposób deterministyczny i hierarchiczny, co w modelach klasycznych zakłada zaufanie do wewnętrznych komponentów infrastruktury sieciowej i użytkowników znajdujących się „wewnątrz" granic organizacyjnych. Uwierzytelnienie jest jednym z kluczowych filarów bezpieczeństwa informacyjnego i cyberbezpieczeństwa, stanowiąc proces weryfikacji tożsamości podmiotu próbującego uzyskać dostęp do chronionych zasobów systemu komputerowego lub sieciowego. W klasycznym ujęciu, zgodnie z definicją przyjętą w literaturze naukowej, uwierzytelnienie polega na potwierdzeniu tożsamości na podstawie zestawu poświadczeń (Khanna, 2024, s. 75). Jak zauważają Poirrier i in. (2025), uwierzytelnienie różni się od autoryzacji – nie przyznaje uprawnień, a jedynie potwierdza tożsamość użytkownika. W praktyce oznacza to, że użytkownik musi „udowodnić, kim jest", zanim otrzyma jakikolwiek dostęp. Skuteczność uwierzytelnienia ma bezpośredni wpływ na odporność systemu na wiele ataków, w szczególności *phishing*, wycieki haseł, *credential stuffing* oraz przejęcie sesji. Wielu autorów podkreśla również znaczenie tzw. uwierzytelnienia ciągłego (*continuous authentication*), które dynamicznie weryfikuje użytkownika w trakcie trwania sesji, np. na podstawie wzorców zachowania (Ali i in., 2025).

Teoria uwierzytelnienia (*authentication theory*) wywodzi się z fundamentalnych prac z zakresu kryptografii i teorii informacji, których początki datowane są na lata siedemdziesiąte XX w. Jej rozwój jest nierozerwalnie związany z wcześniejszymi osiągnięciami Shannona (1949), który w przełomowym artykule *Communication Theory of Secrecy Systems* zapoczątkował formalne ramy teoretyczne dla systemów poufnych. Zdefiniował pojęcie idealnej poufności (*perfect secrecy*), która położyła podwaliny pod dalsze prace nad bezpieczeństwem informacji i stworzeniem modeli uwierzytelniania. Teoria systemów poufnych zakłada istnienie trzech kluczowych kompo-

nentów: nadawcy, odbiorcy i przeciwnika. Celem systemu jest zapewnienie, że tylko uprawniony odbiorca ma dostęp do przesyłanych danych, podczas gdy przeciwnik nie może ich odszyfrować ani zmodyfikować. W tym kontekście uwierzytelnianie odgrywa fundamentalną rolę, umożliwiając potwierdzenie tożsamości uczestników komunikacji oraz integralności przesyłanych danych. Wraz z rozwojem technologii informacyjnych i coraz większą skalą rozproszonych systemów komputerowych potrzeba formalizacji i standaryzacji mechanizmów uwierzytelniania doprowadziła do powstania kompleksowych modeli kontroli dostępu, które opierają się na fundamentalnym założeniu, że przed przyznaniem użytkownikowi określonych praw dostępu musi on przejść proces uwierzytelnienia. Zatem teoria uwierzytelnienia stanowi integralny komponent szerszej dziedziny naukowej, jaką jest bezpieczeństwo informacji, łącząc w sobie elementy kryptografii, teorii informacji oraz informatyki teoretycznej. Jej rozwój odzwierciedla ewolucję potrzeb w zakresie zapewniania bezpieczeństwa komunikacji w systemach informatycznych.

Odpowiedzią na zwiększającą się skalę zagrożeń cybernetycznych oraz konieczność spełniania regulacji prawnych, takich jak unijna dyrektywa PSD2, jest wspomniane już silne uwierzytelnianie klienta (*Strong Customer Authentication*, SCA) – proces wymagający przedstawienia co najmniej dwóch niezależnych dowodów tożsamości spośród trzech kategorii: czegoś, co użytkownik wie (np. hasło), posiada (np. token sprzętowy lub telefon) lub kim jest (np. cechy biometryczne). Celem tego podejścia jest znaczne zwiększenie pewności co do tożsamości użytkownika i ograniczenie ryzyka nieautoryzowanego dostępu wynikającego z przechwycenia jednego z elementów uwierzytelniających. Z perspektywy bezpieczeństwa systemów informatycznych silne uwierzytelnianie pełni funkcję swego rodzaju bramy, chroniącej systemy przed nieautoryzowanym użyciem, kradzieżą danych czy eskalacją uprawnień. Umożliwia egzekwowanie polityk bezpieczeństwa i zapewnia warstwę ochrony niezależnie od lokalizacji użytkownika – co ma szczególne znaczenie w przypadku pracy zdalnej, chmur obliczeniowych i rozproszonych środowisk. W rezultacie SCA ma zastosowanie nie tylko w sektorze finansowym, lecz także w administracji publicznej, medycynie, edukacji i w każdej branży wymagającej ochrony danych wrażliwych. Rozwój koncepcji silnego uwierzytelniania wpisuje się w szersze ramy ewolucji mechanizmów kontroli dostępu, które przeszły drogę od prostych haseł do złożonych systemów adaptacyjnych, opartych na analizie kontekstu (np. geolokalizacji, czasu logowania, zachowań użytkownika). Wprowadzenie silnego uwierzytelniania nie jest jednak pozbawione wyzwań. Należą do nich m.in.: konieczność integracji z istniejącymi systemami, koszt wdrożenia nowych technologii, zapewnienie pozytywnego doświadczenia użytkownika, a także spełnienie wymagań wynikających z przepisów i regulacji. W dalszej części podjęto próbę bardziej szczegółowej analizy tego zagadnienia.

3.2.4. Metody uwierzytelniania

Jak już wspomniano, silne uwierzytelnienie klienta to jedno z kluczowych rozwiązań wprowadzonych w celu zwiększenia bezpieczeństwa transakcji elektronicznych w kontekście rosnącej cyfryzacji usług finansowych i wzrostu zagrożeń cybernetycznych. Jest to obowiązek regulacyjny wynikający z dyrektywy Unii Europejskiej PSD2, która ustanowiła nowe zasady dotyczące bezpieczeństwa płatności elektronicznych oraz otwartego dostępu do danych bankowych. Zgodnie z rozporządzeniem Komisji Europejskiej (tzw. RTS – *Regulatory Technical Standards*) SCA polega na zastosowaniu co najmniej dwóch z trzech niezależnych elementów uwierzytelniających (Rozporządzenie delegowane Komisji (UE) 2018/389…):

- wiedzy – czegoś, co wie tylko użytkownik (np. hasła, PIN-u),
- posiadania – czegoś, co posiada tylko użytkownik (np. telefonu komórkowego, tokena, karty),
- cechy indywidualnej – czegoś, co określa, kim użytkownik jest (np. danych biometrycznych).

Celem wprowadzenia SCA jest zwiększenie odporności systemów płatniczych na nadużycia, oszustwa i przejęcia kont. W tradycyjnych systemach autoryzacji, szczególnie w *e-commerce*, stosowanie pojedynczych metod uwierzytelniania – np. samego hasła – od dawna jest już niewystarczające wobec rosnącej liczby ataków phishingowych, przejęć danych logowania i zautomatyzowanych oszustw. Wprowadzenie SCA stanowi zatem odpowiedź na konieczność podniesienia poziomu bezpieczeństwa przy jednoczesnym zachowaniu funkcjonalności usług cyfrowych (Hettiarachchige i Jahankhani, 2021). W ujęciu regulacyjnym SCA jest obowiązkowe przy wszystkich płatnościach elektronicznych, chyba że zastosowanie mają wyjątki, takie jak (Casanova i in., 2022):

- transakcje niskokwotowe,
- transakcje do zaufanych odbiorców,
- powtarzalne płatności o tej samej kwocie,
- transakcje ocenione jako operacje niskiego ryzyka (na podstawie analizy ryzyka transakcji).

Co istotne, SCA nie ogranicza się wyłącznie do rynku europejskiego. Na świecie można wskazać szereg regulacji zbieżnych z duchem PSD2:

- w Stanach Zjednoczonych podobną funkcję pełnią zalecenia FFIEC (Federal Financial Institutions Examination Council) w zakresie uwierzytelniania wieloskładnikowego,
- w Indiach Bank Rezerw Indii (RBI) od 2012 r. wymaga dwuetapowego uwierzytelniania dla transakcji internetowych,
- w Singapurze Urząd Monetarny (MAS) nakłada obowiązki na cyfrowe instytucje finansowe w zakresie stosowania zaawansowanych metod uwierzytelnienia w bankowości internetowej i mobilnej.

W kontekście systemu bankowego w Polsce obowiązki wynikające z SCA zostały zaimplementowane w ramach Ustawy o usługach płatniczych (Ustawa z dnia 19 sierpnia 2011…). W praktyce banki i instytucje płatnicze działające w Polsce są zobowiązane do stosowania wieloskładnikowego uwierzytelnienia m.in. w logowaniu do bankowości internetowej i mobilnej oraz podczas autoryzacji płatności[52].

Na podstawie obserwacji rynku usług finansowych oraz analizy cytowanej literatury przedmiotu można zaproponować wykaz metod uwierzytelnienia stosowanych w systemach bankowych w Europie.

Czynniki wiedzy są to najstarsze i najpowszechniejsze metody uwierzytelnienia, polegające na znajomości określonych informacji:

- hasła – tradycyjnego statycznego hasła, najczęściej wykorzystywanego w procesach logowania,
- PIN-u – używanego w terminalach kartowych i w aplikacjach mobilnych, będącego również hasłem statycznym,
- odpowiedzi na pytania bezpieczeństwa – często stosowanych jako metoda uzupełniająca,
- hasła jednorazowego przesyłanego e-mailem,
- klucza prywatnego – w przypadku podpisów cyfrowych.

Czynniki posiadania potwierdzają dostęp do fizycznego urządzenia lub obiektu, do którego tylko użytkownik powinien mieć dostęp:

- token sprzętowy – urządzenie generujące hasła jednorazowe, najczęściej dodatkowo zabezpieczone hasłem,
- SMS OTP (*One-Time Password*) – ciąg znaków wysyłany na zarejestrowany numer telefonu,
- TOTP (*Time-based One-Time Password*) – hasło generowane w aplikacji mobilnej,
- powiadomienie *push* generowane przez aplikację mobilną,
- kod QR – jednorazowy kod graficzny skanowany przez dedykowaną aplikację,
- karta chipowa + czytnik,
- klucz sprzętowy NFC, często dodatkowo zabezpieczony biometrią.

Czynniki charakterystyczne dla użytkownika odpowiadają za uwierzytelnienie oparte na cechach fizjologicznych lub behawioralnych:

- rozpoznawanie twarzy,
- odcisk palca,
- rozpoznawanie głosu,

[52] Warto zauważyć, że praktyka implementacji silnego uwierzytelnienia w Polsce jest różna w różnych bankach. Niektóre zastosowały nowe regulacje w sposób dosłowny, inne próbują za wszelką cenę „ułatwiać" proces użytkownikom końcowym. Pomijając szczegółowe analizy takich rozwiązań, jak zaufane urządzenie, zdrapki z hasłami jednorazowymi czy pomijanie SCA przy logowaniu, wszystkie je należy jednoznacznie określić jako wadliwe. Niestety, praktyka bankowa pokazuje także niepełność integracji koncepcji SCA z procesami związanymi z płatnościami kartami.

- biometria behawioralna – analiza sposobu pisania, nawigacji, naciskania klawiszy, wykorzystywana w systemach ciągłego uwierzytelnienia (*continuous authentication*).

Czynniki pomocnicze:

- geolokalizacja – lokalizacja urządzenia jako sygnał potencjalnego naruszenia bezpieczeństwa,
- czas dostępu, urządzenie, przeglądarka, adres IP,
- biometria pasywna – wykrywanie nietypowego zachowania użytkownika.

Współczesne podejście do uwierzytelniania użytkownika w systemach cyfrowych, zwłaszcza w sektorze fintech, ewoluuje w kierunku eliminacji tradycyjnych haseł statycznych jako podstawowego środka zabezpieczeń. Choć jeszcze do niedawna były one uznawane za standardowy element procesu logowania, obecnie coraz częściej traktuje się je jako niewystarczające. W konsekwencji hasła statyczne stają się jedynie komponentem uzupełniającym lub wręcz rezydualnym w całościowej strategii uwierzytelnienia. Dążenie do tzw. bezhasłowej przyszłości ma już odzwierciedlenie w implementacjach takich rozwiązań, jak WebAuthn, FIDO2 czy *passkeys* – standardach wspieranych przez FIDO Alliance[53] i World Wide Web Consortium (W3C). Celem tych inicjatyw jest całkowita eliminacja konieczności zarządzania hasłami przez użytkowników przy jednoczesnym zwiększeniu poziomu bezpieczeństwa i użyteczności systemów.

Różnorodność implementacji mechanizmów spełniających wymogi silnego uwierzytelniania użytkownika, choć na pierwszy rzut oka wydaje się korzystna z perspektywy użytkownika końcowego, w rzeczywistości może mieć poważne konsekwencje dla bezpieczeństwa systemów teleinformatycznych w sektorze finansowym. Zjawisko to wynika w dużej mierze z konkurencyjnej dynamiki rynku, na którym banki oraz inne instytucje finansowe starają się wyróżniać przez wdrażanie autorskich, często uproszczonych pod względem interfejsowym, rozwiązań uwierzytelniających. W rezultacie powstają systemy, których założenia kładą nacisk na użyteczność i doświadczenie użytkownika, kosztem odporności na zaawansowane wektory ataków, takich jak *phishing*, *man-in-the-middle* czy *malware* ukierunkowany na dane uwierzytelniające[54]. Kompromis między użytecznością a bezpieczeństwem jest od dawna ważnym wątkiem analizowanym przez literaturę przedmiotu. Już na początku ery bankowości internetowej wskazywano negatywny wpływ tego zjawiska, podkreślając, że uproszczone metody uwierzytelniania, choć bardziej przyjazne użytkownikowi, mogą sprzyjać powstawaniu nowych luk bezpieczeństwa (Jakobsson i Myers, 2006, s. 241 i n.). Ponadto badania wskazują, że brak interoperacyjności pomiędzy rozwiązaniami różnych dostawców zwiększa podatność systemów na błędy implementacyjne oraz utrudnia

[53] FIDO (Fast Identity Online) to stowarzyszenie branżowe i jednocześnie nazwa koncepcji ukierunkowanej na zmniejszenie – być może docelowo wyeliminowanie – zakresu wykorzystywania haseł statycznych jako narzędzi uwierzytelnienia.

[54] Ważnym, a często niezauważanym aspektem tego zjawiska jest również brak konsekwencji w kreowaniu świadomości informatycznej użytkowników. Problem ten zostanie opisany w rozdziale 3.3.

tworzenie jednolitych standardów w zakresie audytu i zgodności z regulacjami, takimi jak dyrektywa PSD2 (Gounari i in., 2024). W konsekwencji rozdrobnienie krajobrazu uwierzytelnienia może prowadzić do fragmentaryzacji środowiska bezpieczeństwa cyfrowego, w którym nawet najlepsze praktyki są trudne do ustandaryzowania i egzekwowania. Dlatego też w literaturze coraz częściej postuluje się potrzebę harmonizacji oraz opracowania dla mechanizmów silnego uwierzytelniania uniwersalnych ram referencyjnych, które uwzględniałyby zarówno aspekty ergonomiczne, jak i wymagania bezpieczeństwa na poziomie systemowym (Pool i Venter, 2022).

Na zakończenie rozważań nad problematyką silnego uwierzytelnienia warto poddać krytycznej analizie niektóre z jego praktycznych implementacji. Analiza jakości tego typu rozwiązań powinna uwzględniać teoretyczną poprawność zastosowanych algorytmów, protokołów i metod oraz podatność na zagrożenia wykorzystujące aspekty pozatechniczne, w tym głównie ataki phishingowe, nie powinna natomiast brać pod uwagę aspektów związanych z łatwością użytkowania, wygodą użytkownika czy niskim kosztem implementacji. Ich uwzględnienie spowodowałoby bowiem sprowadzenie analizy do poszukiwania kompromisów, a nie rozwiązań najlepszych z punktu widzenia oferowanego poziomu bezpieczeństwa. Biorąc to pod uwagę, należy stwierdzić, że do grupy rozwiązań typu SCA gwarantujących akceptowalny poziom cyberbezpieczeństwa można zaliczyć połączenie statycznego hasła z:

- hasłami jednorazowymi wysyłanymi równolegle na adres e-mail oraz telefon komórkowy,
- tokenem programowym lub sprzętowym zabezpieczonym hasłem dostępu.

Dodatkowe zastosowanie klucza NFC pozwala podwyższyć poziom bezpieczeństwa z akceptowalnego do wysokiego. Pojawia się jednocześnie pytanie: czy tak popularne ostatnio metody biometryczne również powinny zostać dodane do powyższego zestawienia?

Biometria jest nauką zajmującą się badaniem zmienności organizmów, a także nazwą technologii identyfikacji osób na podstawie unikalnych cech fizycznych lub behawioralnych, takich jak odciski palców, geometria twarzy, głos czy dynamika pisania. Zastosowanie biometrii w instytucjach finansowych pierwotnie stanowiło wartość dodaną, zwiększającą odporność systemów na ataki phishingowe czy spoofingowe oraz kradzież tożsamości. Dziś także podkreśla się w badaniach te właśnie elementy (Ramesh i in., 2025). W szczególności biometria behawioralna, jak wykazali Alvarez i in. (2024), okazuje się wyjątkowo skuteczna w odpieraniu nowoczesnych zagrożeń, takich jak *deepfake* i w procesach zdalnej weryfikacji tożsamości. Integracja sztucznej inteligencji z technologiami biometrycznymi znacznie poszerza ich zastosowanie w procesach onboardingu klientów oraz weryfikacji transakcji w czasie rzeczywistym (Manwani, 2025). W literaturze przedmiotu można znaleźć bardzo dużo pozytywnych wyników badań i analiz dotyczących zastosowań biometrii w mechanizmach bezpieczeństwa, głównie w bankowości internetowej i mobilnej. Badacze podkreślają jej potencjał w kontekście zwiększania odporności systemów informatycznych na nie-

autoryzowany dostęp, a także wzmocnienia zaufania klientów do usług finansowych (Waliullah i in., 2025). Praktyka implementacji metod biometrycznych nakazuje jednak bardziej krytyczne spojrzenie na ten problem. Pomimo szerokiego zastosowania biometria nie jest pozbawiona istotnych ograniczeń implementacyjnych oraz funkcjonalnych. W literaturze zwraca się uwagę na ograniczenia związane z niezawodnością mechanizmów biometrycznych w zmiennych warunkach środowiskowych, takich jak m.in. słabe oświetlenie czy hałas, a także zmiany fizjonomii użytkownika (Hammad, 2024). Problemy te szczególnie nasilają się w przypadku biometrii twarzy i głosu, co czyni je nieoptymalnymi w roli jedynego czynnika uwierzytelniającego. Jak wykazali Chitrakar i in. (2024), aż 46% respondentów zgłaszało problemy z dokładnością i stabilnością działania systemów biometrycznych w mobilnych aplikacjach bankowych, wskazując konieczność ich uzupełniania dodatkowymi metodami weryfikacji. Ten problem wydaje się szczególnie ważny. Jeżeli jeden z elementów silnego uwierzytelnienia musi być uzupełniany innym, to powstaje kluczowe pytanie o zasadność jego stosowania. Jednym z powszechnie obserwowanych przykładów ograniczeń funkcjonalnych systemów biometrycznych jest mechanizm odblokowywania urządzeń mobilnych przez rozpoznawanie twarzy lub odcisku palca. W przypadku niepowodzenia w pomiarze biometrycznym system domyślnie uruchamia procedurę zapasową – zazwyczaj w postaci prośby o wprowadzenie kodu PIN lub hasła. Taki scenariusz ujawnia istotny problem: choć biometria ma pełnić funkcję pierwotnego strażnika bezpieczeństwa, to w praktyce jej zawodność powoduje, że funkcję decydującą przejmuje czynnik wiedzy. Tym samym metoda biometryczna nie wnosi wartości dodanej w sensie wzmocnienia modelu bezpieczeństwa – nie jest bowiem niezbędna do uzyskania dostępu. Stawia to potężny znak zapytania przy potencjalnej roli biometrii w świecie bezhasłowym. Co więcej, jak wskazują badania Mecke'ego i in. (2024), wprowadzenie biometrii jako podstawowego mechanizmu uwierzytelniającego może tworzyć iluzję zwiększonego bezpieczeństwa, przy jednoczesnym obniżeniu czujności użytkownika i braku faktycznego zwiększenia poziomu ochrony. Paradoks ten pogłębia się, gdy urządzenia mobilne pozwalają na wielokrotne próby odczytu biometrycznego bez ograniczeń czasowych, co w połączeniu z możliwością przejścia do uwierzytelniania alternatywnego zwiększa wektor potencjalnych ataków. Co istotne, mechanizmy biometryczne są podatne na tzw. *fallback vulnerabilities*, tj. luki wynikające z obecności alternatywnego sposobu logowania, który nierzadko ma niższy poziom zabezpieczeń niż system biometryczny. Liao (2024) wskazuje, że w testach penetracyjnych urządzeń mobilnych stosujących biometrię twarzy możliwe było odtworzenie dostępu do urządzenia za pomocą zdjęcia użytkownika, a po niepowodzeniu – zastosowanie prostych, czterocyfrowych kodów PIN. W takiej konfiguracji system biometryczny nie tylko nie spełnia swojej funkcji ochronnej, ale wręcz osłabia percepcję realnego zagrożenia i sprzyja nadmiernemu poleganiu na zawodnym algorytmie. W konsekwencji, zamiast wzmacniać poziom ochrony, systemy biometryczne w konfiguracji zezwalającej na przejście do tradycyjnego uwierzytelnienia w przypadku błędu mogą prowadzić do zjawiska zwanego *false sense of security*, co może mieć istotne implikacje w kontekście projektowania systemów bezpieczeństwa w sektorze

finansowym. Z tych względów coraz częściej postuluje się stosowanie biometrii wyłącznie jako elementu uwierzytelniania wieloskładnikowego, a nie jako autonomicznego mechanizmu bezpieczeństwa. Rozwijane są również nowoczesne mechanizmy przetwarzania danych biometrycznych lokalnie na urządzeniach użytkowników (Fiore i in., 2025), a także hybrydowe modele uwierzytelniania łączące różne typy biometrii i klasyczne metody (Adil i in., 2025).

Podsumowując, można stwierdzić, że krytyczna analiza literatury oraz doświadczenia praktyczne związane z systemami biometrycznymi funkcjonującymi obecnie podważają zasadność traktowania biometrii jako kluczowego elementu architektury bezpieczeństwa.

3.3. Edukacja i świadomość informatyczna

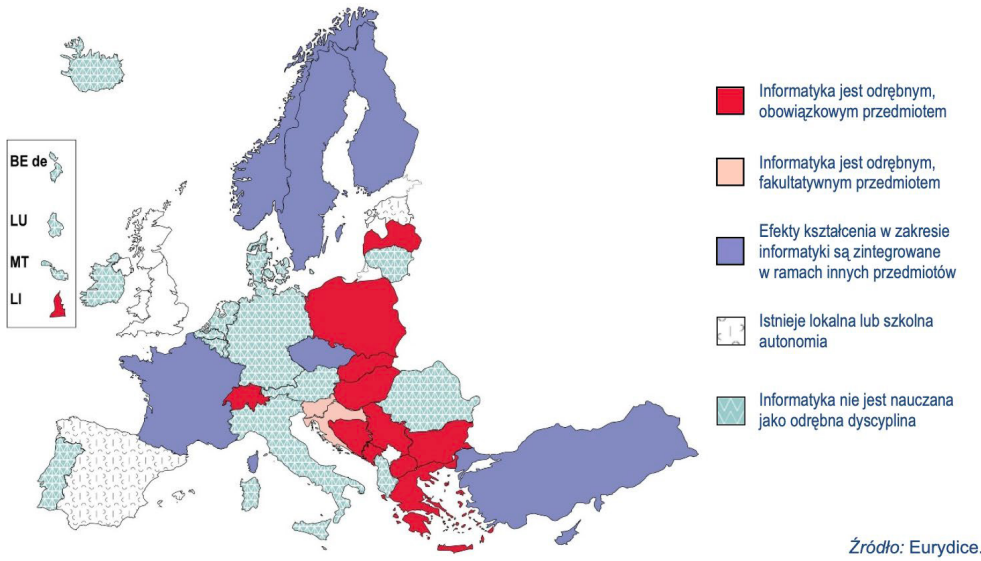
Współczesna transformacja cyfrowa, której rytm i dynamikę wyznaczają innowacje technologiczne, redefiniuje pojęcie kompetencji nie tylko zawodowych, ale także obywatelskich. W społeczeństwie informacyjnym[55] umiejętność efektywnego i bezpiecznego korzystania z technologii staje się równie istotna jak podstawowa umiejętność czytania czy pisania. Edukacja informatyczna, rozumiana szeroko jako proces nabywania wiedzy i umiejętności z zakresu technologii informacyjno-komunikacyjnych, nie ogranicza się już wyłącznie do środowisk akademickich czy specjalistycznych – staje się fundamentem funkcjonowania w każdym sektorze, ze szczególnym uwzględnieniem sektora finansowego. Co ciekawe, tak wydawałoby się oczywisty aspekt edukacyjny jest bardzo różnie postrzegany w państwach Unii Europejskiej. Na rysunku 2 przedstawiono umiejscowienie informatyki w procesie edukacji podstawowej w krajach europejskich.

Współczesne kompetencje cyfrowe obejmują jednak znacznie większy merytorycznie obszar niż tylko umiejętność obsługi komputera. Są to złożone zestawy wiedzy, postaw i zachowań, umożliwiających skuteczne, krytyczne i bezpieczne korzystanie z technologii cyfrowych. Unia Europejska, wprowadzając ramy DigComp (*Digital Competence Framework*) (Vuorikari i in., 2022)[56], usystematyzowała te kompetencje w pięciu głównych obszarach: informacji i danych, komunikacji i współpracy, tworzenia treści cyfrowych, bezpieczeństwa oraz rozwiązywania problemów.

---

[55] Wśród najczęściej przytaczanych definicji tego ważnego pojęcia znajduje się ta, która mówi, że jest to społeczeństwo znajdujące się na takim etapie rozwoju, na którym osiągnięty poziom techniki informatyczno-telekomunikacyjnej stwarza warunki techniczne, ekonomiczne i edukacyjne do wykorzystywania informacji w produkcji wyrobów i świadczeniu usług. Często podkreśla się także znaczenie informacji jako dobra niematerialnego, równoważnego dobrom materialnym lub nawet cenniejszego od nich.

[56] Dokument ten, opracowany przez Komisję Europejską, stanowi jedno z kluczowych narzędzi kształtowania edukacji informatycznej w Europie. Jego wdrożenie powinno wpłynąć na aktualizację podstaw programowych, rozwój narzędzi dydaktycznych oraz systemy oceny umiejętności cyfrowych, przyczyniając się tym samym do bardziej świadomego i bezpiecznego korzystania z technologii cyfrowych przez uczniów i nauczycieli.



Rys. 2. Informatyka jako przedmiot w szkołach podstawowych w Europie

Źródło: (Komisja Europejska/Europejska Agencja Wykonawcza ds. Edukacji i Kultury/Eurydice, 2024, s. 24).

W kontekście cyberbezpieczeństwa szczególne znaczenie mają te aspekty edukacji, które uczą identyfikowania zagrożeń, ochrony prywatności, rozpoznawania prób manipulacji informacją czy bezpiecznego zarządzania tożsamością cyfrową. Dobrze zaprojektowana edukacja informatyczna – prowadzona zarówno na poziomie instytucjonalnym, jak i przez nieformalne formy kształcenia – może znacząco wpłynąć na redukcję ryzyka informatycznego w skali kraju, w tym również związanego z działalnością cyberprzestępczą. Wynika to z tego, że edukacja kształtuje nie tylko indywidualne umiejętności techniczne, lecz także ogólne kompetencje analityczne, poznawcze oraz społeczne, które są kluczowe w identyfikowaniu i właściwym reagowaniu na zagrożenia cyfrowe. W szerszym ujęciu upowszechnianie wiedzy z zakresu cyberbezpieczeństwa wpływa na wzrost odporności cyfrowej całych społeczności i organizacji, sprzyjając budowie kultury bezpieczeństwa opartej na świadomości, odpowiedzialności oraz zdolności adaptacyjnej. Na poziomie krajowym takie działania mogą się przekładać na zmniejszenie skuteczności masowych ataków socjotechnicznych, ograniczenie sukcesów kampanii phishingowych czy zminimalizowanie liczby incydentów związanych z nieautoryzowanym dostępem do systemów. Edukacja prowadzona w sposób skoordynowany – z udziałem szkół, uczelni, instytucji publicznych i sektora prywatnego – powinna tworzyć zintegrowany ekosystem obrony, w którym obywatel nie jest wyłącznie biernym użytkownikiem technologii, lecz aktywnym uczestnikiem procesów bezpieczeństwa. Taka transformacja społeczna ma fundamentalne znaczenie w sektorach wrażliwych, takich jak finanse, gdzie nawet pojedynczy błąd użytkow-

nika może prowadzić do olbrzymich strat oraz poważnych konsekwencji prawnych i reputacyjnych. Warto zauważyć również, że brak odpowiednich kompetencji cyfrowych nie jest wyłącznie problemem indywidualnym. Przekłada się on bezpośrednio na podatność całych instytucji na ataki socjotechniczne, błędy użytkowników czy nieświadome łamanie zasad bezpieczeństwa. Z tego względu rola edukacji informatycznej zyskuje coraz większe uznanie nie tylko w strategiach organizacyjnych, ale także w politykach publicznych, gdzie budowa odporności cyfrowej społeczeństwa jest traktowana jako jedno z priorytetowych zadań. W epoce wszechobecnej cyfryzacji użytkownik końcowy coraz częściej staje się pierwszą linią obrony – lub przeciwnie, pierwszym ogniwem podatnym na cyberatak. Z tego powodu pojęcie świadomości informatycznej (*security awareness*) nabiera szczególnego znaczenia. O ile edukacja informatyczna buduje fundament kompetencyjny, o tyle świadomość informatyczna dotyczy przede wszystkim postaw, nawyków oraz gotowości do rozpoznawania i reagowania na zagrożenia związane z korzystaniem z technologii. Pojęcie świadomości informatycznej nie jest jednoznaczne. Jego pierwszy człon odnosi się bowiem do bardzo wielu zjawisk rozumianych w sposób potoczny lub metaforyczny[57]. Wśród prób stworzenia uniwersalnej definicji na uwagę zasługuje propozycja ENISA (2018), zgodnie z którą świadomość informatyczna to zdolność użytkownika do rozpoznawania zagrożeń informatycznych, rozumienia ich potencjalnych skutków oraz podejmowania odpowiednich działań ochronnych w środowisku cyfrowym. Ważniejsze od terminologii jest w tym wypadku zrozumienie wagi i znaczenia połączenia kompetencji, postaw oraz nawyków w triadę stanowiącą najważniejszą linię obrony przed zagrożeniami bezpieczeństwa informatycznego. Podejście takie nie ogranicza się do wiedzy o istnieniu zagrożeń – obejmuje również zdolność do przewidywania skutków własnych działań w środowisku cyfrowym, unikania ryzykownych zachowań oraz stosowania podstawowych zasad cyberhigieny. Wspomnianą triadę scharakteryzowano w tabeli 10.

Zestawienie z tabeli 10 nie ma być oczywiście kompleksowym ujęciem ogółu problemów bezpieczeństwa informatycznego. Nie można bowiem oczekiwać od wszystkich użytkowników wiedzy specjalistycznej. Należy natomiast dążyć do stanu, w którym konsekwentnie budowana świadomość będzie elementem stale podnoszącym poziom bezpieczeństwa pracy z komputerem, w szczególności pracy z danymi wrażliwymi i wykonywania transakcji elektronicznych. Badania wskazują, że nawet podstawowe braki w świadomości użytkowników mogą prowadzić do poważnych incydentów. W kontekście sektora finansowego, gdzie interakcje użytkownika z systemem odbywają się często bez pośrednictwa specjalisty, znaczenie świadomego użytkownika wzrasta wielokrotnie. Cyberprzestępcy nie muszą już atakować bezpośrednio systemów informatycznych instytucji – wystarczy, że oszukają klienta, skłaniając go do nieświadomego udostępnienia parametrów dostępu. Wyniki badań związanych z problematyką cyberbezpieczeństwa oraz wpływającymi na nią zagad-

[57] Odniesienie do psychologii potocznej jest w tym wypadku bardzo istotne.

nieniami świadomości informatycznej użytkowników nie są często spotykane w literaturze przedmiotu. Specyfika problemu nie ułatwia publikowania wyników badań, a powszechnie wykonywane analizy i testy wewnętrzne różnych instytucji pozostają z oczywistych względów niejawne.

Tabela 10. Triada świadomości informatycznej

Kategoria główna	Podkategorie
Kompetencje – oznaczają zestaw umiejętności poznawczych, operacyjnych i decyzyjnych, które umożliwiają użytkownikowi skuteczne funkcjonowanie w środowisku cyfrowym	● wiedza – znajomość podstawowych zasad opisujących działanie mechanizmów bezpieczeństwa informatycznego, takich jak algorytmy i protokoły kryptograficzne oraz metody kontroli dostępu ● identyfikacja zagrożeń – zdolność do rozpoznawania potencjalnych ataków ● prywatność i ochrona danych osobowych – znajomość zasad ochrony danych osobowych, zarządzania ustawieniami prywatności i mechanizmów autoryzacji ● zarządzanie tożsamością – umiejętność posługiwania się różnymi tożsamościami cyfrowymi i zabezpieczania danych uwierzytelniających
Postawy i nawyki – determinują codzienne zachowania użytkowników w środowisku cyfrowym. Są to elementy silnie zakorzenione w praktyce i trudno podatne na krótkoterminową zmianę	● rozpoznawanie phishingu ● stosowanie silnych haseł, różnych dla różnych systemów ● aktualizacja oprogramowania ● bezpieczne połączenia – stosowanie sieci VPN, unikanie publicznych sieci Wi-Fi do operacji poufnych
Przeciwdziałanie zagrożeniom – prewencja i ochrona	● cyberhigiena – codzienne nawyki cyfrowe, które minimalizują ryzyko ataków, analogiczne do higieny zdrowotnej ● zmęczenie informacyjne – psychologiczne zjawisko polegające na obniżonej percepcji ryzyka w wyniku przesytu komunikatów ostrzegawczych, znane też jako *security fatigue* (Boss i in., 2015) ● ochrona przed socjotechniką – rozpoznawanie prób manipulacji psychologicznej ● kultura bezpieczeństwa – system wartości i norm promujących odpowiedzialne zachowania w organizacjach, oparty na zasadzie współdzielonej odpowiedzialności

Źródło: opracowanie własne na podstawie (Vuorikari i in., 2022).

Dalej przedstawiono próbę przeglądu dostępnych, możliwie aktualnych wyników badań, istotnych dla omawianego zagadnienia. Analizie poddano sześć wartościowych badań empirycznych oraz przeglądów systematycznych, które spełniały następujące kryteria: europejski zakres geograficzny, skupienie na użytkownikach indywidualnych, uwzględnienie świadomości informatycznej oraz znaczna zawartość danych empirycznych. Szczegółowe zestawienie wyników przedstawiono w tabeli 11.

Tabela 11. Syntetyczne zestawienie analizy wyników badań nad poziomem świadomości informatycznej użytkowników systemów informatycznych

Pozycja literatury	Zasięg geograficzny	Wnioski dotyczące poziomu świadomości informatycznej
Yarovenko i in., 2023	35 państw europejskich	Użytkownicy z Danii, Holandii, Islandii, Norwegii, Wielkiej Brytanii, Austrii i Finlandii byli najbardziej odpowiedzialnymi Europejczykami pod względem bezpieczeństwa informatycznego, podczas gdy osoby z Bułgarii, Rumunii, Serbii, Albanii, Macedonii Północnej oraz Bośni i Hercegowiny wykazywały najmniejszą dbałość o ochronę
Zwilling i in., 2022	Izrael, Słowenia, Polska, Turcja	Wyniki pokazują, że użytkownicy Internetu mają odpowiednią świadomość zagrożeń cybernetycznych, jednak stosują jedynie minimalne środki ochrony, zazwyczaj dość powszechne i proste
Zamfirescu i in., 2019	państwa Unii Europejskiej	Istnieje znaczna zmienność wśród użytkowników, na poziomie zarówno indywidualnym, jak i społecznym, w zakresie intensywności aktywności cyfrowej, doświadczeń związanych z cyberatakami, stosowania środków zapobiegawczych oraz troski o bezpieczeństwo
Szumski, 2018	studenci Uniwersytetu Warszawskiego	Badania wykazały, że Internet oraz znajomi i koledzy z pracy są głównymi źródłami wiedzy o cyberbezpieczeństwie w badanej grupie. Na tej podstawie autor uzyskał dowody, że takie praktyki są wadliwe i prowadzą do niewłaściwych wzorców zachowań w zakresie zarówno korzystania z Internetu, jak i ochrony haseł. Badania pokazały również, że studenci wskazują brak wiarygodnych źródeł informacji o cyberbezpieczeństwie

Źródło: opracowanie własne na podstawie cytowanej literatury.

Z przedstawionych w tabeli 11 wyników oraz krytycznej analizy publikacji źródłowych można wyciągnąć następujące wnioski:

- najwyższy poziom świadomości informatycznej występuje w krajach Europy Północnej (Dania, Finlandia, Islandia), a najniższy w regionach Europy Południowo-Wschodniej,
- wciąż dominuje stosowanie jedynie podstawowych środków bezpieczeństwa (np. hasła), mimo znajomości bardziej zaawansowanych rozwiązań,
- poważnym problemem jest wyraźna rozbieżność między wiedzą o zagrożeniach a rzeczywistymi praktykami użytkowników.

W świetle cytowanych badań świadomość informatyczna nie może być sprowadzona wyłącznie do deklaratywnej wiedzy użytkownika o zagrożeniach cybernetycznych. Jak już wspomniano, równie istotne – a często kluczowe – są postawy, nawyki, kanały pozyskiwania wiedzy oraz zdolność do przekładania wiedzy na konkretne działania

ochronne. W tym kontekście szczególnie widoczna jest luka między poziomem deklarowanej wiedzy a realnymi zachowaniami użytkowników (*awareness-behaviour gap*) usług bankowości online i mobilnej. Jest ona stosunkowo najlepiej udokumentowanym zjawiskiem, a polega na tym, że użytkownicy mimo deklarowanej znajomości zagrożeń i zasad bezpiecznego korzystania z systemów rzadko przekładają tę wiedzę na praktykę. Zwilling i in. (2022) wykazali, że większość respondentów w czterech analizowanych krajach (Izraelu, Słowenii, Polsce i Turcji) zna podstawowe zagrożenia, takie jak *phishing* czy kradzież tożsamości, ale nie stosuje podstawowych zabezpieczeń, takich jak uwierzytelnianie wieloskładnikowe czy programy do zarządzania hasłami. Badania Yarovenko i in. (2023), obejmujące aż 35 państw europejskich, potwierdzają tę tendencję: nawet w krajach o stosunkowo wysokim poziomie wiedzy (np. Finlandii, Danii, Holandii) wielu użytkowników ogranicza się do stosowania prostych haseł i nie korzysta z oferowanych przez banki bardziej zaawansowanych środków ochrony, takich jak tokeny, biometria czy e-ID. Wspomniana luka często tłumaczona jest m.in. modelem *Protection Motivation Theory*, który wskazuje, że sam poziom zagrożenia nie jest wystarczającym motywatorem – istotne są także poczucie sprawczości oraz percepcja użyteczności danego środka (Ifinedo, 2012).

Kolejnym istotnym problemem w budowaniu świadomości informatycznej użytkowników jest struktura źródeł, z których czerpią oni wiedzę na temat zagrożeń i metod ochrony. Jak wykazał Szumski (2018), młodzi dorośli – w tym studenci – najczęściej uczą się o cyberzagrożeniach z Internetu, forów internetowych lub od rówieśników. Formalne programy edukacyjne, szkolenia prowadzone przez banki czy instytucje edukacyjne odgrywają marginalną rolę. Konsekwencją jest często fragmentaryczna wiedza, brak umiejętności jej zastosowania oraz utrwalanie mitów lub błędnych przekonań, np. że antywirus „wystarczy" do zabezpieczenia konta bankowego. Istotnym zagadnieniem jest także zbyt małe wykorzystanie dostępnych narzędzi ochrony, mimo ich skuteczności i dostępności. Pomimo dostępności zaawansowanych metod autoryzacji – takich jak uwierzytelnianie dwuskładnikowe, tokeny sprzętowe, biometria czy certyfikaty elektroniczne – użytkownicy nie chcą z nich korzystać. Badania Yarovenko pokazują, że w regionach o wyższym wskaźniku cyberprzestępczości użytkownicy rzeczywiście stosują więcej środków ochronnych, jednak nawet tam wykorzystanie zaawansowanych rozwiązań pozostaje selektywne. Badania literaturowe Grigorescu i in. (2023) nad konwergencją zachowań bankowych w państwach UE potwierdzają, że użytkownicy adaptują technologie elektroniczne szybciej niż zasady bezpieczeństwa, co prowadzi do wzrostu ryzyka. Nawet w państwach wysoko rozwiniętych, takich jak Niemcy czy Szwecja, wiele osób nie korzysta regularnie z aktualizacji, ignoruje komunikaty ostrzegawcze i opiera się wyłącznie na loginie i haśle, często używanym również w innych systemach. W literaturze z zakresu psychologii bezpieczeństwa wskazuje się również, że użytkownicy nie stosują zabezpieczeń nie dlatego, że nie chcą, ale często dlatego, że nie rozumieją ich działania lub uważają je za uciążliwe (Hadlington, 2017). Dla skuteczności działań prewencyjnych kluczowe są zatem uproszczenie interfejsów, automatyzacja ochrony oraz edukacja pokazująca realną

wartość zabezpieczeń. W analizowanych badaniach wyraźnie zaznaczają się różnice geograficzne i kulturowe w zakresie zarówno deklarowanej wiedzy, jak i praktycznych zachowań związanych z bezpieczeństwem. Oznacza to, że obecność programów edukacyjnych na poziomie szkół podstawowych i średnich oraz wsparcie instytucjonalne są bardzo ważnymi elementami wpływającymi na świadomość informatyczną. Należy także zauważyć, że różnice te mogą być wynikiem braku zaufania do instytucji publicznych oraz niekonsekwentnego wdrażania regulacji unijnych, takich jak RODO czy PSD2, w praktyce bankowej. Wnioski te korespondują z koncepcją kultury bezpieczeństwa informacyjnego, która zakłada, że odpowiedzialne zachowania nie są wynikiem jednorazowej edukacji, lecz efektem długotrwałej pracy nad wartościami, normami i procedurami w społeczeństwie (ENISA, 2018).

Wyniki badań wskazują cztery główne obszary problemowe:

- świadomość informatyczna współczesnego społeczeństwa jest stosunkowo duża, ale niewystarczająca do zapewnienia wysokiego poziomu ochrony bez odpowiedniego wsparcia edukacyjnego i instytucjonalnego,
- użytkownicy systemów bankowości internetowej i mobilnej często polegają na niesprawdzonych źródłach wiedzy, co prowadzi do niskiej jakości decyzji dotyczących bezpieczeństwa,
- zaawansowane narzędzia ochrony są dostępne, ale marginalnie wykorzystywane z powodu braku zrozumienia lub postrzegania ich jako niepotrzebnych,
- występują istotne różnice regionalne, które należy uwzględnić w projektowaniu programów edukacyjnych i interfejsów bezpieczeństwa.

Współczesna dyskusja nad zagadnieniami świadomości informatycznej wykracza daleko poza kwestie informatyczne. Coraz częściej pojawia się w niej pojęcie alfabetyzmu bezpieczeństwa (*security literacy*) użytkowników końcowych. Wielu autorów argumentuje, że skuteczne wdrożenie narzędzi ochronnych wymaga ich projektowania w sposób zrozumiały, dostępny i intuicyjny dla wszystkich grup społecznych. Wśród filarów alfabetyzmu bezpieczeństwa najczęściej wymienia się (Naqvi i in., 2025):

- wiedzę na temat różnych technologii i mechanizmów,
- wiedzę na temat zagrożeń dla systemów,
- wiedzę na temat swojej roli w systemie,
- wiedzę na temat prawnych i etycznych implikacji systemu,
- umiejętność stosowania zaleceń i praktyk bezpieczeństwa,
- umiejętność rozumienia złośliwych intencji,
- umiejętność podejmowania decyzji opartych na wartościach.

Wnioskiem z przedstawionych analiz może być stwierdzenie mówiące o tym, że mimo rosnącej świadomości zagrożeń cyfrowych istnieje wyraźna luka między deklarowaną wiedzą a rzeczywistymi działaniami ochronnymi, pogłębiana przez brak

formalnych źródeł edukacji oraz dominację nieformalnych kanałów informacji. Skuteczne przeciwdziałanie zagrożeniom wymaga nie tylko technicznych rozwiązań, lecz przede wszystkim rozwoju alfabetyzmu bezpieczeństwa. Zróżnicowanie regionalne oraz brak integracji wyników badań z praktyką rynkową i edukacyjną wskazują potrzebę systemowego, wielopoziomowego podejścia do budowy globalnej kultury cyberbezpieczeństwa. Ważnym elementem tej kultury powinny być standardy korporacyjne, szczególnie istotne w instytucjach finansowych. Badania pokazują, że jest to jeszcze ciągle obszar wymagający znacznego rozwoju[58].

3.4. Kryptografia i komputery kwantowe

3.4.1. Zastosowania algorytmów kryptograficznych

Współczesne cyberbezpieczeństwo w sposób fundamentalny opiera się na zastosowaniach kryptografii. Mechanizmy kryptograficzne przenikają wszystkie warstwy architektury bezpieczeństwa systemów informatycznych – od zabezpieczania komunikacji sieciowej, poprzez integralność i poufność danych, aż po mechanizmy autoryzacji i uwierzytelniania użytkowników. Nie istnieje dziś obszar praktyki bezpieczeństwa informatycznego, który nie byłby bezpośrednio lub pośrednio uzależniony od skuteczności i odporności stosowanych algorytmów kryptograficznych. Zarówno protokoły bezpieczeństwa warstwy transportowej, jak i systemy zarządzania tożsamością, ochrona danych w spoczynku oraz mechanizmy kontroli dostępu w środowiskach chmurowych – wszystkie te komponenty operują w oparciu o złożone techniki kryptograficzne. W konsekwencji postęp w dziedzinie kryptografii, jak również ewolucja zagrożeń związanych z jej potencjalnymi podatnościami mają bezpośredni wpływ na efektywność całego ekosystemu cyberbezpieczeństwa.

Kryptografią nazywamy naukę o metodach przesyłania wiadomości w zamaskowanej postaci, tak aby tylko odbiorca był w stanie odczytać wysłaną przez nadawcę wiadomość, będąc jednocześnie pewnym, że nie została ona przez nikogo zmodyfikowana. Do zaszyfrowania tekstu jawnego wykorzystuje się algorytm szyfrujący, a do deszyfrowania szyfrogramu – algorytm deszyfrujący[59]. W wyniku szyfrowania po-

[58] Znakomite opracowanie Głównego Urzędu Statystycznego, *Społeczeństwo informacyjne w Polsce w 2024 roku*, prezentuje wiele ciekawych statystyk. Jedna z nich mówi, że w 2024 r. w Polsce jedynie 57% przedsiębiorstw stosowało praktyki mające na celu podnoszenie świadomości pracowników w kwestiach związanych z cyberbezpieczeństwem (GUS, 2024, wykres 57, s. 97).

[59] Analiza polskojęzycznej literatury przedmiotu wskazuje, że synonimem pojęcia „szyfr" (szyfrowanie) jest pojęcie „kod" (kodowanie). Jest to jednak wniosek błędny. Wiele publikacji posługuje się pojęciem kodu w sposób nieprawidłowy. Szyfrowanie jest jedynie szczególnym przypadkiem kodowania. Celem szyfrowania jest zawsze utajnienie komunikatu, podczas gdy przed kodowaniem takiego celu się nie stawia.

wstaje szyfrogram, którego treść można odtworzyć w procesie deszyfrowania. Sztukę łamania szyfrów nazywamy kryptoanalizą, a dziedzinę matematyki obejmującą kryptografię i kryptoanalizę nazywamy kryptologią[60]. W nowoczesnych algorytmach bezpieczeństwo jest zapewniane dzięki stosowaniu klucza. Wyróżnia się dwie grupy algorytmów, w których wykorzystuje się klucze: algorytmy symetryczne i algorytmy asymetryczne. W algorytmach symetrycznych klucze szyfrujący i deszyfrujący są takie same lub jeden jest wyznaczany z drugiego[61]. Przed rozpoczęciem przesyłania wiadomości wymagają one uzgodnienia klucza między nadawcą i odbiorcą[62]. Utrzymanie klucza w tajemnicy jest gwarancją bezpieczeństwa wymiany danych. Całkowicie odmienną grupę stanowią algorytmy asymetryczne, charakteryzujące się tym, że klucz szyfrujący może, a nawet powinien być ujawniony w celu umożliwienia innym osobom szyfrowania wiadomości, której odczytanie możliwe jest jednak tylko dzięki użyciu klucza deszyfrującego (Karbowski, 2008; Welschenbach, 2002).

Współczesna kryptografia wykorzystuje trzy grupy algorytmów: symetryczne, asymetryczne i jednokierunkowe funkcje skrótu. Kryptografia symetryczna, chronologicznie pierwsza w erze komputerowej, odgrywa ważną rolę w sektorze finansowym. Ze względu na efektywność i niewielką złożoność obliczeniową algorytmy symetryczne są szeroko stosowane w szyfrowaniu dużych wolumenów danych – zarówno w bazach danych, jak i w kanałach komunikacyjnych. Algorytmy te mają również zastosowanie w procesach uwierzytelniania użytkowników. W sektorze kart płatniczych, a także w procesach autoryzacji transakcji w czasie rzeczywistym kryptografia symetryczna zapewnia szybkie i bezpieczne przetwarzanie płatności – szczególnie w systemach o wysokich wymaganiach dotyczących przepustowości i niskiego opóźnienia. Najpowszechniejszym obecnie algorytmem symetrycznym jest AES (*Advanced Encryption Standard*), choć nadal w wielu zastosowaniach wykorzystywany jest 3DES.

Algorytmy kryptografii asymetrycznej, których bezpieczeństwo opiera się na trudności problemów matematycznych o wysokiej złożoności obliczeniowej, takich jak faktoryzacja dużych liczb czy obliczenie logarytmu dyskretnego w grupach skończonych, pełnią kluczową funkcję w architekturze bezpieczeństwa współczesnego sektora finansowego. Ich zastosowanie ma charakter dwojaki: z jednej strony umożliwiają bezpieczną dystrybucję kluczy kryptograficznych w środowiskach otwartych, z drugiej zaś zapewniają mechanizmy podpisu cyfrowego, niezbędne do weryfikacji integralności oraz autentyczności informacji. Do najczęściej implementowanych w praktyce algorytmów asymetrycznych należą RSA (*Rivest-Shamir-Adleman*) oraz ECDSA (*Elliptic Curve Digital Signature Algorithm*). W systemach bankowych i finansowych kryptografia asymetryczna stanowi fundament procesu inicjalizacji bezpiecz-

[60] Matematyczne podstawy kryptografii znakomicie prezentuje Koblitz (1995, 2000).

[61] Szczegółowy opis najpopularniejszych algorytmów symetrycznych znaleźć można m.in. w: (Menezes i in., 2005; Pieprzyk i in., 2003; Schneier, 1995).

[62] Jest to przyczyną istnienia tzw. problemu dystrybucji klucza, który skutecznie utrudnia praktyczne implementacje algorytmów symetrycznych w ich klasycznej postaci.

nych kanałów komunikacyjnych. Najpowszechniejszym przykładem jest protokół *Transport Layer Security* (TLS), w którym algorytmy asymetryczne są wykorzystywane do bezpiecznej wymiany kluczy sesyjnych, po której następuje szyfrowanie transmisji za pomocą wydajnych algorytmów symetrycznych. Równocześnie mechanizmy podpisu cyfrowego odgrywają zasadniczą rolę w zapewnieniu cech niepodważalności (*non-repudiation*), integralności oraz autentyczności transakcji i dokumentów w systemach finansowych. Podpisy cyfrowe wykorzystywane są m.in. w procesach autoryzacji przelewów bankowych, podpisywaniu elektronicznych kontraktów, a także w systemach rozrachunkowych oraz hurtowej obsłudze transakcji finansowych. Dzięki temu możliwe jest budowanie zaufania w środowiskach transakcyjnych, które w coraz większym stopniu funkcjonują w przestrzeni cyfrowej i rozproszonej.

Jednokierunkowe funkcje skrótu, charakteryzujące się trudnością odtworzenia danych wejściowych na podstawie ich wartości oraz odpornością na kolizje, stanowią fundamentalny mechanizm w obszarze zarządzania danymi uwierzytelniającymi, zwłaszcza hasłami dostępu. Ich zastosowanie umożliwia przechowywanie informacji w sposób, który minimalizuje ryzyko kompromitacji w przypadku nieautoryzowanego dostępu do zasobów bazodanowych. Funkcje te wykorzystywane są również w połączeniu z technikami wzmacniającymi odporność na ataki słownikowe i siłowe, takimi jak *salting*, *peppering* oraz iteracyjne funkcje kluczopochodne, co stanowi istotny element współczesnych polityk bezpieczeństwa haseł. Ostatnio znaczenie funkcji skrótu znacznie wzrosło w kontekście technologii *blockchain*, gdzie odgrywają one kluczową rolę w zapewnianiu integralności łańcucha bloków, tworzeniu dowodów pracy oraz konstruowaniu struktur danych o wysokiej spójności, takich jak drzewa Merkle'a. W zdecentralizowanych systemach rozproszonych, jakimi są sieci *blockchain*, jednokierunkowe funkcje skrótu stanowią podstawę gwarancji niezmienności danych oraz umożliwiają weryfikację integralności danych bez konieczności odwoływania się do zaufanego pośrednika (Narayanan i in., 2016). Tym samym ich rola wykracza dziś poza konwencjonalne zastosowania w kryptografii stosowanej i obejmuje również kluczowe komponenty nowoczesnych rozwiązań w zakresie finansów rozproszonych, kontraktów inteligentnych oraz systemów tożsamości cyfrowej.

W praktyce systemy bezpieczeństwa stosowane w sektorze finansowym wykorzystują kombinację wielu warstw kryptografii. Przykładami są:

- komunikacja aplikacyjna – TLS z asymetryczną wymianą kluczy i symetrycznym szyfrowaniem sesji,
- szyfrowanie danych w spoczynku – AES-256 dla baz danych i backupów,
- mechanizmy podpisu cyfrowego – ECDSA w transakcjach wysokiej wartości i dokumentach elektronicznych,
- bezpieczne protokoły autoryzacji – np. OAuth 2.0 z *Hash-based Message Authentication Code*,
- wieloskładnikowe uwierzytelnianie.

3.4.2. Wzrost mocy obliczeniowej i komputery kwantowe

Wzrost dostępnej mocy obliczeniowej komputerów stanowi jeden z najistotniejszych czynników napędzających rozwój współczesnych technologii informacyjnych. Od momentu wprowadzenia pierwszych elektronicznych urządzeń obliczeniowych obserwujemy ciągły postęp w zakresie wydajności procesorów, co umożliwia realizację coraz bardziej złożonych zadań obliczeniowych. Kluczowym zjawiskiem, które pozwoliło na ten dynamiczny rozwój, jest sformułowane przez Gordona Moore'a w 1965 r. prawo nazywane prawem Moore'a, zgodnie z którym liczba tranzystorów umieszczanych na układzie scalonym podwaja się średnio co dwa lata, co prowadzi do wykładniczego wzrostu mocy obliczeniowej komputerów. Choć prawo Moore'a było przez wiele lat dokładnym prognostykiem rozwoju technologii mikroprocesorów, współczesne wyzwania związane z miniaturyzacją, efektywnością energetyczną oraz granicami fizycznymi układów scalonych skłaniają do poszukiwania nowych rozwiązań technologicznych. Jednym z nich są komputery kwantowe.

Komputery kwantowe stanowią jedno z najbardziej przełomowych osiągnięć współczesnej informatyki i fizyki kwantowej. Ich potencjał wykracza daleko poza możliwości klasycznych systemów obliczeniowych, co jest szczególnie istotne w kontekście bezpieczeństwa informacyjnego. W obliczu rozwoju technologii kwantowych podstawowe założenia współczesnej kryptografii asymetrycznej oraz niektórych metod uwierzytelniania mogą zostać podważone. Największe znaczenie dla tej zmiany mają dwa algorytmy: Shora i Grovera, wykorzystujące unikatowe właściwości komputerów kwantowych – kubity, superpozycję i splątanie kwantowe.

Komputery kwantowe operują na podstawowych jednostkach informacji zwanych kubitami (*qubits*), będących kwantowym odpowiednikiem klasycznego bitu. Kubit, opisany jako stan kwantowy w przestrzeni Hilberta, może się znajdować w dowolnej superpozycji stanów bazowych $|0\rangle$ i $|1\rangle$. Kubity mogą być fizycznie realizowane na wiele sposobów, m.in. jako nadprzewodzące układy Josephsona, stany jonów w pułapkach elektromagnetycznych, stany polaryzacji fotonów czy stany spinowe (Preskill, 2018). Jedną z fundamentalnych właściwości kubitów jest superpozycja, która umożliwia równoległe przetwarzanie wielu stanów jednocześnie. Komputer kwantowy z n kubitami może symultanicznie reprezentować 2^n stanów. To ekspotencjalne zwiększenie przestrzeni obliczeniowej jest głównym źródłem przewagi komputerów kwantowych w wielu zastosowaniach (Nielsen i Chuang, 2010). Kolejnym kluczowym mechanizmem jest splątanie kwantowe, które powoduje, że stany wielu kubitów są wzajemnie skorelowane w sposób niemożliwy do odtworzenia w systemach klasycznych. Splątanie umożliwia konstrukcję złożonych operacji nielokalnych oraz globalnych stanów kwantowych (Horodecki i in., 2009).

Bezpieczeństwo kryptografii asymetrycznej – w tym takich algorytmów, jak RSA, DSA, DH, a także algorytmów opartych na krzywych eliptycznych – opiera się na matematycznych problemach trudnych dla klasycznych komputerów. Obecne techniki faktoryzacji, takie jak algorytm sita liczbowego, mają wykładniczą złożoność czasową,

co gwarantuje bezpieczeństwo dla dużych liczb. Shor w 1994 r. opracował algorytm kwantowy, który rozwiązuje wymienione problemy w czasie wielomianowym, z wykorzystaniem kwantowego przekształcenia Fouriera (*Quantum Fourier Transform*, QFT). Schemat działania obejmuje redukcję faktoryzacji do problemu znalezienia okresu funkcji, wykorzystanie rejestrów kubitów do superpozycji, zastosowanie QFT oraz klasyczne przetwarzanie wyników (Shor, 1997). Złożoność algorytmu Shora wynosi $O((\log N)^3)$. To radykalna zmiana. Na przykład złamanie RSA-2048 wymagałoby ok. 4000 logicznych kubitów oraz stabilnych mechanizmów korekcji błędów (Gidney i Ekerå, 2021)[63]. Implikacje obejmują kompromitację infrastruktury klucza publicznego, zagrożenie dla integralności podpisów cyfrowych oraz ryzyko odszyfrowania historycznie przechwyconych komunikatów (Mosca, 2018). Problem ten zostanie jeszcze przedyskutowany w dalszej części.

Algorytm Grovera, opracowany w 1996 r., rozwiązuje problem przeszukiwania niestrukturalnego w czasie kwadratowo krótszym niż metody klasyczne[64]. Dla problemu z N możliwymi rozwiązaniami klasyczny *brute-force* wymaga $O(N)$ prób, natomiast Grover (1996) redukuje to do $O(\sqrt{N})$. Algorytm Grovera ma zastosowanie w atakach na algorytmy kryptografii symetrycznej, np. AES, SHA-2. Dla AES-128 efektywny czas ataku wynosi 2^{64}, a dla AES-256 jest równy 2^{128}. W praktyce oznacza to, że algorytmy z kluczami 256-bitowymi są nadal uważane za odporne na ataki kwantowe (Alagic i in., 2020).

3.4.3. Złożoność obliczeniowa jako fundament cyberbezpieczeństwa

Współczesne zastosowania kryptografii w sektorze finansowym opierają się na algorytmach, których poziom bezpieczeństwa jest ściśle powiązany z długością wykorzystywanych kluczy kryptograficznych pełniącą funkcję podstawowego parametru determinującego odporność na ataki brutalne. Należy jednak podkreślić, że sama długość klucza nie stanowi uniwersalnej gwarancji bezpieczeństwa – efektywność zabezpieczenia zależy również od klasy algorytmu, typu zastosowanego problemu matematycznego oraz postępu technologicznego, w tym możliwości obliczeniowych potencjalnego przeciwnika. W przypadku niektórych algorytmów asymetrycznych podatność na określone typy ataków może występować niezależnie od zwiększania długości klucza, co czyni koniecznym uwzględnianie także strukturalnej odporności algorytmu na nowe klasy zagrożeń. Do najpoważniejszych problemów związanych ze złożonością obliczeniową, która ciągle jeszcze zapewnia praktyczne bezpieczeństwo protokołów kryptograficznych, należy zaliczyć m.in. zagadnienia krótko omówione dalej.

---

[63] Określenia typu „złamanie" nie są oczywiście precyzyjne. Ważne jest jednak radykalne obniżenie czasochłonności rozwiązania konkretnego problemu w porównaniu z klasycznymi metodami.

[64] W uproszczeniu można powiedzieć, że algorytm zmniejsza złożoność obliczeniową ataków typu *brute-force*, co nakazuje przedefiniować siłę kryptograficzną algorytmów mierzoną długością klucza.

Nieprzerwanie intrygującym aspektem współczesnej kryptografii jest to, że pozornie prosty problem matematyczny wciąż stanowi fundament bezpieczeństwa komunikacji w sieci Internet. Mowa tu o wspomnianym już problemie faktoryzacji dużych liczb, na którym opiera się klasyczny algorytm RSA, zaproponowany w 1977 r. przez Rivesta, Shamira i Adlemana. Konstrukcja algorytmu wykorzystuje generowanie dwóch dużych, losowo wybranych liczb pierwszych oraz obliczenie ich iloczynu – liczby będącej kluczem publicznym. Najważniejszą operacją jest w tym kontekście zatarcie wiedzy o czynnikach składowych, co zapewnia, że ich późniejsze odzyskanie na podstawie samego iloczynu jest obliczeniowo nieosiągalne przy wykorzystaniu obecnie znanych algorytmów. Trwałość bezpieczeństwa RSA pozostaje zatem nierozerwalnie związana z nierozwiązaną w ogólności trudnością efektywnej faktoryzacji dużych liczb (Boneh, 1999; Pomerance, 1996; Rivest i in., 1978). W algorytmie problem faktoryzacji sprowadza się do następującego zagadnienia: mając daną liczbę *N*, będącą iloczynem dwóch nieznanych liczb pierwszych *p* oraz *q*, należy znaleźć te wartości. W praktycznych implementacjach RSA liczba *N* ma długość od 2048 do 4096 bitów, co odpowiada liczbom rzędów od 10^{617} do 10^{1234}. Choć problem faktoryzacji jest trywialny dla małych liczb, jego trudność szybko rośnie wraz ze wzrostem długości *N*, a żadne znane klasyczne algorytmy nie rozwiązują go w czasie wielomianowym. Najlepszym znanym klasycznym algorytmem faktoryzacji jest algorytm sita kwadratowego oraz jego uogólnienie – algorytm sita liczbowego (*General Number Field Sieve*, GNFS) (A. K. Lenstra i H. W. Lenstra, 1993). Możliwość praktycznej faktoryzacji 768-bitowego RSA została udowodniona wiele lat temu (Kleinjung i in., 2010), ale faktoryzacja 1024-bitowego RSA nadal wymagałaby miesięcy lub lat pracy nawet przy użyciu ogromnych zasobów obliczeniowych. Faktoryzacja RSA-2048 jest ciągle uważana za praktycznie niewykonalną w modelu klasycznym. Nadchodzący rozwój komputerów kwantowych zasadniczo zmienia perspektywę dotyczącą trudności faktoryzacji. Już kilka lat temu sugerowano, że algorytm Shora uruchomiony na odpowiednio dużym i stabilnym komputerze kwantowym może faktoryzować w sensownym czasie liczby na tyle duże, że RSA-2048 przestanie być uznawany za bezpieczny, przynajmniej w niektórych zastosowaniach (Aggarwal i in., 2017). Rozwój komputerów kwantowych na szczęście nie podlega prawu Moore'a i obecne szacunki dotyczące praktycznego łamania RSA-2048 bardzo się różnią. Niektóre oszacowania wskazują, że złamanie RSA-2048 w tydzień wymagałoby około miliona logicznych kubitów i znacznego narzutu związanego z korekcją błędów (Swayne, 2025), ale są też wyniki symulacji, zgodnie z którymi wystarczyłoby 50 kubitów i mniej niż jedna godzina (Azhari i Salsabila, 2024). Bez względu jednak na przyrost szybkości działania komputerów kwantowych jeszcze przez jakiś czas fascynujące właściwości liczb pierwszych będą stanowić wystarczającą w praktyce ochronę przed kompromitacją protokołów kryptograficznych. Jednocześnie wszystko wskazuje na to, że to właśnie podatności RSA będą pierwszą determinantą fundamentalnych zmian w zastosowaniach kryptografii w świecie finansów. Zmian związanych z początkiem ery postkwantowej.

Kolejnym filarem bezpieczeństwa licznych protokołów kryptograficznych jest problem logarytmu dyskretnego (*Discrete Logarithm Problem*, DLP). W swojej klasycznej postaci DLP polega na znalezieniu wykładnika x, dla którego zachodzi: $g^x \equiv h \pmod{p}$, gdzie g jest elementem generującym grupy multiplikatywnej modulo p, h jest danym elementem tej grupy, a p jest dużą liczbą pierwszą. Z punktu widzenia kryptoanalityka znalezienie x na podstawie znajomości g, h oraz p stanowi zadanie trudne obliczeniowo – nieznane są algorytmy klasyczne, które rozwiązywałyby ten problem w czasie wielomianowym[65]. Problem logarytmu dyskretnego leży u podstaw wielu popularnych protokołów kryptograficznych, w tym: Diffiego-Hellmana służącego do bezpiecznej wymiany kluczy, ElGamala stosowanego w systemach szyfrowania i podpisu cyfrowego i DSA (*Digital Signature Algorithm*) szeroko wykorzystywanego w sektorze publicznym i finansowym. Szczególną odmianą DLP, istotną w zastosowaniach finansowych, jest problem logarytmu dyskretnego na krzywych eliptycznych (ECDLP). W tym przypadku zadanie polega na znalezieniu liczby skalarnej k, dla której: $P = k \cdot G$, gdzie G jest ustalonym punktem na krzywej eliptycznej nad ciałem skończonym, a P jest danym punktem tej krzywej. Bezpieczeństwo takich rozwiązań, jak: *Elliptic Curve Diffie-Hellman* (ECDH) stosowanego do wymiany kluczy w TLS czy *Elliptic Curve Digital Signature Algorithm* (ECDSA) powszechnie używanego w podpisach cyfrowych w sektorze finansowym (m.in. PSD2, EMV), bazuje na trudności ECDLP. Kluczową zaletą kryptografii opartej na krzywych eliptycznych jest mała długość kluczy przy wysokim poziomie bezpieczeństwa, np. 256-bitowy klucz ECC oferuje poziom bezpieczeństwa porównywalny z 3072-bitowym kluczem RSA (Bernstein i Lange, 2017).

Wraz z rozwojem komputerów kwantowych problem DLP – w wersji zarówno klasycznej, jak i ECDLP – staje się fundamentalnie zagrożony. Algorytm Shora umożliwia rozwiązanie DLP w czasie wielomianowym. Analogicznie, algorytm Shora rozwiązuje także ECDLP, czyniąc wszelkie systemy oparte na ECC podatnymi na ataki w erze komputerów kwantowych. Szacunki wskazują, że do złamania ECC-256 wystarczyłoby kilka tysięcy logicznych kubitów oraz skuteczne mechanizmy korekcji błędów (Biasse i in., 2022).

Innym fundamentem współczesnego cyberbezpieczeństwa są funkcje jednokierunkowe, a w szczególności funkcje skrótu[66]. Odgrywają one fundamentalną rolę w zapewnianiu bezpieczeństwa systemów informatycznych. Są to przekształcenia, które dla argumentów dowolnej długości (ciągów znaków) wyznaczają wartości o długościach ściśle określonych. Właściwości funkcji są kluczowe zarówno dla bezpieczeństwa mechanizmów przechowywania i uwierzytelniania haseł, jak i dla integralności danych w rozmaitych zastosowaniach, w tym w sieciach *blockchain*. Właściwościami tymi są[67]:

---

[65] Jedną z klasycznych publikacji opisujących teorię liczb w zastosowaniach kryptograficznych jest książka Koblitza (1995).

[66] Literatura przedmiotu używa do określenia tej grupy algorytmów różnych określeń: funkcje skrótu, funkcje mieszające, funkcje haszujące. Więcej informacji na ten temat znaleźć można m.in. w (Kutyłowski i Strothmann, 1999).

[67] To klasyczne ujęcie własności jednokierunkowych funkcji skrótu. Wśród najnowszych analiz zagadnienia warto zwrócić uwagę na: (Alagic i in., 2025; Masri i Susanti, 2025; Salih i Kashmar, 2024).

- jednokierunkowość – wyznaczenie wartości funkcji jest bardzo proste, odnalezienie argumentu dla danej wartości jest jednak praktycznie niewykonalne,
- odporność na kolizje – oznaczająca, że nie da się w praktyce znaleźć dwóch różnych ciągów znaków, które dałyby w wyniku taką samą wartość funkcji; niewielka zmiana argumentu prowadzi do całkowicie innej wartości funkcji,
- odporność na znalezienie drugiego przeciwobrazu – oznaczająca, że dla zadanego argumentu nie da się w praktyce odnaleźć innego, który dałby tę samą wartość funkcji skrótu.

W przypadku przechowywania haseł użytkowników w systemach informatycznych stosuje się funkcje, które utrudniają skuteczne odtworzenie oryginalnych haseł nawet w razie kompromitacji bazy danych. Do współcześnie zalecanych funkcji należą: bcrypt – oparty na Blowfish, PBKDF2 – iteracyjna funkcja haszująca oparta na HMAC, Argon2 – zwycięzca konkursu Password Hashing Competition (*Password Hashing*…, b.d.). Oczywisty jest także fakt uzupełniania implementacji funkcji przez stosowanie soli – losowego ciągu dodawanego do hasła przed wyznaczeniem wartości jednokierunkowej funkcji skrótu[68].

Tabela 12. Efektywność ataków na funkcje skrótu

Jednokierunkowa funkcja skrótu	Technologia ataku	Przybliżona liczba łamanych haseł na sekundę	Odporność na ataki
MD5	GPU (RTX 4090)[(a)]	> 100 mld	bardzo niska – nieakceptowalna
SHA-1	GPU (RTX 4090)	> 50 mld	bardzo niska – nieakceptowalna
SHA-256	GPU (RTX 4090)	15-20 mld	średnia
bcrypt	GPU (RTX 4090)	5000-10 000	dobra
PBKDF2 (100k iteracji)	GPU (RTX 4090)	30 000-50 000	dobra
Argon2id	GPU (RTX 4090)	500-3000	bardzo dobra

[(a)] To jeden z najwydajniejszych obecnie wyspecjalizowanych procesorów będących punktem odniesienia w analizie wydajności.

Źródło: opracowanie własne na podstawie (Carter, b.d.) i innych źródeł.

Warto w tym miejscu zasygnalizować dyskusję – częściowo rozpoczętą w rozdziale poświęconym świadomości informatycznej – dotyczącą jakości haseł stosowanych przez użytkowników systemów bankowości internetowej. Problemy z tzw. wyciekami haseł mają źródło nie tyle w podatnościach technologii, ile w słabościach haseł tworzonych przez użytkowników. Współczesne ataki na hasła dostępu są przygotowywane permanentnie przez tworzenie słowników skrótów. Przechwycenie wartości

[68] Rozwiązanie takie pozwala uniknąć sytuacji, w której takie same hasła różnych użytkowników będą reprezentowane przez takie same wartości funkcji, co w przypadku kompromitacji tych drugich wiąże się z dodatkową informacją dla atakującego; zob. np. (Anbari i Sugiantoro, 2024).

funkcji skrótu dla haseł w danym systemie oznacza więc, że automatycznie znaczna ich część ulega skompromitowaniu. Połączenie przez cyberprzestępców ataku słownikowego z atakiem typu *brute-force* najczęściej przynosi bardzo negatywne – z punktu widzenia właścicieli haseł – rezultaty. Badania pokazują, że nawet do 90% haseł wyciekających z baz danych zabezpieczonych standardowymi funkcjami MD5 lub SHA-1 można złamać w ciągu kilku godzin (Biasse i in., 2022). W tabeli 12 przedstawiono efektywność ataków na popularne funkcje skrótu.

Analiza wyników badań pokazuje, że stosowanie tradycyjnych rozwiązań, takich jak MD-5 i funkcje rodzin SHA, już dziś wiąże się z ryzykiem praktycznie natychmiastowej kompromitacji haseł dostępu. Nowoczesne mechanizmy funkcji haszujących, takie jak Argon2, PBKDF2 czy bcrypt (przy odpowiednio dobranych parametrach), znacznie podnoszą koszt ataku – zarówno w modelu klasycznym, jak i w scenariuszach uwzględniających potencjalne przyspieszenie kwantowe wynikające z zastosowania algorytmu Grovera (Xie i Kang, 2025). Funkcje skrótu stanowią także kluczowy komponent infrastruktury kryptograficznej sieci *blockchain*. Od ich bezpieczeństwa – a zwłaszcza od odporności na kolizje, odporności *preimage* i właściwości entropijnych – zależy integralność całego systemu rozproszonego rejestru. W praktyce *blockchain* wykorzystuje funkcje skrótu w czterech podstawowych obszarach:

- w procesie generowania bloków (*Proof-of-Work*),
- w budowie struktur danych (drzewa Merkle'a),
- w identyfikacji transakcji,
- w mechanizmach skrótu adresów i kluczy publicznych.

Wadliwość lub osłabienie funkcji skrótu może prowadzić do poważnych konsekwencji systemowych – od naruszenia integralności łańcucha po umożliwienie ataków pozwalających np. na podwójne wydatkowanie. Pierwsze generacje blockchainów (np. Bitcoin) wykorzystywały funkcję SHA-256, która jak dotąd zachowuje odporność na znane ataki (Bernstein i Lange, 2017). Jednak inne systemy – m.in. starsze implementacje blockchainów prywatnych – stosowały słabsze funkcje, takie jak SHA-1 lub nawet MD5 w warstwach pomocniczych (Ibrahim i in., 2025). Wykazano, że funkcje te są całkowicie kompromitowane przez znane techniki kolizyjne (Stevens i in., 2017), co czyni je nieodpowiednimi do jakiegokolwiek zastosowania w nowoczesnym łańcuchu bloków. Na przykład atak kolizyjny na funkcję skrótu stosowaną w strukturze drzewa Merkle'a umożliwia teoretycznie skonstruowanie dwóch różnych zbiorów transakcji o identycznym korzeniu drzewa, co prowadziłoby do powstania bloków o różnych treściach, lecz z identycznym skrótem nagłówka. To bezpośrednio podważałoby właściwość niezmienności, będącej filarem zaufania w sieci *blockchain*. Mechanizmy PoW, takie jak te stosowane w Bitcoinie i licznych pochodnych, opierają się na znajdowaniu wartości *nonce*, która w połączeniu z danymi bloku daje wartość funkcji skrótu spełniającą określony warunek[69]. Osłabienie funkcji skrótu może zabu-

[69] W sieci *Bitcoin nonce* jest wartością, która dodana do bloku powoduje, że wartość skrótu dla całego bloku zaczyna się od określonej liczby zer.

rzyć rozkład wyników wyznaczania wartości funkcji, upraszczając lub przyspieszając znajdowanie *nonce*, a tym samym zakłócając podstawowe reguły działania sieci (Salih i Kashmar, 2024). Może to prowadzić do centralizacji produkcji bloków w rękach podmiotów dysponujących zoptymalizowanymi narzędziami. Badania wykazują, że przy zastosowaniu komputerów kwantowych algorytm Grovera może zmniejszyć efektywną odporność funkcji haszujących o połowę (Alagic i in., 2020). Dlatego też sieci *blockchain*, planujące długoterminowe bezpieczeństwo (np. w sektorze finansowym), przechodzą na funkcje SHA-3 lub BLAKE2, a nowe projekty stosują już funkcje typu *sponge*, zapewniające dodatkowe właściwości odpornościowe (Masri i Susanti, 2025).

Tabela 13. Odporność na ataki klasyczne i postkwantowe algorytmów kryptograficznych

Algorytm	Typ algorytmu	Typowa długość klucza	Szacowana odporność na ataki klasyczne	Odporność na ataki kwantowe	Zalecenia post-kwantowe
RSA	asymetryczny	2048 bitów	dobra (do niedawna standard sektora finansowego)	bardzo niska (podatność na algorytm Shora)	zalecana migracja do PQC
RSA	asymetryczny	3072-4096 bitów	wysoka w klasycznym modelu	niska (podatność na algorytm Shora)	zalecana migracja do PQC
ECC (np. ECDSA)	asymetryczny (krzywe eliptyczne)	256 bitów (bezpieczeństwo porównywalne z RSA-3072)	bardzo wysoka	niska (podatność na algorytm Shora)	zalecana migracja do PQC
AES-128	symetryczny	128 bitów	wysoka	efektywne bezpieczeństwo ~64 bity (Grover)[(a)]	zmiana na AES-256
AES-256	symetryczny	256 bitów	bardzo wysoka	efektywne bezpieczeństwo ~128 bitów (Grover)	uznawany za bezpieczny
SHA-2	funkcja skrótu	256 bitów	wysoka	efektywne bezpieczeństwo ~128 bitów (Grover)	dla zastosowań o podwyższonych wymogach bezpieczeństwa zalecane SHA-3
Lattice-based (np. Kyber, Dilithium)	asymetryczny/ PQC	parametry konfigurowalne	bardzo wysoka	odporny na znane algorytmy kwantowe	rekomendowany do wdrożenia
Hash-based signatures (np. XMSS)	asymetryczny/ PQC	parametry konfigurowalne	bardzo wysoka	odporny na znane algorytmy kwantowe	rekomendowany do wdrożenia

[(a)] Oznacza, że atak wymaga w przybliżeniu 2^{64} prób.

Źródło: opracowanie własne na podstawie cytowanej literatury przedmiotu.

Obserwowany wzrost mocy obliczeniowej – zarówno w przypadku komputerów klasycznych, jak i w kontekście rozwoju komputerów kwantowych – stawia nowe wyzwania przed architekturą kryptograficzną sektora finansowego. Analizy literatury wskazują, że systemy asymetryczne oparte na RSA i ECC mogą w niedalekiej przyszłości zostać zagrożone w sposób fundamentalny poprzez zastosowanie algorytmu Shora, co wymusza już dziś planowanie migracji do algorytmów odpornych na ataki kwantowe (*Post-Quantum Cryptography*, PQC). W tabeli 13 zaprezentowano próbę podsumowania powyższych rozważań w kontekście potencjalnej przyszłości standardowych algorytmów kryptograficznych.

3.4.4. Algorytmy postkwantowe

Algorytmy postkwantowe[70] projektowane są w taki sposób, aby były odporne na ataki przeprowadzane za pomocą przyszłych komputerów kwantowych. Uwzględniają zatem opisane uprzednio problemy związane ze złożonością obliczeniową oraz efektywnością wykorzystywania bardzo długich kluczy. Istnieje kilka obiecujących koncepcji algorytmów postkwantowych, które stale są badane i rozwijane w celu zapewnienia bezpieczeństwa w przyszłości. Najważniejsze z nich to:

- algorytmy oparte na kratkach (*Lattice-Based Algorithms*),
- problem *Learning with Errors*,
- kody korekcyjne,
- funkcje skrótu,
- kryptografia wielomianowa.

Algorytmy oparte na kratkach stanowią jeden z najczęściej badanych i najbardziej obiecujących obszarów kryptografii postkwantowej. Kratki to struktury matematyczne, które obejmują zestawy punktów rozmieszczonych w przestrzeni o określonych właściwościach geometrycznych. Koncepcja algorytmów tego typu jest związana z rozwiązaniami równań matematycznych w takich strukturach. Wśród algorytmów opartych na kratkach na uwagę zasługuje NTRU (*N-th degree Truncated Polynomial Ring Units*) – jeden z najstarszych i najbardziej rozpoznawalnych algorytmów opartych na problemie kratki. Jest systemem szyfrowania związanym z problemem znajdowania najkrótszych wektorów w kratce. NTRU wydaje się odporny na ataki kwantowe z wykorzystaniem algorytmu Shora. Ponadto oferuje szybsze operacje w porównaniu z innymi systemami kryptograficznymi, takimi jak RSA, przy zachowaniu wysokiego poziomu bezpieczeństwa. Ze względu na swoje właściwości NTRU jest szeroko rozważany w kontekście przyszłych systemów kryptograficznych (Micciancio i in., 2009). Podstawy algorytmu zaproponowali Hoffstein i in. (1998).

[70] Postkwantowość nie ma nic wspólnego z pojęciem kryptograficznego algorytmu kwantowego, który wykorzystuje prawa mechaniki kwantowej.

Mimo dużego potencjału algorytmy oparte na kratkach napotykają również szereg wyzwań, szczególnie związanych z rozmiarami kluczy i wydajnością. Z jednej strony zapewniają wysoce odporne na ataki kwantowe mechanizmy kryptograficzne, z drugiej jednak wymagają dużych zasobów obliczeniowych i pamięciowych, co sprawia, że są trudniejsze do wdrożenia w systemach o ograniczonych zasobach. W związku z tym jednym z obszarów intensywnych badań w tej dziedzinie jest optymalizacja tych algorytmów pod kątem zarówno efektywności, jak i bezpieczeństwa. Badania koncentrują się na zmniejszeniu rozmiarów kluczy z jednoczesnym zachowaniem wysokiego poziomu ochrony przed atakami kwantowymi (Micciancio i in., 2009).

Kolejnym ważnym problemem matematycznym, który stanowi fundament dla wielu algorytmów postkwantowych, jest *Learning with Errors* (LWE). Problem LWE polega na próbie odzyskania informacji o tajnym wektorze z rozmytych danych, które zawierają szum. LWE jest uznawane za jedno z najbardziej odpornych na ataki kwantowe zagadnień, a jego zastosowanie w kryptografii daje możliwość tworzenia zarówno szyfrowania, jak i podpisów cyfrowych. Przykładem takiego algorytmu jest NTS-KEM, który służy do wymiany kluczy oraz pozwala tworzyć różne algorytmy do generowania podpisów cyfrowych (Regev, 2009). Dodatkowo LWE może być rozszerzone na wersję Ring-LWE, która poprawia wydajność algorytmu dzięki wykorzystaniu struktur algebraicznych, takich jak pierścienie (Lyubashevsky i in., 2010).

Algorytmy oparte na problemie kodów korekcyjnych również stanowią jeden z kluczowych obszarów kryptografii postkwantowej, gdyż są uważane za trudne do rozwiązania zarówno przez klasyczne, jak i przez kwantowe algorytmy. Algorytmy kodowe opierają się na strukturach kodów korekcyjnych, które zapewniają odporność na zakłócenia w przesyłanych danych, a także stanowią solidną podstawę dla bezpiecznego szyfrowania i podpisywania. Wśród algorytmów wykorzystujących tę koncepcję na uwagę zasługują: algorytm McEliece'a, algorytm Niederreitera i kody LDPC (*Low-Density Parity-Check Codes*).

Algorytm McEliece'a jest jednym z najbardziej znanych algorytmów opartych na problemie kodowania. Został zaprezentowany w 1978 r. przez Roberta McEliece'a. Algorytm ten opiera się na problemie dekodowania kodów Goppa, który jest uznawany za trudny nawet w kontekście komputerów kwantowych, jednak jego wadą są duże rozmiary kluczy, co czyni go mniej praktycznym. Postuluje się zatem różne optymalizacje, takie jak stosowanie bardziej efektywnych kodów, co pozwala na zmniejszenie rozmiarów kluczy bez znaczącej utraty bezpieczeństwa.

Algorytm Niederreitera jest wariantem algorytmu McEliece'a, również opartym na problemie dekodowania kodów Goppa, ale zamiast wykorzystywania klasycznych kodów liniowych, stosuje się tu kody wektorowe, co umożliwia większą elastyczność w budowie kluczy. Algorytm ten jest uznawany za równie odporny na ataki kwantowe co jego poprzednik, ale charakteryzuje się mniejszymi wymaganiami dotyczącymi rozmiaru kluczy (Niederreiter, 1986).

Kody LDPC charakteryzują się rzadkimi macierzami kontrolnymi, co sprawia, że ich dekodowanie jest wysoce odporne na zakłócenia i trudne do rozwiązania. Choć

kody LDPC nie są bezpośrednio związane z algorytmami szyfrowania, wykorzystuje się je w ramach kryptografii opartej na kodach (MacKay, 2003). Algorytmy oparte na funkcjach skrótu stanowią istotną grupę kryptograficznych algorytmów postkwantowych, które są oparte na trudności problemów związanych z omówionymi wcześniej funkcjami skrótu. Właściwości funkcji skrótu przestają gwarantować bezpieczeństwo komputerów kwantowych, ponieważ algorytmy kwantowe, takie jak algorytm Grovera, mogą znacznie przyspieszyć proces wyszukiwania *preimage* oraz kolizji. Jednym z najważniejszych obszarów zastosowania funkcji skrótu w kryptografii postkwantowej jest tworzenie podpisów cyfrowych. XMSS (*eXtended Merkle Signature Scheme*) jest algorytmem opartym na drzewach Merkle'a i oferuje odporność na ataki kwantowe. W tym systemie wiadomość jest haszowana wielokrotnie przez różne poziomy drzewa Merkle'a, co zapewnia wysoką odporność na ataki polegające na próbie manipulacji podpisem. XMSS jest jednym z najlepszych kandydatów na postkwantowy algorytm podpisu cyfrowego, ponieważ jego bezpieczeństwo opiera się na trudności obliczeniowej związanej z problemem znalezienia kolizji w funkcjach skrótu, co wciąż stanowi wyzwanie nawet dla komputerów kwantowych. Innym algorytmem w omawianej kategorii jest SPHINCS+ (*Stateless Practical Hash-Based Incredibly Efficient Signature Scheme*). Jest to algorytm podpisu cyfrowego, który łączy różne techniki haszujące, aby stworzyć bezpieczne, ale efektywne rozwiązanie do generowania podpisów cyfrowych w środowisku postkwantowym. SPHINCS+ oparty jest na strukturze wielokrotnych funkcji skrótu, przy czym każda iteracja algorytmu wykorzystuje inny zestaw funkcji, zapewniając większą odporność na ataki (Bernstein i Lange, 2017).

Kolejnym kandydatem do standardu postkwantowego jest kryptografia wielomianowa (*multivariate cryptography*), która opiera się na trudności rozwiązywania układów równań wielomianowych o dużej liczbie zmiennych. Najlepszym przykładem rozwiązania tego typu jest system *Unbalanced Oil and Vinegar* zaprojektowany przez Jacques'a Patarina. Jest to protokół podpisu cyfrowego, a jego bezpieczeństwo opiera się na matematycznym problemie należącym do klasy NP-trudnych (Kipnis i in., 1999).

Komputery kwantowe, dzięki zdolnościom przetwarzania informacji w sposób równoległy, a także możliwościom redukcji złożoności obliczeniowej problemów matematycznych, są potencjalnym zagrożeniem dla istniejących algorytmów kryptograficznych. Algorytmy kryptografii postkwantowej stanowią istotną alternatywę wobec klasycznych rozwiązań. Ich konstrukcja opiera się na problemach matematycznych, które – zgodnie z aktualnym stanem wiedzy – pozostają trudne do rozwiązania nawet w obliczu radykalnego wzrostu mocy obliczeniowej, wykraczającego poza obserwowane tempo zgodne z historycznymi obserwacjami. Mimo istnienia precyzyjnych rekomendacji organizacji standaryzacyjnych – takich jak NIST – dotyczących harmonogramów wycofywania algorytmów opartych na faktoryzacji i logarytmie dyskretnym (Moody i in., 2024) (m.in. RSA, DSA, ECDSA) światowe standardy kryptografii postkwantowej pozostają w fazie finalizacji. Trwający proces standaryzacyjny (np. NIST PQC Standardization Project) wskazuje kilku kandydatów o dużym potencjale implementacyjnym,

lecz żaden z nich nie osiągnął jeszcze statusu powszechnie obowiązującego standardu technicznego ani legislacyjnego. W konsekwencji, pomimo istotnych postępów w teorii i inżynierii kryptograficznej, środowisko stosowanych rozwiązań nadal charakteryzuje się stanem przejściowym i dużym stopniem niepewności.

3.5. Systemy wykrywania włamań wykorzystujące sztuczną inteligencję

W rozdziale pierwszym rozpoczęto dyskusję nad zastosowaniami sztucznej inteligencji w systemach instytucji finansowych. Swego rodzaju klamrę stanowi zatem niniejszy rozdział, sygnalizujący wybrane zagadnienia związane z przyszłością mechanizmów cyberbezpieczeństwa w kontekście szeroko rozumianych rozwiązań AI. Do najbardziej istotnych obszarów zastosowań w obszarze cyberbezpieczeństwa należą już obecnie systemy wykrywania włamań (anomalii). Są to narzędzia bezpieczeństwa sieciowego, które monitorują ruch sieciowy i aktywność systemów w celu wykrywania złośliwej aktywności lub naruszeń zasad bezpieczeństwa. W klasycznym ujęciu działają na zasadzie analizy danych i porównywania ich ze wzorcami ataków. Sztuczna inteligencja ma potencjał przeniesienia ich na nieporównywalnie wyższy poziom. Technologiami kluczowymi w tym obszarze są:

- *Machine Learning* (uczenie maszynowe) – technika polegająca na trenowaniu modeli komputerowych do rozpoznawania wzorców w danych i podejmowania decyzji bez jawnego programowania,
- *Deep Learning* (głębokie uczenie) – zaawansowana forma uczenia maszynowego, wykorzystująca wielowarstwowe sieci neuronowe do analizy skomplikowanych i nieliniowych zależności w dużych zbiorach danych,
- *Support Vector Machine* (maszyna wektorów nośnych) – algorytm klasyfikacyjny, który znajduje optymalną hiperpowierzchnię oddzielającą różne klasy danych z maksymalnym marginesem,
- *Random Forest* (losowy las) – technika uczenia zespołowego wykorzystująca wiele drzew decyzyjnych, której celem jest poprawa dokładności klasyfikacji i redukcja nadmiernego dopasowania,
- *Autoencoders* (autokodery) – sieci neuronowe uczące się efektywnej reprezentacji (kodowania) danych poprzez ich kompresję i rekonstrukcję, wykorzystywane m.in. do wykrywania anomalii,
- *Convolutional Neural Networks* (splotowe sieci neuronowe) – specjalistyczne sieci neuronowe zaprojektowane do przetwarzania danych o strukturze siatki (np. obrazów, danych sieciowych), zdolne do automatycznego wyodrębniania cech,
- *Reinforcement Learning* (uczenie ze wzmocnieniem) – model uczenia oparty na podejmowaniu decyzji w środowisku przez próbę i błąd, w którym agent uczy się maksymalizować nagrodę w długim okresie,

- *SHapley Additive exPlanations* (SHAP – wyjaśnienia addytywne Shapleya) – metoda interpretacji modeli AI, która przypisuje każdej cesze wkład w końcową decyzję modelu, bazując na teorii wartości Shapleya,
- *Federated/Explainable Artificial Intelligence* (federacyjna/wyjaśnialna sztuczna inteligencja) – podejście umożliwiające trenowanie modeli AI w sposób rozproszony (bez przesyłania danych) i jednocześnie dostarczające wyjaśnień podejmowanych decyzji,
- *Convolutional Neural Network-Long Short-Term Memory* (splotowe sieci neuronowe połączone z długoterminową pamięcią krótkotrwałą) – model hybrydowy łączący zdolności CNN do analizy przestrzennej z LSTM do analizy sekwencji czasowych, bardzo efektywny w detekcji anomalii w ruchu sieciowym,
- *Spatial Feature Learning* (uczenie przestrzennych cech) – technika polegająca na ekstrakcji cech z danych o strukturze przestrzennej, co pozwala lepiej uchwycić zależności topologiczne w ruchu sieciowym,
- *Adaptive Security and Cognitive Hybrid Intrusion Detection System* (adaptacyjny i kognitywny hybrydowy system wykrywania włamań) – system łączący różne metody AI i reguły bezpieczeństwa, uczący się dynamicznie i dostosowujący do zmieniających się zagrożeń w czasie rzeczywistym,
- *Fully Connected Neural Network* (w pełni połączona sieć neuronowa) – typ sieci neuronowej, w której każdy neuron jednej warstwy jest połączony z każdym neuronem warstwy następnej, używany do klasyfikacji i regresji.

Wyniki badań nad skutecznością tego typu rozwiązań pokazują ich znaczną przewagę nad klasycznymi mechanizmami. Na przykład modele oparte na architekturach takich jak *Convolutional Neural Networks*, *Long Short-Term Memory* oraz ich połączenia (np. Conv1d-LSTM) osiągają najwyższe wyniki skuteczności. Lukogo i in. (2024) wskazują 99,97% skuteczności detekcji intruzji przy zastosowaniu modelu Conv1d-LSTM, co znacznie przewyższa tradycyjne metody oparte na sygnaturach. Sieci neuronowe tego typu cechują się wysoką zdolnością do rozpoznawania wzorców w danych sieciowych, co pozwala na skuteczne wykrywanie nawet nieznanych wcześniej anomalii. Szczególne znaczenie mają tu także aspekty wydajnościowe. Vo i in. (2024) donoszą o czasie detekcji 22,29 mikrosekundy na przepływ sieciowy przy zastosowaniu równoległych modeli zespołowych (*Parallel Ensemble Learning*) i technik augmentacji danych (*Augmented GAN*). Znaczącym trendem jest także integracja różnych podejść AI w celu zwiększenia skuteczności i elastyczności systemów bezpieczeństwa. Larriva-Novo i in. (2023) zastosowali *Random Forest* z technikami wyjaśnialnej AI, uzyskując wysoką skuteczność (do 98,9%) przy jednoczesnym obniżeniu wskaźnika fałszywie pozytywnych alarmów do 2,21%. Innym istotnym nurtem jest zastosowanie metod uczenia ze wzmocnieniem (*Reinforcement Learning*), pozwalających na dynamiczne dostosowanie działania systemu do zmieniających się warunków sieciowych. Otoum i in. (2020) wykazali, że system oparty na tej metodzie osiąga 100% skuteczności w środowiskach symulowanych sieci sensorowych, co wskazuje na duży potencjał

adaptacyjnych systemów detekcji zagrożeń w środowiskach krytycznych, takich jak systemy instytucji finansowych. Równolegle z efektywnością detekcji analizowane są także aspekty wdrożeniowe, takie jak skalowalność czy elastyczność. Kim i in. (2020) wskazują np. możliwość konteneryzacji modeli przy użyciu dockera[71], co umożliwia ich wdrażanie w złożonych środowiskach rozproszonych. W literaturze coraz większą wagę przykłada się również do problematyki wyjaśnialności (*explainability*) oraz zdolności adaptacyjnych. Cytowani już Larriva-Novo i in. (2023) akcentują potrzebę równowagi między dużą skutecznością detekcji a przejrzystością procesu decyzyjnego, co ma szczególne znaczenie w kontekście zgodności z regulacjami oraz audytowalności działań systemu. Alzaylaee (2025) podkreśla znaczenie modeli uczących się w sposób ciągły, zdolnych do reagowania na nowe klasy zagrożeń, w tym ataki *zero-day*.

Systemy wykrywania włamań odgrywały fundamentalną rolę w zapewnianiu bezpieczeństwa środowisk informatycznych w sektorze finansowym od początku procesu jego cyfryzacji. Już na wczesnych etapach rozwoju technologii bankowości elektronicznej i sieci korporacyjnych narzędzia te stanowiły pierwszą linię obrony przed nieautoryzowanym dostępem, atakami typu DDoS, rozpowszechnianiem złośliwego oprogramowania oraz innymi formami anomalii w ruchu sieciowym. Tradycyjne podejścia oparte na modelach statystycznych, regułach heurystycznych i analizie sygnatur zapewniały ograniczoną, lecz istotną ochronę, umożliwiając identyfikację znanych zagrożeń na podstawie ich charakterystycznych wzorców. Współczesne środowiska finansowe, charakteryzujące się wysoką złożonością, dynamicznością i rosnącym wolumenem przetwarzanych danych, wymagają jednak bardziej zaawansowanych metod detekcji, które pozwalają na wykrywanie nie tylko znanych, lecz także nowych, wcześniej nieobserwowanych zagrożeń. W tym kontekście szczególnego znaczenia nabiera właśnie integracja rozwiązań z zakresu sztucznej inteligencji, w szczególności technik uczenia maszynowego, z klasycznymi systemami. Tym samym AI nie tylko zwiększy precyzję i zakres wykrywania zagrożeń, ale również umożliwi proaktywną ocenę ryzyka oraz adaptacyjną reakcję na incydenty bezpieczeństwa, co uczyni z systemów klasy IDS kluczowy element współczesnych strategii zarządzania cyberbezpieczeństwem w sektorze finansowym.

3.6. Podsumowanie

Omówione w niniejszym rozdziale cztery obszary: silne uwierzytelnienie, problemy świadomości i edukacji informatycznej, potencjalny wpływ komputerów kwantowych na kryptografię oraz zastosowanie sztucznej inteligencji w systemach detekcji zagrożeń stanowią fundamenty współczesnej architektury cyberbezpieczeństwa. Ich znaczenie wykracza poza sektor finansowy, obejmując również inne obszary infra-

[71] Docker to platforma *open source* służąca do tworzenia, wdrażania i zarządzania aplikacjami w tzw. kontenerach. Konteneryzacja pozwala na spakowanie aplikacji wraz z jej zależnościami w izolowane środowisko, co zapewnia spójność działania niezależnie od platformy.

struktury krytycznej, w tym energetykę, transport, opiekę zdrowotną czy administrację publiczną. Każdy z tych komponentów pełni odrębną, a zarazem komplementarną funkcję w procesie budowania odporności systemów teleinformatycznych na coraz większe, coraz bardziej złożone i często wielowektorowe spektrum zagrożeń.

Silne uwierzytelnienie jest kluczowym elementem kontroli dostępu, ograniczającym ryzyko przejęcia tożsamości cyfrowej oraz nieautoryzowanego dostępu do zasobów, co znajduje potwierdzenie w raportach branżowych czy wytycznych ENISA. Problemy świadomości i edukacji informatycznej mają charakter przekrojowy, ponieważ nawet najbardziej zaawansowane technologie ochronne mogą zostać zniweczone przez błąd ludzki lub brak wiedzy użytkowników, co zgodnie z wynikami badań stanowi wciąż jeden z głównych wektorów ataku w sektorze finansowym. Potencjalny wpływ komputerów kwantowych na kryptografię wprowadza zupełnie nowy wymiar wyzwań, wymuszając prace nad kryptografią postkwantową i adaptacją standardów bezpieczeństwa w perspektywie długoterminowej. Zastosowanie sztucznej inteligencji w systemach detekcji zagrożeń umożliwia automatyzację analizy incydentów, wczesne wykrywanie anomalii oraz adaptacyjne reagowanie na dynamicznie zmieniające się techniki ataków, choć równocześnie rodzi pytania o przejrzystość modeli, podatność na manipulacje i etyczne aspekty ich użycia. Wszystkie te obszary wzajemnie się przenikają i wzmacniają, tworząc zintegrowany system ochrony, który może być skuteczny tylko wtedy, gdy będzie spójny na poziomie technologicznym, organizacyjnym oraz regulacyjnym. Wynika to zarówno z wyników badań naukowych oraz analiz eksperckich, jak i z raportów branżowych, które konsekwentnie wskazują, że efektywne cyberbezpieczeństwo wymaga synergii działań technologicznych, proceduralnych oraz edukacyjnych. Nie oznacza to oczywiście, że inne zagadnienia, takie jak chociażby zarządzanie incydentami, bezpieczeństwo aplikacji czy ochrona fizyczna infrastruktury, mają mniejsze znaczenie. Niemniej to właśnie silne uwierzytelnienie, podnoszenie świadomości użytkowników, gotowość na wyzwania postkwantowe oraz wdrożenie AI w systemach detekcji stanowią te filary, które w najbliższej przyszłości będą w największym stopniu kształtować ewolucję i kierunki rozwoju cyberbezpieczeństwa w systemie finansowym.

Zakończenie

Podsumowując rozważania podjęte w tej książce, należy podkreślić, że cyberbezpieczeństwo systemu finansowego stanowi dziś nie tylko wyzwanie technologiczne, lecz także problem społeczny, ekonomiczny i regulacyjny o wymiarze strategicznym. W dobie dynamicznego rozwoju cyfryzacji system finansowy podlega transformacji, której tempo i skala są bez precedensu w historii gospodarki. Ta transformacja nie ogranicza się do samej modernizacji infrastruktury informatycznej, lecz oznacza głębokie przekształcenia w sferze architektury ryzyka, modeli operacyjnych oraz sposobu interakcji pomiędzy uczestnikami rynku. Jednocześnie zwiększa się znaczenie czynników niefinansowych, takich jak kompetencje cyfrowe, świadomość informatyczna, kultura bezpieczeństwa organizacyjnego czy jakość współpracy między sektorem finansowym a instytucjami nadzoru. Analizy przedstawione w niniejszej publikacji ukazały, że transformacja technologiczna sektora finansowego przynosi istotne korzyści w zakresie efektywności, personalizacji usług i szybkości realizacji operacji, ale jednocześnie rodzi nowe, złożone zagrożenia. W szczególności niepokojące pozostaje zjawisko luki między deklarowanym poziomem wiedzy użytkowników a ich rzeczywistymi zachowaniami w zakresie bezpieczeństwa. Badania potwierdzają, że wysoki poziom deklaratywnej świadomości nie wystarcza, jeśli nie towarzyszą mu konsekwentne stosowanie dostępnych narzędzi ochronnych oraz odpowiednie procedury reagowania na incydenty. Konieczne staje się więc projektowanie rozwiązań bezpieczeństwa z uwzględnieniem rzeczywistych możliwości poznawczych i behawioralnych użytkowników. Podjęta w książce analiza technologicznych trendów – od sztucznej inteligencji, przez Internet Rzeczy, po chmurę obliczeniową i *blockchain* – unaocznia, że innowacje w sektorze finansowym mają charakter dualny. Mogą stać się fundamentem rozwoju i wzrostu konkurencyjności, ale równie dobrze mogą posłużyć jako wektor ataku dla cyberprzestępców. Tę dwoistość należy traktować jako kluczowy punkt wyjścia w projektowaniu polityki bezpieczeństwa finansowego, która powinna być nieustannie aktualizowana i testowana w kontekście zmieniających się uwarunkowań technologicznych i regulacyjnych. Jednocześnie nie można zapominać o problemach strukturalnych, które zostały zarysowane w rozdziale trzecim, w szczególności o jakości i odporności mechanizmów uwierzytelniania, problematyce zarządzania tożsamością cyfrową, roli kryptografii w obliczu rozwoju komputerów kwantowych oraz wyzwaniach związanych z wykorzystaniem sztucznej inteligencji do wykrywania anomalii. To obszary wymagające dalszych, pogłębionych badań empirycznych i teoretycznych, zwłaszcza w kontekście ich integracji z praktyką bankową i regulacyjną. Wydaje się, że niewystarczająco eksplorowane pozostają także kwestie transmisyjności zagrożeń w ramach ekosystemu finansowego, gdzie atak na jedno ogniwo może się błyskawicznie przenosić na kolejne instytucje w wyniku silnych po-

wiązań systemowych. Kolejnym obszarem wartym dalszych studiów jest zagadnienie odporności społecznej i kulturowej w kontekście cyberbezpieczeństwa finansowego. Dotychczasowe badania, choć w dużej mierze koncentrują się na aspektach technologicznych i organizacyjnych, w niewielkim stopniu uwzględniają psychologiczne uwarunkowania zachowań użytkowników, mechanizmy budowania zaufania, a także wpływ komunikacji kryzysowej na stabilność rynku finansowego w czasie cyberincydentów. W świetle rosnącego znaczenia czynników behawioralnych w bezpieczeństwie cyfrowym uzupełnienie tej luki badawczej może przynieść cenne wnioski dla projektowania bardziej skutecznych programów edukacyjnych i kampanii społecznych. Przyszłe badania powinny jeszcze szerzej uwzględnić problem współdziałania między sektorem finansowym a instytucjami publicznymi i organami regulacyjnymi, także w wymiarze transgranicznym. Globalny charakter cyberzagrożeń sprawia, że wyłącznie krajowe regulacje i procedury mogą się okazać niewystarczające. Z tego powodu potrzebne są dalsze analizy dotyczące harmonizacji regulacji, wymiany danych o zagrożeniach oraz budowania wspólnych standardów reagowania w ramach międzynarodowych inicjatyw.

Podjęta w książce próba syntetycznego ujęcia cyberbezpieczeństwa systemu finansowego jest z konieczności ograniczona, ze względu zarówno na rozległość materiału, jak i na tempo zmian technologicznych. Autor ma jednak nadzieję, że przedstawione wnioski i refleksje staną się inspiracją do dalszych dyskusji oraz pogłębionych badań w tym dynamicznie rozwijającym się obszarze. Świadomość wyzwań, przed którymi staje sektor finansowy, powinna motywować zarówno praktyków, jak i badaczy do nieustannego poszukiwania innowacyjnych, a zarazem realistycznych rozwiązań, które zapewnią stabilność i odporność finansów w cyfrowej przyszłości.

Literatura

A New Frontier in Transaction Banking. Unlocking the Value of Open API Technology. (2022). Raiffeisen Bank International AG, Innopay. Pobrano 2 listopada 2025 z https://www.rbinternational.com/content/dam/rbi/marketing/ww/open-apis/Whitepaper_OpenAPI.pdf.coredownload.pdf

Abdajabar, A. i Idbeaa, T. (2024). Cybercrime's Threat to Financial Institutions During COVID-19. *AlQalam Journal of Medical and Applied Sciences*, *7* (Suppl. 2), 46-52. https://doi.org/10.54361/ajmas.2472207

Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., Morozova, A., Schwarz, N. i Wilson, C. (2020). *Cyber Risk and Financial Stability: It's a Small World After All*. International Monetary Fund. https://doi.org/10.5089/9781513512297.006

Adil, M., Farouk, A., Ali, A., Song, H. i Jin, Z. (2025). Securing Tomorrow of Next-Generation Technologies with Biometrics, State-of-The-Art Techniques, Open Challenges, and Future Research Directions. *Computer Science Review*, *57*, artykuł 100750. https://doi.org/10.1016/j.cosrev.2025.100750

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M. i Tomamichel, M. (2017). Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger*, *3*. https://doi.org/10.5195/ledger.2018.127

Ahmad, A., Webb, J., Desouza, K. C. i Boorman, J. (2019). Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack. *Computers & Security*, *86*(5), 402-418. https://doi.org/10.1016/j.cose.2019.07.001

Ahmed, S., Masood, M., Bee, A. W. T. i Ichikawa, K. (2025). False Failures, Real Distrust: The Impact of an Infrastructure Failure Deepfake on Government Trust. *Frontiers in Psychology* (Brief Research Report), *16*. https://doi.org/10.3389/fpsyg.2025.1574840

Alagic, G., Alperin-Sheriff, J., Apon, D. C., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-C., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A. i Smith-Tone, D. (2020). *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8309. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8309

Alagic, G., Carolan, J., Majenz, C. i Tokat, S. (2025). *The Sponge Is Quantum Indifferentiable*. Cryptology ePrint Archive, Paper 2025/731. https://doi.org/10.48550/arXiv.2504.16887

Ali, H. I., Kurunathan, H., Eldefrawy, M. H., Gruian, F. i Jonsson, M. (2025). Navigating the Challenges and Opportunities of Securing Internet of Autonomous Vehicles with Lightweight Authentication. *IEEE Access*, *13*, 24207-24222. https://doi.org/10.1109/ACCESS.2025.3537800

Allioui, H. i Mourdi, Y. (2023). Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. *Sensors*, *23*(19), artykuł 8015. https://doi.org/10.3390/s23198015

Alvarez, N., Menon, R., Zhao, Y., Koenig, D. i Al-Fulan, F. (2024). *Behavioral Biometrics Fusion for Deepfake-Resistant Remote Identity Verification in Fintech Platforms*. Pobrano 2 listopada 2025 z https://www.researchgate.net/publication/391827811_Behavioral_Biometrics_Fusion_for_Deepfake-Resistant_Remote_Identity_Verification_in_Fintech_Platforms

Alzaylaee, M. K. (2025). Enhancing Cybersecurity Through Artificial Intelligence: A Novel Approach to Intrusion Detection. *International Journal of Advanced Computer Science and Applications*, *16*(4), 577-586. https://doi.org/10.14569/IJACSA.2025.0160458

Anbari, M. Z. i Sugiantoro, B. (2024). Enhancing the Resistance of Password Hashing Using Binary Randomization Through Logical Gates. *International Journal of Electrical and Computer Engineering, 14*(5), 5400-5407. http://doi.org/10.11591/ijece.v14i5.pp5400-5407

Angelbeck, B. (2014). The Faustian Bargain of Technological Change: Evaluating the Socioeconomic Effects of the Bow and Arrow Transition in the Coast Salish Past. *Journal of Anthropological Archaeology*, *36*, 93-109.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. i Zhou, Y. (2017). Understanding the Mirai Botnet. W: E. Kirda, T. Ristenpart (red.), *EC'17: Proceedings of the 26th USENIX Conference on Security Symposium* (s. 1093-1110). USENIX Association.

Armis. (2025). *The State of Cyberwarfare*. Pobrano 2 listopada 2025 z https://www.armis.com/cyberwarfare/

Arner, D. W., Barberis, J. N. i Buckley, R. P. (2017). FinTech, RegTech and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law and Business*, *37*(3), 341-414. Pobrano 2 listopada 2025 z https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2/

Arora, N. i Kaur, P. (2020). Augmenting Banking and FinTech with Intelligent Internet of Things Technology. W: *IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)* (s. 648-653). IEEE. https://doi.org/10.1109/ICRITO48877.2020.9198018

Arshad, H., Johansen, C. i Owe, O. (2022). Semantic Attribute-Based Access Control: A Review on Current Status and Future Perspectives. *Journal of Systems Architecture*, *129*, artykuł 102625. https://doi.org/10.1016/j.sysarc.2022.102625

Azhari, R. i Salsabila, A. N. (2024). Analyzing the Impact of Quantum Computing on Current Encryption Techniques. *IAIC Transactions on Sustainable Digital Innovation*, *5*(2), 148-157. https://doi.org/10.34306/itsdi.v5i2.662

Bank for International Settlements. (2020). OPE10 Definitions and Application. W: *Basel Committee on Banking Supervision. The Basel Framework* (s. 761-764). Pobrano 2 listopada 2025 z https://gestionderiesgo.org/wp-content/uploads/2021/03/BaselFramework.pdf

Bansal, M., Oberoi, N. i Sameer, M. (2021). IoT in Online Banking. *Journal of Ubiquitous Computing and Communication Technologies*, *2*(4), artykuł 5. https://doi.org/10.36548/JUCCT.2020.4.005

Basel Committee on Banking Supervision. (2024). *Digitalisation of Finance*. Bank for International Settlements. Pobrano 18 maja 2025 z https://www.bis.org/bcbs/publ/d575.pdf

Basha, S. A., Zia, A., Kirankumar, B., Sekhar, S. C., Sumithra, S. i Monisha, J. R. (2025). Artificial Intelligence in Financial Trading Predictive Models and Risk Management Strategies. *ITM Web of Conferences*, *76*, artykuł 01007. https://doi.org/10.1051/itmconf/20257601007

Bell, D. E. i LaPadula, L. J. (1973). *Secure Computer Systems: Mathematical Foundations and Model*. MITRE Corporation Report MTR-2547. Pobrano 2 listopada 2025 z https://apps.dtic.mil/sti/html/tr/AD0770768/index.html

Bernstein, D. J. i Lange, T. (2017). Post-Quantum Cryptography. *Nature*, *549*(7671), 188-194. https://doi.org/10.1038/nature23461

Białas, A. (2006). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Wydawnictwa Naukowo-Techniczne.

Biasse, J. F., Bonnetain, X., Kirshanova, E., Schrottenloher, A. i Song, F. (2022). Quantum Algorithms for Attacking Hardness Assumptions in Classical and Post-Quantum Cryptography. *IET Information Security*, *17*(3), 171-209. https://doi.org/10.1049/ise2.12081

Biggio, B. i Roli, F. (2018). Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. *Pattern Recognition*, *84*, 317-331. https://doi.org/10.1016/j.patcog.2018.07.023

Boer, M. i Vazquez, J. (2017). *Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System*. Institute of International Finance. Pobrano 2 listopada 2025 z https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver%3D2019-02-19-150125-767

Bokkena, B. (2024). Enhancing IT Security with LLM-Powered Predictive Threat Intelligence. W: *2024 Proceedings of the 5th International Conference on Smart Technologies & Systems for Next Generation Computing* (s. 751-756). IEEE.

Boneh, D. (1999). Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the AMS*, *46*(2), 203-213. Pobrano 2 listopada 2025 z https://www.ams.org/journals/notices/199902/boneh.pdf

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. i Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837-864. Pobrano 2 listopada 2025 z https://www.jstor.org/stable/26628654

Brauchle, J.-P., Göbel, M., Seiler, J. i von Busekist, C. (2020). *Cyber Mapping the Financial System*. Cyber Policy Initiative Working Paper Series, „Cybersecurity and the Financial System" No. 6. Carnegie Endowment for International Peace. Pobrano 2 listopada 2025 z https://carnegieendowment.org/files/Brauchle_Cyber_Mapping_the_Financial_System_final.pdf

Brennen, S. i Kreiss, D. (2016). Digitalization. W: K. B. Jensen, R. T. Craig, J. D. Pooley i E. W. Rothenbuhler (red.), *The International Encyclopedia of Communication Theory and Philosophy*. Wiley-Blackwell. https://doi.org/10.1002/9781118766804.wbiect111

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S. J., Belfield, H., Farquhar, S., Lyle, C., … i Amodei, D. (2024). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. arXiv:1802.07228, 2024. https://doi.org/10.48550/arXiv.1802.07228

Buckley, R. P., Arner, D. W., Zetzsche, D. A. i Selga, E. (2019). *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*. European Banking Institute Working Paper No. 2019/54. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640#

Bustos-Tabernero, A., López-Sánchez, D., González-Arrieta, A. i Novais, P. (2024). Study of Infostealers Using Graph Neural Networks. *Logic Journal of the IGPL*, *33*(4), jzae105. https://doi.org/10.1093/jigpal/jzae105

Carter, E. (b.d.). *GPU Password Cracking Benchmarks 2025: RTX vs CPUs*. Online Hash Crack. Pobrano 2 listopada 2025 z https://www.onlinehashcrack.com/guides/password-recovery/gpu-password-cracking-benchmarks-2025-rtx-vs-cpus.php?utm_source=chatgpt.com

Casanova, J., Savoie, M. i Twist, A. (2022). The Regulatory Framework for Payment Services in the EU and UK, W: J. Casanova, M. Savoie (red.), *Payment Services: Law and Practice* (s. 37-100). Edward Elgar Publishing.

CERT. (2025). *Raport Roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu*. Pobrano 2 listopada 2025 z https://cert.pl/uploads/docs/Raport_CP_2024.pdf

Chawda, Y. i Parmar, M. (2025). Toward Intelligent Data Access Control: A Dual-Layered Zero Trust and Blockchain-Based Data Access Model. *Scientific and Practical Cyber Security Journal*, *9*(1). Pobrano 2 listopada 2025 z https://journal.scsa.ge/papers/toward-intelligent-data-access-control-a-dual-layered-zero-trust-and-blockchain-based-data-acess-model/

CheckPoint. (2025). *The State of Cybersecurity 2025*. Pobrano 2 listopada 2025 z https://www.checkpoint.com/security-report/

Chen, H. (2025). The Impact of Fintech on Traditional Banking Industry and Future Development Trends. *Highlights in Business, Economics and Management*, *49*, 191-198. https://doi.org/10.54097/xjdn8360

Chen, X., Ma, C.-Q., Ren, J.-S. i Lei, Y.-T. (2023). Explainable Artificial Intelligence in Finance: A Bibliometric Review. *Finance Research Letters*, *56*, artykuł 104145. https://doi.org/10.1016/j.frl.2023.104145

Chitrakar, L., Panta, I., Paneru, B., Paneru, B., Poudel, S. i Kansakar, L. (2024). *User-Centric Design of Ui for Mobile Banking Apps: Improving Ui and Features for Better Customer Experience*. SSRN. https://ssrn.com/abstract=5056829

Chiu, J. i Koeppl, T. V. (2018). Blockchain-Based Settlement for Asset Trading. *The Review of Financial Studies*, *32*(5), 1716-1753.

Choudhary, S. K. (2025). Real-Time Fraud Detection Using AI-Driven Analytics in the Cloud: Success Stories and Applications. *International Research Journal of Modernization in Engineering Technology and Science*, *7*(2), 4874-4880. https://www.doi.org/10.56726/IRJMETS68076

Cialdini, R. (2023). *Pre-swazja. Jak w pełni wykorzystać techniki wpływu społecznego* (S. Pikiel, Tłum.). Gdańskie Wydawnictwo Psychologiczne.

Cisco. (2024). *Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette*. Cisco Umbrella. Pobrano 2 listopada 2025 z https://umbrella.cisco.com/info/cyber-threat-trends-report

Crowdstrike. (2025). *2025 Global Threat Report*. Pobrano 2 listopada 2025 z https://www.crowdstrike.com/en-us/global-threat-report/

Custom Market Insights. (b.d.). *Global API Banking Market 2024-2033*. Pobrano 2 listopada 2025 z https://www.custommarketinsights.com/report/api-banking-market/

Czechowska, I. D., Stawska, J. i Witczak, R. (2020). *Bezpieczeństwo i stabilność systemu finansowego – perspektywa makro- i mikroekonomiczna*. Wydawnictwo Uniwersytetu Łódzkiego.

Danielsson, J. i Uthemann, A. (2025). *Artificial Intelligence and Financial Crises*. Pobrano 2 listopada 2025 z https://arxiv.org/pdf/2407.17048

Danry, V., Pataranutaporn, P., Groh, M., Epstein, Z. i Maes, P. (2024). *Deceptive AI Systems That Give Explanations Are More Convincing Than Honest AI Systems and Can Amplify Belief in Misinformation*. arXiv:2408.00024. https://doi.org/10.48550/arXiv.2408.00024

Danzig, R. J. (2014). *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Center for a New American Security.

Del Giudice, M., Campanella, F. i Dezi, L. (2016). The Bank of Things: An Empirical Investigation on the Profitability of the Financial Services of the Future. *Business Process Management Journal*, *22*(2), 324-340. https://doi.org/10.1108/BPMJ-10-2015-0139

Deloitte. (2024a). *Generative AI and the Fight for Trust*. Pobrano 2 listopada 2025 z https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-generative-ai-and-the-fight-for-trust.pdf

Deloitte. (2024b). *Generative AI Is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking*. Deloitte Financial Services. Pobrano 2 listopada 2025 z https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

Deloitte. (2025). *Global Risk Management Survey, 12th Edition*. Pobrano 2 listopada 2025 z https://iapp.org/media/pdf/resource_center/Deloitte_Global_Risk_Management_Survey.pdf

Dhieb, N., Ghazzai, H., Besbes, H. i Massoud, Y. (2020). A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2983300

DTCC. (2019). *Systemic Risk Barometer. 2020 Risk Forecast*. Pobrano 2 listopada 2025 z https://www.dtcc.com/-/media/Files/Downloads/Risk-Management/DTCC-Systemic-Risk-2019.pdf

Dugbartey, A. (2025). Systemic Financial Risks in an Era of Geopolitical Tensions, Climate Change, and Technological Disruptions: Predictive Analytics, Stress Testing and Crisis Response Strategies. *International Journal of Science and Research Archive*, *14*(2), 1428-1448. https://doi.org/10.30574/ijsra.2025.14.2.0563

Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: Significance and Applicability. *Journal of Cybersecurity*, *5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę

2007/64/WE (Dz. U. L 337 z 23.12.2015). Pobrano 2 listopada 2025 z https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32015L2366

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. L 333 z 27.12.2022). Pobrano 2 listopada 2025 z https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555

ENISA. (2018). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Union Agency for Network and Information Security. Pobrano 2 listopada 2025 z https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA. (2020). *AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence.* European Union Agency for Cybersecurity. Pobrano 2 listopada 2025 z https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Artificial%20Intelligence%20Cybersecurity%20Challenges.pdf

ENISA. (2025). *Threat Landscape: Finance Sector, January 2023 to June 2024*. European Union Agency for Cybersecurity. Pobrano 2 listopada 2025 z https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector

eSentire. (2025). *Cybercrime to Cost the World $9.5 Trillion USD Annually in 2024*. Pobrano 2 listopada 2025 z https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

European Banking Authority [EBA]. (2025). *Guidelines Amending Guidelines EBA/GL/2019/04 on ICT and Security Risk Management*. Pobrano 2 listopada 2025 z https://www.eba.europa.eu/sites/default/files/2025-02/23684f95-f669-4852-94a0-dac6c2ae67ad/Final%20report%20on%20amending%20GLs%20on%20ICT%20risk%20and%20security.pdf

European Systemic Risk Board. (2020). *Systemic Cyber Risk*. Pobrano 2 listopada 2025 z https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

European Union Agency for Cybersecurity [ENISA]. (2023). AI Cybersecurity Challenges.

Experis. (2025). *The Experis CIO 2025 Outlook: Key Priorities for Tech Leaders*. Pobrano 2 listopada 2025 z https://www.experis.pl/pl/cio-2025-outlook-key-priorities-for-tech-leaders

Farnaaz, N. i Jabbar, M. A. (2016). Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*, *89*, 213-217. https://doi.org/10.1016/j.procs.2016.06.047

Federal Bureau of Investigation. (2024). *Internet Crime Report 2024*. Pobrano 2 listopada 2025 z https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Femighty, S., Caleb, A., Manager, I. i Brown, J. (2022). *Zero Trust Security Models for SMEs in the Era of Cloud Computing*. Pobrano 2 listopada 2025 z https://www.researchgate.net/publication/391458799_Zero_Trust_Security_Models_for_SMEs_in_the_Era_of_Cloud_Computing

Feng, S. (2024). Integrating Artificial Intelligence in Financial Services: Enhancements, Applications, and Future Directions. *Applied and Computational Engineering*, *69*(1), 19-24. https://doi.org/10.54254/2755-2721/69/20241455

Financial Stability Board [FSB]. (2017). *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*. Pobrano 2 listopada 2025 z https://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

Financial Stability Board [FSB]. (2019). *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*. Pobrano 2 listopada 2025 z https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/

Fiore, M., Carrozzino, F., Coppola, G., Guariglia, G. i Mongiello M. (2025). Generating an Iris-Based Seed for Key-Pairs in a Blockchain Platform. *Journal of Communications Software and Systems*, *21*(2),144-155. https://doi.org/10.24138/jcomss-2024-0100

Fujisaki, E., Nishimaki, R. i Tanaka, K. (2009). On the Insecurity of the Fiat-Shamir Signatures with Iterative Hash Functions. W: Pieprzyk, J., Zhang, F. (red.), *Provable Security. Third International Conference, ProvSec 2009, Guangzhou, China, November 11-13, 2009* (Lecture Notes in Computer Science, vol. 5848). Springer. https://doi.org/10.1007/978-3-642-04642-1_11

Gahane, S., Nakhate, D., Ugemuge, K. i Pohankar, R. (2025). The Awareness of Decision Making Process, Data Governance Policies for Quality and Security of Big Data with Cloud Environment and Data Science. W: *International Conference on Emerging Materials, Smart Manufacturing, and Computational Intelligence, 7-8 December 2023, Rajpura, India* (AIP Conference Proceedings, Vol. 3227, artykuł 060007). https://doi.org/10.1063/5.0241639

Gasparski, P. (2016). Myślenie szybkie i wolne a optymizm dotyczący osobistych zasobów pieniężnych. *Studia Ekonomiczne. Economic Studies*, (1(88), 115-134.

Gidney, C. i Ekerå, M. (2021). How to Factor 2048-bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. *Quantum*, *5*, 433-464. https://doi.org/10.22331/q-2021-04-15-433

Giudici, P., Centurell, M. i Turchetta, S. (2024). Artificial Intelligence Risk Measurement. *Expert Systems with Applications*, *235*, artykuł 121220. https://doi.org/10.1016/j.eswa.2023.121220

Giudici, P. i Raffinetti, E., (2023). SAFE Artificial Intelligence in Finance. *Finance Research Letters*, *56*(26), artykuł 104088. https://doi.org/10.1016/j.frl.2023.104088

Główny Urząd Statystyczny [GUS]. (2024). *Społeczeństwo informacyjne w Polsce w 2024 roku. Information Society in Poland in 2024*. Pobrano 2 listopada 2025 z https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku,1,18.html

Gounari, M., Stergiopoulos, G., Pipyros, K. i Gritzalis, D. (2024). Harmonizing Open Banking in the European Union: An Analysis of PSD2 Compliance and Interrelation with Cybersecurity Frameworks and Standards. *International Cybersecurity Law Review*, *5*, 79-120. Pobrano 2 listopada 2025 z https://link.springer.com/article/10.1365/s43439-023-00108-8

Graham, M. i Dutton, W. H. (red.). (2019). *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives* (wyd. 2). Oxford University Press.

Grigorescu, A., Oprisan, O., Lincaru, C. i Pirciog, C. S. (2023). E-Banking Convergence and the Adopter's Behavior Changing Across EU Countries. *SAGE Open*, *13*(4). https://doi.org/10.1177/21582440231220455

Group-IB. (2025). *High-Tech Crime Trends. Report 2025*. Pobrano 2 listopada 2025 z https://www.group-ib.com/landing/high-tech-crime-trends-2025/#form

Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. W: *STOC'96: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (s. 212-219). Association for Computing Machinery. https://doi.org/10.1145/237814.237866

Hadlington, L. (2017). Human Factors in Cybersecurity. Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Wiley.

Hammad, M. (2024). Biometric Security and Access Management in E-health Services. W: M. Hammad, G. Ali, M. A. El-Affendi, Y. Maleh, A. A. Abd El-Latif (red.), *Secure Health. A Guide to Cybersecurity for Healthcare Managers* (s. 76-103). Taylor & Francis. https://doi.org/10.1201/9781003470038-5

Heiding, F., Lermen, S., Kao, A., Schneier, B. i Vishwanath, A. (2024). *Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects*. Pobrano 2 listopada 2025 z arXiv:2412.00586. https://doi.org/10.48550/arXiv.2412.00586

Hettiarachchige, H. H. i Jahankhani, H. (2021). Holistic Authentication Framework for Virtual Agents: UK Banking Industry. W: R. Montasari, H. Jahankhani, H. Al-Khateeb (red.), *Challenges in the IoT and Smart Environments. A Practitioners' Guide to Security, Ethics and Criminal Threats* (s. 245-286). Springer. Pobrano 2 listopada 2025 z https://link.springer.com/chapter/10.1007/978-3-030-87166-6_10

Hoffstein, J., Pipher, J. i Silverman, J. H. (1998). NTRU: A Ring-Based Public Key Cryptosystem. W: J. P. Buhler (red.), *Algorithmic Number Theory. Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings* (s. 267-288). Springer. Pobrano 2 listopada 2025 z https://www.ntru.org/f/hps98.pdf

Horodecki, R. Horodecki, P., Horodecki, M. i Horodecki, K. (2009). Quantum Entanglement. *Review of Modern Physics*, *81*(2). https://doi.org/10.1103/RevModPhys.81.865

Hovav, A. i D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Howcroft, E. (2025). AI-Generated Content Raises Risks of More Bank Runs, UK Study Shows. Reuters. Pobrano 2 listopada 2025 z https://www.reuters.com/technology/artificial-intelligence/ai-generated-content-raises-risks-more-bank-runs-uk-study-shows-2025-02-14

Höhenberger, C. i Redlein, A. (2020). The Prevalence of IoT in the Facility Services Industry. *Journal of Facility Management Education and Research*, *4*(1), 9-13. https://doi.org/10.22361/2474-6630-4.1.9

Iansiti, M. i Lakhani, K. (2019). *The Digital Business Divide: Analyzing the Operating Impact of Digital Transformation*. Microsoft Download Center. Pobrano 2 listopada 2025 z https://download.microsoft.com/download/7/3/5/735BFE87-DF07-4117-929C-A0F194FD24A1/The_Digital_Business_Divide_white_paper_en-GB.pdf

IBM. (2024). *Cost of a Breach Data Report 2024.* Pobrano 2 listopada 2025 z https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Ibrahim, M. M., Venkatesan, R., Ali, N., Qureshi, M. I., Siddiqui, H. M. A., Tolasa, F. T. i Abdallah, S. A. O. (2025). Enhanced Image Hash Using Cellular Automata with Sponge Construction and ECC. *Scientific Reports*, *15*, artykuł 14148. https://doi.org/10.1038/s41598-025-98027-7

Idzik, M. i Gieorgica, J. (2019). Reputacja sektora bankowego w Polsce – wnioski z badania w 2019 roku. *Bezpieczny Bank*, *76*(3), 75-93. https://doi.org/10.26354/bb.4.3.76.2019

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

International Telecommunication Union [ITU]. (1991). *Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800*. Pobrano 2 listopada 2025 z https://www.itu.int/rec/T-REC-X.800-199103-I

Jadhav, A. i Mirza, V. (2025). Large Language Models in Equity Markets: Applications, Techniques, and Insights. *Frontiers in Artificial Intelligence*. Pobrano 2 listopada 2025 z https://www.researchgate.net/publication/395011321_Large_Language_Models_in_equity_markets_applications_techniques_and_insights

Jagatic, T., Johnson, N. A., Jakobsson, M. i Menczer, F. (2007). Social Phishing. *Communications of the ACM*, *50*(10), 94-100. https://doi.org/10.1145/1290958.1290968

Jakobsson, M. i Myers, S. (red.). (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. John Wiley & Sons.

Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar, M. I. i Al Mahmud, M. A. (2024). AI Advances: Enhancing Banking Security with Fraud Detection. W: *First International Conference on Technological Innovations and Advance Computing* (*TIACOMP*), *Bali, 29-30 June 2024* (s. 289-294). https://doi.org/10.1109/tiacomp64125.2024.00055

Johri, S., Singh, S. K., Reddy, C. V., Nijhavan, G., Alawadi, A. H. i Reddy, U. (2023). Improving Security and Effectiveness in Banking Operations with IoT Integration. W: *10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)* (s. 1732-1737). IEEE. https://doi.org/10.1109/UPCON59197.2023.10434723

Kahneman, D. (2023). *Thinking, Fast and Slow*. Penguin Books.

Karbowski, M. (2008). *Podstawy kryptografii*. Helion.

Karina, R., Siti-Nabiha, A. K. i Jurnali, T. (2025). Big Data Integration in Performance Management and Control: A Socio-Technical Perspective. *Journal of Accounting & Organizational Change* (March). https://doi.org/10.1108/JAOC-07-2024-0238

Karmańska, A. (2021). Internet of Things in the Accounting Field – Benefits and Challenges, *31*(3), 23-39. https://doi.org/10.37190/ord210302

Khan, N. i State, R. (2020). Lightning Network: A Comparative Review of Transaction Fees and Data Analysis. W: J. Prieto, A. K. Das, S. Ferretti, A. Pinto, J. M. Corchado (red.), *Blockchain and Applications. International Congress* (s. 11-18). Springer.

Khanna, A. (2024). *Securing an Enterprise. Maximizing Digital Experiences Through Secure Enterprise Design*. Apress.

Kim, A., Park, M. i Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2986882

Kim, S., Chida, M. i Naoyuki, Y. (2025). Cybersecurity and Macroeconomy with Neoclassical Growth Model. SSRN. https://doi.org/10.2139/ssrn.5171075

Kipnis, A., Patarin, J. i Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. W: J. Stern (red.), *Advances in Cryptology – EUROCRYPT'99. International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceedings* (s. 206-222). Springer. https://doi.org/10.1007/3-540-48910-X_15

Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., Gaudry, P., Kruppa, A., Montgomery, P. L., Osvik, D. A., te Riele, H., Timofeev, A. i Zimmermann, P. (2010). Factorization of a 768-bit RSA Modulus. W: T. Rabin (red.), *Advances in Cryptology – CRYPTO 2010. 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010, Proceedings* (s. 333-350). Springer. https://doi.org/10.1007/978-3-642-14623-7_18

Klimczak, K. M., Fryczak, J. M. i Kaużyński, A. (2022). Cyfryzacja jako zmiana strategiczna w polskich spółkach giełdowych. *Organizacja i Kierowanie*, (2(191), 53-66. Pobrano 2 listopada 2025 z https://econjournals.sgh.waw.pl/OiK/article/view/4003

Klimontowicz, M. (2020). Wpływ cyfryzacji na modele biznesowe i operacyjne banków. W: E. Miklaszewska, M. Folwarski (red.), *Bankowość emocjonalna. Cyfrowa transformacja banków a oczekiwania klientów* (s. 149-159). Wydawnictwo Poltext.

Koblitz, N. (1995). *Wykład z teorii liczb i kryptografii* (W. Guzicki, Tłum.). Wydawnictwa Naukowo-Techniczne.

Koblitz, N. (2000). *Algebraiczne aspekty kryptografii* (W. Kraśkiewicz, Tłum.). Wydawnictwa Naukowo-Techniczne.

Kolias, C., Kambourakis, G., Stavrou, A. i Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/MC.2017.201

Komisja Europejska/Europejska Agencja Wykonawcza ds. Edukacji i Kultury/Eurydice. (2024). *Nauczanie informatyki w szkołach w Europie. Raport Eurydice*. Pobrano 2 listopada 2025 z https://www.frse.org.pl/brepo/panel_repo_files/2024/03/26/i4dnec/nuaczanieinformatyki-pl.pdf

Komisja Nadzoru Finansowego [KNF]. (2024). *Planowane uchylenie rekomendacji i wytycznych dot. zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz odwołanie komunikatu chmurowego w związku z rozpoczęciem stosowania Rozporządzenia DORA*. Pobrano 2 listopada 2025 z https://www.knf.gov.pl/?articleId=91750&p_id=18

Kost, E. (2025). *10 Biggest Data Breaches in Finance*. Upguard. Pobrano 2 listopada 2025 z https://www.upguard.com/blog/biggest-data-breaches-financial-services

Kshetri, N. (2025). *Cybersecurity in Financial Services: Challenges and Strategic Responses*. Springer.

Kumar, R. (2022). Cloud Cybersecurity: Navigating Evolving Threats and Architecting Resilient Defenses. *Journal of Software Engineering and Simulation*, *8*(8), 21-29. https://doi.org/10.35629/3795-08082129

Kumar, S., Singh, N. P. i Kumar, N. (2022). Literature Review of Distributed Denial of Service (DDoS) Attacks, Its Detection Techniques and Prevention Mechanisms. *International Journal for Research in Applied Science and Engineering Technology*, *10*(9), 1681-1685. https://doi.org/10.22214/ijraset.2022.46882

Kutyłowski, M. i Strothmann, W. B. (1999). *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych*. Lupus, Oficyna Wydawnicza Read Me.

Kuźnar, A. (2019). Cyfryzacja polskiej gospodarki i wykorzystanie innowacji informatycznych oraz *Big Data* przez polskie przedsiębiorstwa. W: A. M. Kowalski, M. A. Weresa (red.), *Polska – Raport o konkurencyjności 2019. Konkurencyjność międzynarodowa w kontekście rozwoju przemysłu 4.0* (s. 275-293). Oficyna Wydawnicza SGH.

Lande, R. S., Meshram, S. A. i Deshmukh, P. P. (2018). Smart Banking Using IoT. W: *Proceedings of the International Conference on Research in Intelligent and Computing in Engineering RICE III*. IEEE.

Larriva-Novo, X., Sánchez-Zas, C., Villagrá, V. A., Marín-Lopez, A. i Berrocal, J. (2023). Leveraging Explainable Artificial Intelligence in Real-Time Cyberattack Identification: Intrusion Detection System Approach. *Applied Sciences*, *13*(15), artykuł 8587. https://doi.org/10.3390/app13158587

Laxman, V., Ramesh, N., Prakash, S. K. J. i Aluvala, R. (2024). Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review. *Journal of Digital Economy*, *3*, 205-222. https://doi.org/10.1016/j.jdec.2025.04.002

Lenstra, A. K. i Lenstra, H. W. (red.). (1993). *The Development of the Number Field Sieve* (Lecture Notes in Mathematics). Springer.

Leżoń, K. (2019). *Otwarta bankowość w świetle wymogów dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*. Urząd Komisji Nadzoru Finansowego.

Liao, Z. (2024). *Towards Building Trustworthy Blockchain-Enabled Decentralized Applications: Data Feeds Reliability, Multi-Service Authentication* (student dissertation, Iowa University). https://doi.org/10.31274/td-20250502-236

Lickus, P. (2012). The Value of Social Network as Function of Number of Users. *International Journal of Economics and Finance Studies*, *4*(1), 181-189.

Lin, I.-C. i Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653-659. https://doi.org/10.6633/IJNS.201709.19(5).01

Lukogo, C. C., Muriira, L. M. i Murungi, R. M. (2024). Deep Learning Network Intrusion Detection with the Conv1d-Lstm Model: Integrating CNN and LSTM For Superior Performance. *International Journal of Professional Practice*, *12*(4), 41-49. https://doi.org/10.71274/ijpp.v12i4.475

Luong, T.-T., Luong, V.-G., Tran, A. H. T. i Nguyen, T. M. (2025). Application of Machine Learning Techniques for Customer Churn Prediction in the Banking Sector. *Interdisciplinary Journal of Information, Knowledge and Management*, *20*, 009. https://doi.org/10.28945/5469

Lyubashevsky, V., Peikert, C. i Regev, O. (2010). On Ideal Lattices and Learning with Errors Over Rings. W: H. Gilbert (red.), *Advances in Cryptology – EUROCRYPT 2010. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30-June 3, 2010, Proceedings* (s. 1-23). Springer. https://doi.org/10.1007/978-3-642-13190-5_1

MacKay, D. J. C. (2003). *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press.

Mahjabin, T., Xiao, Y., Sun, G. i Jiang, W. (2017). Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques. *International Journal of Distributed Sensor Networks*, *13*(12). https://doi.org/10.1177/1550147717741463

Małek, A. (2020). Internet of Things (IoT): Considerations for Life Insurers. W: M. Borda, S. Grima, I. Kwiecień (red.), *Life Insurance in Europe* (s. 177-202). Springer. https://doi.org/10.1007/978-3-030-49655-5_12

Manwani, P. (2025). AI-Enhanced Customer Authentication and Onboarding. *International Journal of Trend in Scientific Research and Development*, *9*(2), 683-692. Pobrano 2 listopada 2025 z https://www.ijtsrd.com/papers/ijtsrd78505.pdf

Marciszewski, W. (2011). Na czym polega świadomość informatyczna. W: W. Marciszewski, P. Stacewicz, *Umysł – Komputer – Świat. O zagadce umysłu z informatycznego punktu widzenia* (s. 211-219). Akademicka Oficyna Wydawnicza EXIT.

Masri, I. H. i Susanti, B. H. (2025). Hortex: A Chaotic Sponge Hash Function. *IAENG International Journal of Computer Science*, *52*(2), 491-506. Pobrano 2 listopada 2025 z https://www.researchgate.net/profile/Bety-Susanti/publication/390997999

Mecke, L., Saad, A., Prange, S., Gruenefeld, U., Schneegass, S. i Alt, F. (2024). *Do They Understand What They Are Using? – Assessing Perception and Usage of Biometrics*. https://doi.org/10.48550/arXiv.2410.12661

Menezes, A. J., van Oorschot, P. C. i Vanstone, S. A. (2005). *Kryptografia stosowana* (E. Andrukiewicz, W. Chocianowicz, K. Janowski, J. Pejaś, Tłum.). Wydawnictwa Naukowo-Techniczne.

Micciancio, D., Regev, O. (2009). Lattice-Based Cryptography. W: D. J. Bernstein, J. Buchmann, E. Dahmen (red.). *Post-Quantum Cryptography*. Springer.

Mirkovic, J. i Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53. https://doi.org/10.1145/997150.997156

Mirsky, Y. i Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys*, *54*(1), artykuł 7. https://doi.org/10.1145/3425780

Moody, D., Perlner, R., Regenscheid, A., Robinson, A. i Cooper, D. (2024). *Transition to Post-Quantum Cryptography Standards*. NIST Internal Report NIST IR 8547. https://doi.org/10.6028/NIST.IR.8547.ipd.pdf

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, *16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A. i Dwivedi, Y. K. (2023). Deepfakes: Deceptions, Mitigations, and Opportunities. *Journal of Business Research*, *154*, artykuł 113368. https://doi.org/10.1016/j.jbusres.2022.113368

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Pobrano 2 listopada 2025 z https://bitcoin.org/bitcoin.pdf

Naqvi, B., Wolff, A. i Racanelli, D. (2025). Equitable Cybersecurity: Towards Generating Requirements Through the Lens of Security Literacy. *Information and Software Technology*, *188*, artykuł 107891. https://doi.org/10.1016/j.infsof.2025.107891

Narayanan, A., Bonneau, J., Felten, E., Miller, A. i Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Narodowy Bank Polski. (2019). *Raport o stabilności systemu finansowego, grudzień 2019*. Departament Stabilności Finansowej. Pobrano 2 listopada 2025 z https://nbp.pl/wp-content/uploads/2022/09/rsf122019.pdf

National Institute of Standards and Technology [NIST]. (2022). *Cybersecurity Framework Profile for Financial Services*. NIST IR 8383, 2022.

National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Niederreiter, H. (1986). Knapsack-Type Cryptosystems and Algebraic Coding Theory. *Problems of Control and Information Theory*, *15*, 159-166. https://ci.nii.ac.jp/naid/80003180051

Nielsen, M. A. i Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.

Oest, A., Zhang, P., Wardman, B., Nunes, S., Burgis, J., Zand, A., Thomas, K., Dupé, A. i Ahn, G.-J. (2020). Sunrise to Sunset: Analyzing the End-to-End Life Cycle and Effectiveness of Phishing Attacks at Scale. W: *SEC'20: Proceedings of the 29th USENIX Conference on Security Symposium* (s. 361-377). USENIX Association. https://dl.acm.org/doi/10.5555/3489212.3489233

Office of Financial Research. (2017). *Cybersecurity and Financial Stability: Risks and Resilience*. Pobrano 2 listopada 2025 z https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

Ogunmolu, A. M. (2025). Leveraging Generative AI and Behavioral Biometrics to Strengthen Zero Trust Cybersecurity Architectures in Healthcare Systems. *Journal of Engineering Research and Reports*, *27*(5), 194-213. https://doi.org/10.9734/jerr/2025/v27i51502

Olenick, D. (2020). *Garmin Reportedly Paid a Ransom. Company Says 'Temporary Limitations' on Services Continue*. Bank Info Secutity. Pobrano 2 listopada 2025 z https://www.bankinfosecurity.com/garmin-reportedly-paid-ransom-a-14773

Otoum, S., Kantarci, B. i Mouftah, H. (2020). A Comparative Study of AI-Based Intrusion Detection Techniques in Critical Infrastructures. *ACM Transactions on Internet Technology*, *21*(4), artykuł 81. https://doi.org/10.1145/3406093

Ozili, P. K. (2023). Role of Embedded Finance in Increasing Financial Inclusion. W: *IGI Book: Adoption and Use of Technology Tools and Services by Economically Disadvantaged Communities: Implications for Growth and Sustainability*. https://doi.org/10.2139/ssrn.4629444

Parviainen, P., Tihinen, M., Kääriäinen, J. i Teppola, S. (2017). Tackling the Digitalization Challenge: How to Benefit from Digitalization in Practice. *International Journal of Information Systems and Project Management*, *5*(1), 63-77. https://doi.org/10.12821/ijispm050104

Pasławski, K. (2024). *Polskie banki są atakowane 1728 razy tygodniowo*. CRN. Pobrano 2 listopada 2025 z https://crn.pl/aktualnosci/polskie-banki-sa-atakowane-1728-razy-tygodniowo

Password Hashing Competition and Our Recommendation for Hashing Passwords: Argon2. (b.d.). Pobrano 2 listopada 2025 z https://www.password-hashing.net/

Pieprzyk, J., Hardjono, T. i Seberry J. (2003). *Teoria bezpieczeństwa systemów komputerowych* (T. Żmijewski, A. Grażyński, Tłum.). Helion.

Pieriegud, J. (2016). Cyfryzacja gospodarki i społeczeństwa – wymiar globalny, europejski i krajowy. W: J. Gajewski, W. Paprocki, Pieriegud J. (red.), *Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych* (s. 11-37). Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa.

Pigola, A. i de Souza Meirelles, F. (2025). Zero Trust in Cybersecurity: Managing Critical Challenges for Effective Implementation. *Journal of Systems and Information Technology*. https://doi.org/10.1108/JSIT-08-2024-0326

Poirrier, A., Cailleux, L. i Clausen, C. H. (2025). Is Trust Misplaced? A Zero-Trust Survey. *Proceedings of the IEEE*, *113*(1), 5-39. https://doi.org/10.1109/JPROC.2025.3555131

Pomerance, C. (1996). A Tale of Two Sieves. *Notices of the AMS*, *43*(12), 1473-1485. Pobrano 2 listopada 2025 z https://www.ams.org/notices/199612/pomerance.pdf

Ponemon Institute. (2021). *The 2021 Cost of Phishing Study*. Pobrano 2 listopada 2025 z https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-ponemon-2021-cost-of-phishing-study.pdf

Pool, J. H. i Venter, H. (2022). A Harmonized Information Security Taxonomy for Cyber Physical Systems. *Applied Sciences*, *12*(16), artykuł 8080. https://doi.org/10.3390/app12168080

Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond. *Quantum*, *2*, 79-101. https://doi.org/10.22331/q-2018-08-06-79

Purnell, M. (2025). *Open Banking APIs Market 2025-2029*. Juniper Research. Pobrano 29 maja 2025 z https://www.juniperresearch.com/research/fintech-payments/banking/open-banking-apis-market-research-report/

PWN. (b.d.). Cyfryzacja. W: Słownik języka polskiego. Pobrano 17 maja 2025 z https://sjp.pwn.pl/sjp/cyfryzacja;2553935.html

Ramalingam, H. i Venkatesan, V. (2019). Conceptual Analysis of Internet of Things Use Cases in Banking Domain. W: *IEEE Region 10 Conference TENCON* (s. 2034-2039). IEEE. https://doi.org/10.1109/TENCON.2019.8929473

Ramesh, J. V. N., Rajesh, M. V., Veerajyothi, B., Sowmya V. J., Verma, A. i Ghodhbani, R. (2025). Strengthening Security Protocol to Combat Financial Fraud: Advances in Authentication and Access Control. *Journal of Theoretical and Applied Information Technology*, *103*(7). Pobrano 2 listopada 2025 z https://www.researchgate.net/publication/391161799

Regev, O. (2009). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, *56*(6), artykuł 34. https://doi.org/10.1145/1568318.1568324

Rigaki, M. i Garcia, S. (2018). Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection. W: *2018 IEEE Symposium on Security and Privacy Workshops SPW 2018* (s. 70-75). https://doi.org/10.1109/SPW.2018.00019

Rivest, R. L., Shamir, A. i Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21*(2), 120-126. https://doi.org/10.1145/359340.359342

Rizvi, I., Raj, S. i Singh, V. (2025). Cybersecurity in the Digital Age. W: L. O. Yesufu, P. N. E. Nohuddin (red.), *Technology for Societal Transformation* (s. 131-148). Springer. https://doi.org/10.1007/978-981-96-1721-0_8

Robling Denning, D. E. (1992). *Kryptografia i ochrona danych* (B. Szafrański, Tłum.). Wydawnictwa Naukowo-Techniczne.

Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Dz. U. L 69 z 13.03.2018). Pobrano 2 listopada 2025 z https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32018R0389

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. L 151 z 7.06.2019). Pobrano 2 listopada 2025 z https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. U. L 333 z 27.12.2022. Pobrano 2 listopada 2025 z https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32022R2554

Salampasis, D. (2025). Advances on Fintech-Based Lending Practices: Orchestrating the Dialogue on Transformative Innovation. W: M Moussa, A. McMurray (red.), *The Palgrave Handbook of Breakthrough Technologies*. Springer.

Salih, R. K. i Kashmar, A. H. (2024). Enhancing Blockchain Security by Developing the SHA256 Algorithm. *Iraqi Journal of Science*, *65*(10), 5678-5693. https://doi.org/10.24996/ijs.2024.65.10.30

Saltzer, J. H. i Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Proceedings of the IEEE*, *63*(9), 1278-1308. https://doi.org/10.1109/PROC.1975.9939

Sandhu, R., Coyne, E. J., Feinstein, H. L. i Youman, C. E. (1996). Role-Based Access Control Models. *Computer*, *29*(2), 38-47. https://doi.org/10.1109/2.485845

Schneier, B. (1995). *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C* (R. Rykaczewski, R. Sobczak, P. Szpryngier, Tłum.). Wydawnictwa Naukowo-Techniczne.

Schulte, P. i Liu, G. (2017). FinTech Is Merging with IoT and AI to Challenge Banks: How Entrenched Interests Can Prepare. *The Journal of Alternative Investments*, *20*(3), 41-57. https://doi.org/10.3905/jai.2018.20.3.041

Securelist. (2015). *The Great Bank Robbery: The Carbanak APT*. Securelist by Kaspersky. Pobrano 2 listopada 2025 z https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732

Sen, J. (2013). Security and Privacy Issues in Cloud Computing. W: A. Ruiz-Martinez, R. Marin-Lopez, F. Pereniguez-Garcia (red.), Architectures and Protocols for Secure Information Technology Infrastructures (s. 1-45). IGI-Global. https://doi.org/10.4018/978-1-4666-4514-1.ch001

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Sharif, M., Bhagavatula, S., Bauer, L. i Reiter, M. K. (2019). A General Framework for Adversarial Examples with Objectives. *ACM Transactions on Privacy and Security*, *22*(3), artykuł 16. https://doi.org/10.1145/3317611

Shepherd, C., Petitcolas, F. A. P., Akram, R. N. i Markantonakis, K. (2017). An Exploratory Analysis of the Security Risks of the Internet of Things in Finance. W: J. Lopez, S. Fischer-Hübner, C. Lambrinoudakis (red.), *Trust and Privacy in Digital Business. 14th International Conference, TrustBus 2017, Lyon, France, August 30-31, 2017, Proceedings* (Lecture Notes in Computer Science, vol. 10442, s. 164-179). Springer. https://doi.org/10.1007/978-3-319-64483-7_11

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26*(5), 1484-1509. https://doi.org/10.1137/S0097539795293172

Singh, J. i Behal, S. (2020). Detection and Mitigation of DDoS Attacks in SDN: A Comprehensive Review, Research Challenges and Future Directions. *Computer Science Review*, *37*, artykuł 100279. https://doi.org/10.1016/j.cosrev.2020.100279

Souppaya, M. i Scarfone, K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (Special Publication 800-83, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-83r1

Stevens, M., Bursztein, E., Karpman, P., Albertini, A. i Markov, Y. (2017). The First Collision for Full SHA-1. W: J. Katz, H. Shacham (red.), *Advances in Cryptology – CRYPTO 2017. 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part I* (s. 570-596). Springer. Pobrano 2 listopada 2025 z https://www.researchgate.net/publication/318750485

Sunna, A. A., Sultana, T., Kshetri, N. i Uddin, M. M. (2025). AssessCICA: Assessing and Mitigating Financial Losses from Cyber Attacks with Role of Cyber Insurance in Post-Pandemic Era. W: *13th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE. https://doi.org/10.1109/ISDFS65363.2025.11012092

Surabhi, R. i Shiva, K. (2024). Evolution of FinTech: A Systematic Literature Review. *Nowoczesne Systemy Zarządzania. Modern Management Systems*, *19*(2), 49-62. https://doi.org/10.37055/nsz/200426

Swayne, M. (2025). *Google Researcher Lowers Quantum Bar to Crack RSA Encryption*. Quantum Insider. Pobrano 2 listopada 2025 z https://thequantuminsider.com/2025/05/24/google-researcher-lowers-quantum-bar-to-crack-rsa-encryption/

Szumski, O. (2018). Cybersecurity Best Practices Among Polish Students. *Procedia Computer Science*, *126*, 1271-1280. https://doi.org/10.1016/j.procs.2018.08.070

Tabakow, M., Korczak, J. i Franczyk, B. (2014). Big Data – definicje, wyzwania i technologie informatyczne. *Informatyka Ekonomiczna. Business Informatics*, (1(31)), 138-153. https://doi.org/10.15611/ie.2014.1.12

Taib, R., Yu, K., Berkovsky, S., Wiggins, M. i Bayl-Smith, P. (2019). Social Engineering and Organizational Dependencies in Phishing Attacks. W: D. Lamas, F. Loizides (red.), *IFIP TC13 International Conference on Human-Computer Interaction. Paphos, Cyprus, September 2–6, 2019, Proceedings, Part I* (s. 564-584). Springer. https://doi.org/10.1007/978-3-030-29381-9_35

Tao, Y., Yang, R., Zeng, K., Yin, C., Lu, Y., Lu, W., Shi, Y., Wang, B. i Huang, B. (2025). FLFT: A Large-Scale Pre-Training Model Distributed Fine-Tuning Method That Integrates Federated Learning Strategies. *IEEE Access*, *13*, 56439-56453. https://doi.org/10.1109/ACCESS.2025.3549819

Thirumagal, P. G., Das, T., Das, S., Khatri, E., Kiran, S. i Rani, S. (2024). The Role of IoT in Revolutionizing Payment Systems and Digital Transactions in Finance. W: G. C. Mahato, Sangeeta, S. Dash (red.), *5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)* (s. 171-176). IEEE. https://doi.org/10.1109/ICRTCST61793.2024.10578351

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, *59*(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433

Tyagi, S., Tyagi, A., Rani, S., Kumar, A., Adhav, S. i Gupta S. (2025). The Role of Artificial Intelligence in Risk Management and Fraud Detection in Financial Services. *Journal of Informatics Education and Research*, *5*(1), 112-118. https://doi.org/10.52783/jier.v5i1.1964

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2011 r. Nr 199, poz. 1175). Pobrano 2 listopada 2025 z https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20111991175

Vegesna, R. (2025). Proactive Maintenance Alerts for ATG and Dispensers Based on Usage Patterns: Advanced Software Solutions for Fuel System Optimization. *International Scientific Journal of Engineering and Management*, *4*(2), 1-8 https://doi.org/10.55041/ISJEM02261

Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Enterprise. Pobrano 2 listopada 2025 z https://www.verizon.com/business/resources/reports/dbir/

Vo, H. V., Du, H. P. i Nguyen, H. N. (2024). APELID: Enhancing Real-Time Intrusion Detection with Augmented WGAN and Parallel Ensemble Learning. *Computers & Security*, *136*, artykuł 103567. https://doi.org/10.1016/j.cose.2023.103567

Von Neumann, J. (1966). *Theory of Self-Reproducing Automata* (A. W. Burks, red.). University of Illinois Press. Pobrano 2 listopada 2025 z https://archive.org/details/theoryofselfrepr00vonn_0/page/n19/mode/2up

Von Solms, R. i van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Vuorikari, R., Kluzer S. i Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens – with New Examples of Knowledge, Skills and Attitudes*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/115376

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., i Siddiqui, N. A. (2025). Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(1), 226-257. https://doi.org/10.63125/fh49gz18

Warburton, D. (2020). *2020 Phishing and Fraud Report*. F5 Labs. Pobrano 2 listopada 2025 z https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

Wawrzyniak, D. (2012). *Ryzyko informatyczne w działalności bankowej*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Wawrzyniak, D. (2016). Nowe spojrzenie na ryzyko informatyczne w działalności bankowej. W: A. Nosowski, D. Wawrzyniak, G. Woźniewska (red.), *Oblicza bankowości*. Polskie Wydawnictwo Ekonomiczne.

Welschenbach, M. (2002). *Kryptografia w C i C++* (P. Walczak, Tłum.). Mikom.

Wikipedia. (b.d.). 2015-2016 SWIFT Banking Hack. W: Wikipedia. The Free Encyclopedia. Pobrano 16 maja 2025 z https://en.wikipedia.org/wiki/2015–2016_SWIFT_banking_hack

Williams, M., Yussuf, M. F. i Olukoya, A. O. (2021). Machine Learning for Proactive Cybersecurity Risk Analysis and Fraud Prevention. *International Journal of Engineering Technology Research & Management*, *5*12, 160-177. https://doi.org/10.5281/zenodo.14735561

Winkler, I. (2002). Przedmowa. W: D. L. Pipkin, *Bezpieczeństwo informacji* (E. Andrukiewicz, Tłum.). Wydawnictwa Naukowo-Techniczne.

Wrzosek, M. (2023). Suwerenność cyfrowa. W: L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe, nowe tendencje i możliwości* (s. 9-30). Oficyna Wydawnicza Politechniki Warszawskiej.

Xie, T. i Kang, W. (2025). A Random-Binding Based Bio-Hashing Template Protection Method for Palm Vein Recognition. *IEEE Transactions on Information Forensics and Security*, *20*, 4243-4255. https://doi.org/10.1109/TIFS.2025.3559791

Xu, H., Niu, K., Lu, T. i Li, S. (2024). Leveraging Artificial Intelligence for Enhanced Risk Management in Financial Services: Current Applications and Future Prospects. *Engineering Science & Technology Journal*, *5*(8), 2402-2426. https://doi.org/10.51594/estj.v5i8.1363

Yarovenko, H., Lyeonov, S., Wojcieszek, K. A. i Szira, Z. (2023). Do IT Users Behave Responsibly in Terms of Cybercrime Protection? *Human Technology*, *19*(2), 178-206. https://doi.org/10.14254/1795-6889.2023.19-2.3

Zachariadis, M. i Ozcan, P. (2017). *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*. SWIFT Institute Working Paper No. 2016-001. https://doi.org/10.2139/ssrn.2975199

Zaffer, Z., Thadathii, T. J. i Wagh, S. (2025). AI and Finance: A Study of Stakeholder Perceptions on Operational and Experiential Evolution. *Integrated Journal for Research in Arts and Humanities*, *5*(1), 107-114. https://doi.org/10.55544/ijrah.5.1.15

Zamfirescu, R., Rughinis, C., Hosszu, A. i Cristea, D. (2019). Cyber-Security Profiles of European Users: A Survey. W: *2019 22nd International Conference on Control Systems and Computer Science CSCS 2019* (s. 438-442). IEEE. https://doi.org/10.1109/CSCS.2019.00080

Zetter, K. (2025). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Ohio State University.

Zetzsche, D. A., Arner, D. W., Buckley, R. P. i Tang, B. (2020). *Artificial Intelligence in Finance: Putting the Human in the Loop*. CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, No. 1, University of Hong Kong Faculty of Law Research Paper No. 2020/006. Pobrano 2 listopada 2025 z https://ssrn.com/abstract=3531711

Zhang, P., Shi, X. i Khan, S. U. (2017). Can Quantitative Finance Benefit from IoT? W: *SmartIoT '17: Proceedings of the Workshop on Smart Internet of Things,* artykuł 12. Association for Computing Machinery. https://doi.org/10.1145/3132479.3132491

Zwilling, M., Klien, G. Lesjak, D., Wiechetek, Ł., Cetin, F. i Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computational Information Systems*, *62*(1), 82-97 https://doi.org/10.1080/08874417.2020.1712269

Spis rysunków

Spis tabel