DOI: 10.26354/bb.2.3.96.2024

Marek Kot*
ORCID: 0000-0002-3293-2377
marek.kot@ue.wroc.pl

Ocena odporności banków na przestępstwa finansowe

Streszczenie

Artykuł dotyczy przestępstw finansowych w sektorze bankowym, ze szczególnym uwzględnieniem przestępstw przeciwko bankom komercyjnym. Przeanalizowano w nim definicje przestępstw finansowych i odporności na nie. Systematyczny przegląd literatury, wzbogacono o raport z badania ankietowego wśród ekspertów z banków notowanych na Warszawskiej Giełdzie Papierów Wartościowych, a także wykorzystano metodę porównywania parami w ramach *Analytical Hierarchy Process* (AHP).

Wynikiem prac badawczych jest zestaw kryteriów oceny odporności banku na przestępstwa finansowe. Natomiast badanie ankietowe miało na celu walidację tych kryteriów.

Słowa kluczowe: przestępstwa finansowe, odporność, sektor bankowy, bankowość

Kody JEL: G100, G210

Evaluation criteria of a banks' resilience to financial crimes

Abstract

The article concerns financial crimes in the banking sector, with particular emphasis on crimes against commercial banks. It analyses the definitions of financial crimes and resilience to them as well as develops a catalogue of such crimes.

The article uses tools such as a systematic literature review, which is enriched with a report from a survey among experts from banks listed on the Warsaw Stock Exchange. It also uses the pairwise comparison method within the Analytical Hierarchy Process (AHP). The article

* Marek Kot – Uniwersytet Ekonomiczny we Wrocławiu.
** Badanie ankietowe wykorzystane w artykule zostało sfinansowane z grantu wewnętrznego Wydziału Ekonomii i Finansów Uniwersytetu Ekonomicznego we Wrocławiu (nr decyzji: DEF-B.4500.2024.22), a w treści artykułu wykorzystuję fragmenty rozprawy doktorskiej autora.

describes the results of research on the resilience of banks to financial crimes. The result of the research is a set of criteria for assessing the resilience of banks to financial crimes. The survey was aimed at validating these criteria.

Key words: financial crimes, resilience, banking sector, banking

JEL Codes: G100, G210

Wstęp

Dzięki rozwojowi regulacji i technologii oraz zmianom na rynku przestępczość finansowa w ostatnich latach znacząco ewoluowała. Jej coraz silniejszy negatywny wpływ na gospodarkę jest stymulowany przynajmniej dwojako. Po pierwsze, z natury przestępstw finansowych pojawiają się ofiary, niezależnie od tego, czy skutki mają charakter pośredni czy bezpośredni. Ofiarami przestępców mogą być wybrane sektory, a nawet gospodarki kraju, częściej zaś pojedyncze instytucje czy osoby fizyczne, jako podmioty. Po drugie, zjawisko przestępczości finansowej z roku na rok przybiera na sile (Reurink 2019). Skutki tych przestępstw mogą oznaczać dla ofiar niekorzystny wpływ na wyniki finansowe, stratę materialną, negatywny rozgłos lub pogorszenie reputacji, obniżenie wyceny rynkowej, a nawet sankcje prawne lub regulacyjne (Deloitte 2019). Z tych powodów instytucje finansowe powinny podejmować wszelkie dostępne działania w celu zwiększenia swojej odporności na tego typu zagrożenia.

Odporność banków na przestępstwa finansowe jest znacząca także dla ich własnego bezpieczeństwa oraz ich klientów, niekiedy nawet dla stabilności systemu finansowego.

Instytucje finansowe mogą odgrywać jedną z trzech ról w tego rodzaju przestępstwach: ofiary, sprawcy lub środka realizacji (International Monetary Fund 2001). Rozważania w artykule koncentrują się na przestępstwach finansowych przeciw dużym bankom, gdzie banki, a zwłaszcza ich infrastruktura lub ich klienci, są celem przestępców.

W badaniach wykorzystano systematyczny przegląd literatury, badanie ankietowe wśród ekspertów oraz analizy z wykorzystaniem metody porównywania parami w ramach *Analytical Hierarchy Process* (AHP). Przeprowadzony przegląd literatury nie pozwolił zidentyfikować pozycji bezpośrednio i *explicite* poświęconych kryteriom i ocenie odporności banków na przestępstwa finansowe. Stanowiło to asumpt do podjęcia własnych badań w tym zakresie.

Celem artykułu jest opracowanie zestawu kryteriów oceny odporności banku na przestępstwa finansowe. Opracowany zestaw kryteriów poddano walidacji w sondażu ankietowym wśród ekspertów z zakresu przeciwdziałania przestępstwom finansowym w badanych bankach, działających na polskim rynku. Kryteria oceny odporności zostały opracowane na podstawie analizy danych udostępnianych przez badane banki, co stanowi o prawomocności ustaleń.

W rezultacie procesu badawczego powstał zestaw kryteriów i subkryteriów oceny odporności banków obejmujący takie obszary, jak: pranie pieniędzy, finansowanie terroryzmu, korupcję, oszustwa kredytowe oraz cyberprzestępczość. Poszczególnym kryteriom przypisano współczynniki wagowe. Opracowana procedura umożliwia kompleksową ocenę odporności banku na każde z wyróżnionych przestępstw finansowych. Do katalogu takich przestępstw, na podstawie przeprowadzonego przeglądu literatury, zaliczono: pranie pieniędzy, finansowanie terroryzmu, korupcję, oszustwa kredytowe oraz cyberprzestępczość. Jednak w rzeczywistości zakres ten jest szerszy.

Redakcyjny limit objętości artykułu wymusił pominięcie wielu wyjaśnień czy rozwinięć, jakie znajdują się w przygotowywanej rozprawie doktorskiej.

1. Definicje

1.1. Definicja i katalog przestępstw finansowych

Zagrożenia, jakie stwarza przestępczość finansowa dla międzynarodowego systemu finansowego, mają często charakter globalny i wymagają zarówno kompleksowych, jak i skoordynowanych działań instytucji krajowych oraz organizacji czy struktur międzynarodowych, reakcji i jasnego ukierunkowania polityki publicznej. Walka z przestępczością finansową wymaga rozległych specjalistycznych uzgodnień, regulacji i współpracy, mających na celu działania profilaktyczne, jak i skuteczne przeciwdziałanie przepływu nielegalnych środków finansowych, służących m.in. akcjom terrorystycznym, oszustwom na wielką skalę, a ostatnio coraz częściej cyberprzestępczości. Integralność finansów i stabilność systemu finansowego są zagrożone przez coraz bardziej zaawansowaną międzynarodową przestępczość (Deloitte 2022). Jednak A. Pilarczyk dowodzi, że nieprzestrzeganie obowiązujących regulacji lub procedur w niemały sposób umożliwia dokonywanie przestępstw finansowych, które przyczyniają się do znaczących strat operacyjnych banków (Pilarczyk 2016).

W literaturze nie ma jednej definicji przestępstwa finansowego (Reurink 2019), zwłaszcza w publikacjach polskojęzycznych. Różnorodność odzwierciedla m.in. indywidualność autora, charakter instytucji, specyfikę norm prawnych kraju, w którym jest formułowana (International Monetary Fund 2001). Zresztą w języku codziennym albo publicystyce częściej występują określenia ‘oszustwo’, ‘nadużycie finansowe’ lub ‘nadużycie/przestępstwo gospodarcze’ niż ‘przestępstwo finansowe’ .

W. Jasiński (2014) definiuje nadużycia gospodarcze jako nieprawidłowości w obrocie gospodarczym, a także w działalności zawodowej wykonywanej w sposób zorganizowany i ciągły. W opracowaniu definicji przestępstwa finansowego istotne znaczenie ma baza danych obejmująca oszustwa lub nadużycia finansowe, które mają konotację szerszą. W polskim porządku prawnym przestępstwo można zdefiniować jako zachowanie człowieka będące czynem realizującym znamiona określone w ustawie karnej, naruszającym normę sankcjonowaną (Bojarski 2015).

Proczek, Szczepańska (2017) nadużycie finansowe określają jako działanie lub zaniechanie, łącznie z podaniem błędnych informacji, które w sposób świadomy lub lekkomyślny wprowadza w błąd lub usiłuje wprowadzić w błąd stronę w celu osiągnięcia korzyści finansowej lub innej korzyści albo uniknięcia zobowiązania. Biuro Statystyki Wymiaru Sprawiedliwości USA określa nadużycie jako celowe i świadome oszukanie ofiary, poprzez wprowadzanie jej w błąd, ukrywanie lub pomijanie informacji dotyczących obiecanych towarów, usług lub innych korzyści, których sprawca nie miał zamiaru dostarczyć w celu osiągnięcia korzyści pieniężnych (Morgan 2017). Zbliżoną definicję nadużycia finansowego opracowało Stowarzyszenie Biegłych ds. Wykrywania Nadużyć Gospodarczych, Audytorów Wewnętrznych oraz Amerykańskiego Instytutu Biegłych Rewidentów (ACFE, IIA, AICPA 2007).

Przestępstwo finansowe *per se* popełniane jest bez użycia przemocy, a jego skutkiem jest zazwyczaj strata finansowa (United Nations 2005). Jest to także każde przestępstwo polegające na oszustwie lub nieuczciwości; niewłaściwe postępowanie lub niewłaściwe wykorzystanie informacji związanych z rynkiem finansowym lub zajmowanie się dochodami z przestępstwa. Akanni, et al. (2020), Jung, Lee (2017), Suzumura et al. (2019) stwierdzają, że przestępstwa finansowe to szeroka i coraz powszechniejsza kategoria działalności przestępczej obejmująca niewłaściwe wykorzystanie, sprzeniewierzenie lub wprowadzenie w błąd jednostek lub podmiotów. Według Birdi (2021) przestępstwa te zazwyczaj polegają na oszukiwaniu kogoś w zwodniczy sposób w celu uzyskania osobistych korzyści finansowych bez przemocy i powodujące stratę finansową.

W kontekście przytoczonych definicji, a także w świetle traktowania infrastruktury banku jako środka przestępstwa albo banku jako ofiary przestępstwa, do katalogu przestępstw finansowych należy zaliczyć: pranie pieniędzy (Houben, Snyers 2018; Xu, Bao 2023; Wright 2017; Patora 2024), finansowanie terroryzmu (Houben, Snyers 2018; Birdi 2021; Ryder 2015), korupcję (Amjad et al. 2022; Xu, Bao 2023; Birdi 2021), oszustwo kredytowe (Płókarz et al. 2020; FATF 2023; Bahnsen et al. 2016) oraz cyberprzestępczość (Xu, Bao 2023; Trozze et al. 2022; FATF 2023).

Każde przestępstwo jest zagrożone karą na podstawie odpowiedniego przepisu prawa. Przykładowo, w polskim prawie przestępstwo prania pieniędzy zostało usankcjonowane w art. 299 kodeksu karnego (k.k.). Blisko związane z praniem pieniędzy jest przestępstwo finansowania terroryzmu, za które ustawodawca przewidział karę w art. 165a k.k. Korupcja w sektorze prywatnym została ujęta w art. 296a k.k. Z kolei sankcja za oszustwo kredytowe jest zawarta w art. 297. Cyberprzestępczość ujęta jest, m.in. w: art. 190a § 2, art. 267, art. 268a, art. 269 § 1 i 2, art. 269a, art. 269b, art. 286 kodeksu karnego, z zwłaszcza w art. 287 k.k., który w sposób ogólny traktuje o oszustwie komputerowym (Kodeks karny 1997).

1.2. Definicja odporności

W tej części artykułu przeanalizowano definicję odporności organizacji. W ostatnich latach definicja odporności ewoluowała m.in. na skutek przyjmowania przez autorów różnych perspektyw, co doprowadziło w rezultacie do opracowania wielu definicji i typologii, mających na uwadze różne perspektywy (Gundel 2005). Pomimo odmiennego kontekstu, większość definicji podkreśla negatywne skutki, jakie niosą za sobą różnego rodzaju zagrożenia dla organizacji oraz osób fizycznych. Podkreśla się, że bardzo istotna z perspektywy przeciwdziałania tym zagrożeniom jest zdolność systemu do reagowania na nie. Odporność definiuje się jako zdolność organizacji do absorbowania i adaptacji w zmieniającym się otoczeniu (ISO 2017). Inna definicja mówi o zdolności do przewidywania, unikania i dostosowywania się do zakłóceń i zmian płynących z zagrożeń. Pojęcie odporności odnosi się do zdolności organizacji do sprawnego przywrócenia działania po wystąpieniu negatywnego zdarzenia oraz rozwinięcia niezbędnych cech do podejmowania reakcji (Rajesh 2017). Kisiała i Suszyńska definiują odporność na kryzysy jako długoterminową zdolność przedsiębiorstwa do rozwoju, przy jednoczesnym utrzymaniu dobrej kondycji biznesu, pomimo recesji gospodarczej (Kisiała, Suszyńska 2018).

Dbanie o odporność organizacji jest kluczowe w rozwijaniu efektywnego i solidnego systemu. Rozwiązania pomagające kształtować odporność polegają m.in. na poprawie świadomości sytuacyjnej, zmniejszeniu podatności organizacji na ryzyko systemowe oraz przywróceniu skuteczności działania organizacji po zaistnieniu takiego zdarzenia. Dlatego też, odporność, poza radzeniem sobie z zagrożeniami, rozciąga się na skuteczne dostosowanie funkcjonowania organizacji zarówno do przewidywalnych, jak i nieprzewidywalnych warunków bliższego i dalszego otoczenia, a także może poprawić efektywność organizacji (Burnard 2018; Bhamra et al. 2011). W tabeli 1 przedstawiono wybrane definicje odporności ze względu na kontekst jej wystąpienia.

W celu zbudowania odporności na zagrożenia organizacje muszą być świadome tych zagrożeń oraz ich skutków. Ryzyko wystąpienia niepożądanego zdarzenia występuje w każdej organizacji. A to wymaga analiz i symulacji lub prognozowania oraz projektowania procedur zarządzania zdarzeniami kryzysowymi czy awariami. (Crichton 2009).

Tabela 1. Definicje pojęcia odporności w różnych kontekstach systemowych

Kontekst merytoryczny	Definicja
Systemowy	Zdolność systemu do absorpcji zakłóceń oraz reorganizacji w trakcie zmiany przy zachowaniu tej samej funkcji, tożsamości i struktury.
Socjoekologiczny	Zdolność systemu do utrzymania funkcjonalności, w przypadku zakłóceń lub do reorganizacji, jeśli bodźce otoczenia modyfikują strukturę funkcji systemu lub zdolność składowych systemu do jego odnowienia.
Psychologiczny	Zdolność adaptacji systemu do przezwyciężenia napotykanych „przeciwności losu".
Zarządzanie krytyczne	Zdolność jednostek do łagodzenia skutków zaistniałych zagrożeń, powstrzymywania skutków negatywnych zdarzeń w momencie ich wystąpienia oraz prowadzenia działań naprawczych, które minimalizują zakłócenia społeczne i łagodzą skutki przyszłych zagrożeń.
Organizacyjny	Odporność jest podstawową cechą umożliwiającą efektywne reagowanie na znaczące zmiany, które zakłócają oczekiwany wzorzec zdarzeń bez wprowadzania zbyt długiego okresu regresywnego zachowania.
Technologiczny	Zdolność do przewidywania, rozpoznawania, adaptacji i wchłaniania wariacji, zmian, zakłóceń oraz niespodziewanych zdarzeń w infrastrukturze technicznej.

Źródło: opracowanie własne na podstawie Bhamra, Dani, Burnard 2011.

2. Przegląd literatury

Do pozyskania literatury do przeglądu piśmiennictwa wykorzystano bazy Scopus i Web of Science, a następnie dokonano selekcji zgromadzonego zbioru według następujących kryteriów. Pierwszym był język publikacji. Z uwagi na brak lub niewiele publikacji w języku polskim, przyjęto język angielski jako kryterium włączenia. To z kolei wymusiło użycie różnych kombinacji słów/fraz kluczy. Zbyt ogólne dawały bardzo wiele wyników wyszukiwania (np. *fraud resilience* czy *fraud resistance*). Natomiast przyjęcie ostrej frazy skutkowało brakiem lub nielicznymi znalezionymi publikacjami (np. *crime resilience in banking sector*). Ostatecznie przyjęto dwie frazy, które miały racjonalne podstawy merytoryczne: *financial fraud resilience* oraz *financial crime resilience*.

Mając na uwadze stosunkowo szybko rozwijające się zjawisko przestępczości finansowej, do analizy włączono jedynie publikacje z lat 2010–2023[1]. W tabeli 2 zaprezentowano dyscypliny i specjalności, które zostały włączone i wyłączone z przeglądu literatury.

Tabela 2. Dyscypliny i specjalności zidentyfikowane w przeglądzie literatury

Dziedziny/ kategorie wyłączone	Chemia, Zdrowie, Materiałoznawstwo, BHP, Biochemia, Pielęgniarstwo, Fizyka i Astronomia, Studia rodzinne, Psychologia, Nauki o środowisku, Nauki decyzyjne, Nauki o Ziemi i Planetach, Geografia, Nauki o energii, Medycyna, Nauki o sztuce i Humanistyczne, Meteorologia, Urbanistyka, Sport, Historia, Studia kulturowe, Antropologia, Prace społeczne, Psychiatria, Polityka, Nauki etniczne, Gerontologia
Dziedziny/ kategorie włączone	Nauki komputerowe, Inżynieria, Prawo, Nauki społeczne, Kryminologia, Publikacje multidyscyplinarne, Ekonomia, Zarządzanie i Rachunkowość, Ekonometria i Finanse, Stosunki Międzynarodowe, Biznes, Finanse Biznesu

Źródło: opracowanie własne.

Dodatkowe kryteria selekcji pozycji z utworzonego zbioru to wersja publikacji w formacie pdf. W ten sposób otrzymano zbiór liczący 30 pozycji, który poddano wstępnej analizie według treści abstraktów, a następnie słowa kluczowe: *model, bank* i *index*, co miało pozwolić na zidentyfikowanie publikacji poruszającej problem kryteriów, modelu czy sposobu oceny odporności banku. Podsumowując, znaleziono 138 pozycji, z czego, po usunięciu duplikatów, do dalszego przeglądu zakwalifikowano 53. Jedynie 30 z nich było dostępnych w formacie pdf, a zaledwie 4 poruszały kwestię modeli odporności lub zapobiegania przestępstwom finansowym. Tabela 3 zawiera podsumowanie wyników wyszukiwania w podziale na poszczególne bazy danych, oryginalną liczbę wyników wyszukiwania oraz ostateczną liczbę publikacji zakwalifikowanych do finalnej analizy.

Cztery publikacje, które przeszły pozytywnie cały proces selekcji, poddano krytycznej analizie, a jej syntetyczne wyniki zamieszczono poniżej. Traktowały one, choć w minimalnym stopniu, o modelu odporności lub poruszały problem tworzenia modeli przeciwdziałania przestępstwom finansowym[2]. Pierwsza z publikacji porusza problem rozpoznawania nowych łańcuchów wartości w złośliwym oprogramowaniu dedykowanym do użycia przeciwko instytucjom finansowym. Celem

[1] Do przeglądu zaliczono publikacje akademickie, tj. artykuły, materiały konferencyjne i raporty, a także następujące rodzaje literatury szarej (określanej jako materiały niekontrolowane przez wydawców komercyjnych (Mazur, Orłowska 2018)): raporty, publikacje wydane przez jednostki inne niż uniwersyteckie.

[2] Takie podejście charakteryzuje się pewnymi wadami. Problematyka mogła być analizowana zarówno we wcześniejszym okresie, jak i później. Co więcej, nie wszystkie pozycje były uwzględnione w bazach, a wybrane słowa klucze oraz systemowy opis słowny mógł stanowić istotne ograniczenie.

autorów był przegląd literatury oraz praktyki na styku biznesu i bankowości. Zbadali oni przestępczy model prowadzenia biznesu oraz wątek *outsourcingu* pewnych czynności przez zorganizowane grupy przestępcze. Ponadto autorzy opisali model *crimeware-as-a-service*, który zakłada zakup oraz wykorzystanie wielu form nielegalnych usług wpisujących się w zakres cyberprzestępczości na nielegalnych rynkach. Pomimo, że badanie nie dotyczy bezpośrednio zagadnienia odporności, to koncentruje się na bankach, jako ofiarach takiego procederu (Van Wegberg 2017).

Tabela 3. Podsumowanie ilościowe przeglądu literatury

Fraza	Baza danych	Liczba wyników wyszukiwania	Liczba wyników wyszukiwania po wyłączeniu zbędnych dziedzin/kategorii i eliminacji duplikatów	Liczba publikacji dostępnych w formacie pdf	Liczba publikacji poruszających temat modelu odporności/ zapobiegania przestępstwom finansowym
Financial fraud resilience	Scopus	15	9	4	1
Financial crime resilience	Scopus	49	19	5	0
	Suma $_{Scopus}$	**64**	**28**	**9**	**1**
Financial fraud resilience	Web of Science	16	6	3	1
Financial crime resilience	Web of Science	58	19	18	2
	Suma $_{WoS}$	**74**	**25**	**21**	**3**
	Suma	**138**	**53**	**30**	**4**

Źródło: opracowanie własne.

Druga wyselekcjonowana publikacja dotyczy wskaźnika oceny skutków finansowych przestępczości w Stanach Zjednoczonych. Autorzy na podstawie tego wskaźnika opracowali portfel zabezpieczenia od przestępstw w USA, który wykorzystuje straty finansowe wykryte i zaraportowane przez FBI. Indeks ma na celu zabezpieczenie inwestycji, emitując europejskie opcje kupna i sprzedaży wybranych instrumentów finansowych, a także zapewniając budżety ryzyka. Zastosowane podej-

ście ma pomóc inwestorom ocenić ekspozycję na ryzyko rynkowe, ocenić ryzyko inwestycyjne oraz przyjąć strategie zabezpieczające przed potencjalnymi stratami. Portfel dotyczący przestępstw został opracowany dla Stanów Zjednoczonych, ale istnieje możliwość jego modyfikacji w celu szacowania ryzyka w innych regionach lub krajach, przy użyciu zestawu danych o przestępstwach porównywalnego do posiadanego przez FBI. Choć publikacja ta nie dotyczy bezpośrednio analizowanego w tym artykule problemu, to ilustruje ciekawe podejście do modelowania instrumentów finansowych opartych na danych o przestępczości (Mahanama, Shrivani, Rachev 2021).

W kolejnej publikacji poruszono problem modelu odporności organizacji z perspektywy reagowania na cyberataki. Model służy do wyjaśniania podejścia i dynamiki procesu, za pomocą których organizacje wykorzystują wiedzę oraz swoje zasoby do zwalczania skutków cyberataków w codziennej działalności biznesowej. Na podstawie niedawnych przypadków cyberataków na organizacje zidentyfikowano zestaw strategicznych i taktycznych reakcji ofiar takich ataków, które mogą zostać wykorzystane do przywrócenia stanu organizacji sprzed ataku. Model odporności organizacji na cyberataki składa się z 3 etapów. W pierwszym etapie model skupia się na monitorowaniu, analizowaniu i identyfikacji zagrożeń. Drugi etap polega na taktycznych reakcjach organizacji w momencie wystąpienia ataku. Natomiast ostatni etap polega na długoterminowym budowaniu odporności organizacji (Appiah, Amankwah-Amoah, Liu 2020).

Następna wybrana publikacja poświęcona jest identyfikacji czynników ryzyka oraz czynników ochronnych dla osób, które padły ofiarą tzw. oszustw romantycznych (*romance scam*). Różni się ona od pozostałych trzech skupiając się na osobach fizycznych, a nie organizacjach. Pomimo tej różnicy została ona zakwalifikowana do tego etapu badania na podstawie wcześniej opisanego postępowania. Autorzy proponują model podatności i odporności ofiar. Wykorzystali do tego dane opracowane na podstawie osobistych relacji ofiar. W efekcie zidentyfikowano *social media* oraz portale randkowe, poprzez które oszuści znaleźli swoje ofiary. Analiza pozwoliła także na opisanie technik stosowanych przez oszustów (Wang, Topalli 2022). Pomimo że pozycja ta wykracza poza główny nurt analizy w tym artykule dotyczący przestępstw przeciw organizacji, to warto o niej wspomnieć, ze względu na oryginalność, a także bliskie związki z obowiązkami osób działających w imieniu i na rzecz organizacji.

Jak zasugerowano, żadna z wybranych publikacji nie porusza problemu oceny odporności banków na przestępstwa finansowe w stopniu odpowiadającym zamierzeniom autora tego artykułu, co można określić jako zidentyfikowanie luki poznawczej w zakresie rozwiązań pozwalających ocenić odporność banku na zjawisko przestępczości finansowej. Nie oznacza to jednak, że przeprowadzone analizy krytyczne nie będą przydatne w dalszych pracach nad podjętą tematyką.

3. Metodologia

3.1. Opracowanie zestawu kryteriów oceny odporności banków na przestępstwa finansowe

W procesie doboru kryteriów oceny posłużono się sprawozdaniami niefinansowymi banków notowanych na Giełdzie Papierów Wartościowych w Warszawie, ze szczególnym uwzględnieniem tych, które odnosiły się do przeciwdziałania i wykrywania prania pieniędzy, finansowania terroryzmu, korupcji, oszustw kredytowych i cyberprzestępczości. Dodatkowo przeanalizowano raporty CSR, ESG, kodeksy etyki, dostępne polityki wewnętrzne i inne dokumenty odnoszące się do przestępstw finansowych.

Analizie poddano 10 banków notowanych na GPW w Warszawie, a były to: Powszechna Kasa Oszczędności Bank Polski S.A. (PKO BP), Bank Polski Kasa Opieki S.A. (PEKAO), Santander Bank Polska S.A., ING Bank Śląski S.A., mBank S.A., Alior Bank S.A., Bank Millennium S.A., Bank Handlowy w Warszawie S.A., BNP Paribas Bank Polska S.A., i Bank Ochrony Środowiska S.A[3].

Przeanalizowano raporty i sprawozdania niefinansowe za lata 2021 i 2022. Tam, gdzie banki odnosiły się do innych dokumentów, rozszerzano zakres analizy również na nie, jeśli ich treść była dostępna. Przedmiotem zasadniczego zainteresowania były przedsięwzięcia zmierzające do zapobiegania każdemu z pięciu rodzajów przestępstw finansowych, przy czym zakres informacji udostępnianych przez banki różnił się szczegółowością. Zebrane informacje pozwoliły opracować wstępną listę kryteriów, które są istotne z punktu widzenia odporności na pranie pieniędzy, finansowanie terroryzmu, korupcji, cyberprzestępczości i oszustw kredytowych. W opracowaniu typologii kryteriów uczestniczyli akademicy interesujący się problematyką bankowości. Do każdego z analizowanych przestępstw przypisano od 6 do 8 kryteriów, zawierających po 3 subkryteria precyzujące obszary, na których powinno się skoncentrować analizy w procesie ewaluacji odporności banku. Zestaw roboczy kryteriów składał się z 5 typów przestępstw, 36 kryteriów oraz 108 subkryteriów (por. tabela 4). Taki roboczy zestaw kryteriów był wykorzystany w badaniach ankietowych.

Tabela 4. Zestaw kryteriów oceny odporności banków na przestępstwa finansowe

PRANIE PIENIĘDZY
1. Proces Know Your Customer (KYC)
1.1. Wstępna weryfikacja klientów.
1.2. Bieżąca weryfikacja klientów w trakcie trwania relacji.
1.3. Stosowane sankcje.

[3] Z różnych powodów wyeliminowano pozostałe trzy banki notowane na GPW w Warszawie.

Tabela 4. (cd.)

2. Procedury wewnętrzne banku
2.1. Programy dedykowane przeciwdziałaniu praniu brudnych pieniędzy.
2.2. Jednostki lub komórki powołane w celu zwiększenia efektywności przeciwdziałania.
2.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do problemu prania pieniędzy.
3. Whistleblowing
3.1. Czy są specjalne kanały komunikacji umożliwiające anonimowe zgłaszanie podejrzanych transakcji lub aktywności?
3.2. Czy wdrożono dedykowane polityki/procedury gwarantujące anonimowość?
3.3. Liczba przypadków zgłoszeń naruszeń.
4. Zarządzanie ryzykiem
4.1. Zarządzanie ryzykiem braku zgodności, operacyjnym i fraudów.
4.2. Informacje o audytach wewnętrznych prowadzonych w zakresie *compliance* dotyczącym prania pieniędzy.
4.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do zarządzania ryzykiem.
5. Szkolenia wewnętrzne
5.1. % przeszkolonych pracowników.
5.2. Liczba godzin szkoleń na pracownika w roku.
5.3. Dodatkowe szkolenia dla pracowników szczególnie narażonych na ryzyko prania pieniędzy.
6. Dodatkowe dokumenty
6.1. Ile dodatkowych dokumentów/polityk dotyczących prania pieniędzy bank opracował?
6.2. Stopień szczegółowości dokumentów.
6.3. Stopień zaangażowania banku w adresowanie problemu prania pieniędzy w publikowanych materiałach.
7. Wykrywanie
7.1. Liczba zgłoszonych przypadków prania pieniędzy w poprzednim roku.
7.2. Liczba potwierdzonych przypadków (np. zapadł wyrok sądu) w poprzednim roku.
7.3. Kary finansowe nałożone na bank (np. UOKiK lub KNF za brak spełnienia wymogów w zakresie compliance).
8. Budowanie świadomości klientów
8.1. Kampanie informacyjne.
8.2. Bieżąca komunikacja na temat najnowszych zagrożeń płynących z działalności przestępców mającej na celu, np. pozyskanie ‘słupów’.
8.3. Merytoryczna zawartość stron internetowych.

Tabela 4. (cd.)

FINANSOWANIE TERRORYZMU
1. Proces Know Your Customer (KYC)
1.1. Wstępna weryfikacja klientów.
1.2. Bieżąca weryfikacja klientów w trakcie trwania relacji.
1.3. Stosowane sankcje.
2. Procedury wewnętrzne
2.1. Programy dedykowane przeciwdziałaniu finansowaniu terroryzmu.
2.2. Wewnętrzne jednostki powołane w celu zwiększenia efektywności przeciwdziałania.
2.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do problemu finansowania terroryzmu.
3. Whistleblowing
3.1. Czy są specjalne kanały komunikacji umożliwiające anonimowe zgłaszanie podejrzanych transakcji lub aktywności?
3.2. Czy wdrożono dedykowane polityki/procedury gwarantujące anonimowość?
3.3. Liczba przypadków zgłoszeń naruszeń.
4. Zarządzanie ryzykiem
4.1. Zarządzanie ryzykiem braku zgodności, operacyjnym i fraudów.
4.2. Informacje o audytach wewnętrznych prowadzonych w zakresie *compliance* dotyczącym finansowania terroryzmu.
4.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do tego problemu.
5. Szkolenia wewnętrzne
5.1. % przeszkolonych pracowników.
5.2. Liczba godzin szkoleń na pracownika w roku.
5.3. Dodatkowe szkolenia dla pracowników szczególnie narażonych na ryzyko finansowania terroryzmu.
6. Dodatkowe dokumenty
6.1. Ile dodatkowych dokumentów/polityk bank opracował w temacie finansowania terroryzmu?
6.2. Stopień szczegółowości dokumentów.
6.3. Ogólny stopień zaangażowania banku w adresowanie problemu finansowania terroryzmu w publikowanych materiałach.
7. Wykrywanie
7.1. Liczba zgłoszonych przypadków finansowania terroryzmu w poprzednim roku.
7.2. Liczba potwierdzonych przypadków (np. zapadł wyrok sądu).
7.3. Kary finansowe nałożone na bank (np. UOKiK lub KNF) za brak spełnienia wymogów w zakresie *compliance*.

Tabela 4. (cd.)

8. Budowanie świadomości klientów
8.1. Kampanie informacyjne.
8.2. Bieżąca komunikacja na temat najnowszych zagrożeń płynących z działalności przestępców mającej na celu np. pozyskanie ‘słupów’.
8.3. Merytoryczna zawartość stron internetowych.
KORUPCJA
1. Procedury wewnętrzne
1.1. Programy dedykowane przeciwdziałaniu korupcji.
1.2. Wewnętrzne jednostki powołane w celu zwiększenia efektywności przeciwdziałania.
1.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do problemu korupcji.
2. Whistleblowing
2.1. Czy są specjalne kanały komunikacji umożliwiające anonimowe zgłaszanie podejrzanych transakcji lub aktywności?
2.2. Czy wdrożono dedykowane polityki/procedury gwarantujące anonimowość?
2.3. Liczba przypadków zgłoszeń naruszeń.
3. Zarządzanie ryzykiem
3.1. Zarządzanie ryzykiem braku zgodności, operacyjnym i fraudów.
3.2. Informacje o audytach wewnętrznych prowadzonych w zakresie *compliance* dotyczącym korupcji.
3.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do tego problemu.
4. Szkolenia wewnętrzne
4.1. % przeszkolonych pracowników.
4.2. Liczba godzin szkoleń na pracownika w roku.
4.3. Dodatkowe szkolenia dla pracowników szczególnie narażonych na ryzyko korupcji.
5. Dodatkowe dokumenty
5.1. Ile dodatkowych dokumentów/polityk bank opracował w temacie korupcji?
5.2. Stopień szczegółowości dokumentów.
5.3. Ogólny stopień zaangażowania banku w adresowanie problemu korupcji w publikowanych materiałach.
6. Wykrywanie
6.1. Liczba zgłoszonych przypadków korupcji w poprzednim roku.
6.2. Liczba potwierdzonych przypadków (np. zapadł wyrok sądu).
6.3. Kary finansowe nałożone na bank (np. UOKiK lub KNF) za brak spełnienia wymogów w zakresie *compliance*.

Tabela 4. (cd.)

7. Budowanie świadomości klientów
7.1. Kampanie informacyjne.
7.2. Bieżąca komunikacja na temat najnowszych zagrożeń płynących z działalności przestępców mającej na celu, np. dotarcie do osób decyzyjnych i uwikłanie ich w działalność korupcyjną.
7.3. Merytoryczna zawartość stron internetowych.
CYBERPRZESTĘPCZOŚĆ
1. Standardy zarządzania
1.1. Wdrożone standardy zarządzania cyberbezpieczeństwem i cyberryzykiem.
1.2. Bieżąca aktualizacja polityk i procedur.
1.3. Opracowane zasady reagowania na incydenty.
2. Ciągły monitoring
2.1 Wdrożone systemy monitoringu i wykrywania anomalii.
2.2. Testy penetracyjne.
2.3. Audyty zewnętrzne.
3. Kontrola dostępu
3.1. Silne uwierzytelnienie klienta.
3.2. Wewnętrzne systemy zarządzania dostępem.
3.3. Zarządzanie dostawcami technologii i usług.
4. *Compliance* i raportowanie
4.1. Zgodność z przepisami prawa i regulacjami.
4.2. Raportowanie wewnętrzne.
4.3. Transparentność zewnętrzna.
5. Szkolenia wewnętrzne
5.1. % przeszkolonych pracowników.
5.2. Liczba godzin szkoleń na pracownika w roku.
5.3. Dodatkowe szkolenia dla pracowników szczególnie narażonych na ryzyko cyberprzestępczości.
6. Budowanie świadomości klientów
6.1. Kampanie informacyjne.
6.2. Bieżąca komunikacja na temat najnowszych zagrożeń płynących z działalności przestępców w nowych kanałach dostępu.
6.3. Merytoryczna zawartość stron internetowych.

Tabela 4. (cd.)

OSZUSTWA KREDYTOWE
1. Procedury wewnętrzne
1.1. Wdrożone silne procedury związane z procesem kredytowym.
1.2. Wewnętrzne jednostki powołane w celu zwiększenia efektywności przeciwdziałania.
1.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do tego problemu.
2. Whistleblowing
2.1. Czy są specjalne kanały komunikacji umożliwiające anonimowe zgłaszanie podejrzanych transakcji lub aktywności.
2.2. Czy wdrożono dedykowane polityki/procedury gwarantujące anonimowość.
2.3. Liczba przypadków zgłoszeń naruszeń.
3. Zarządzanie ryzykiem
3.1. Zarządzanie ryzykiem braku zgodności, operacyjnym i fraudów.
3.2. Informacje o audytach wewnętrznych prowadzonych w zakresie *compliance* dotyczącym oszustw kredytowych.
3.3. Stosowanie się do rekomendacji sektorowych (np. KNF) odnoszących się do tego problemu.
4. Szkolenia wewnętrzne
4.1. % przeszkolonych pracowników.
4.2. Liczba godzin szkoleń na pracownika w roku.
4.3. Dodatkowe szkolenia dla pracowników szczególnie narażonych na ryzyko oszustw kredytowych.
5. Dodatkowe dokumenty
5.1. Ile dodatkowych dokumentów/polityk bank opracował w temacie oszustw kredytowych?
5.2. Stopień szczegółowości dokumentów.
5.3. Ogólny stopień zaangażowania banku w adresowanie problemu oszustw kredytowych w publikowanych materiałach.
6. Wykrywanie
6.1. Liczba zgłoszonych przypadków oszustw kredytowych w poprzednim roku.
6.2. Liczba potwierdzonych przypadków (np. zapadł wyrok sądu).
6.3. Kary finansowe nałożone na bank (np. UOKiK lub KNF) za brak spełnienia wymogów w zakresie *compliance*.
7. Budowanie świadomości klientów
7.1. Kampanie informacyjne.
7.2. Bieżąca komunikacja na temat najnowszych zagrożeń płynących z działalności przestępców mającej na celu np. znalezienie ‘słupów’.
7.3. Merytoryczna zawartość stron internetowych.

Źródło: opracowanie własne.

3.2. Badanie ankietowe

W celu walidacji i uzupełnienia opracowanych kryteriów przeprowadzono badanie ankietowe wśród ekspertów z zakresu przeciwdziałania przestępstwom finansowym z banków działających na polskim rynku. Głównymi grupami respondentów byli eksperci pracujący m.in. w działach *Compliance*, AML (Anti-Money Laundering), KYC, *FinCrime* czy *Fraud Prevention*. Zadaniem ekspertów było porównanie parami wszystkich kryteriów wykorzystując dziewięciostopniową fundamentalną skalę porównań Saaty'ego w ramach metody AHP. Ponadto zostali oni poproszeni o dopisanie subkryteriów w obszarach, w których uznają to za potrzebne.

Badanie ankietowe było skierowane do reprezentantów 10 wspomnianych banków. Swoje formularze zwrócili przedstawiciele 9 z nich i w takiej liczbie odpowiedzi zostały poddane dalszemu badaniu. Oceny udzielone przez respondentów w ramach porównań parami zostały naniesione na macierze porównań zgodnie z metodą AHP. Badanie było obszerne. Respondenci dokonali porównań parami 36 kryteriów, których zakres został doprecyzowany przez 108 subkryteriów. Liczba porównań w jednym arkuszu ankietowym wynosiła 113, co w sumie dało 1017 porównań w ramach całego badania.

3.3. Badanie metodą Analytic Hierarchy Process (AHP)

Pomiar miał charakter względny z uwagi na porównywanie wspólnych części analizowanych kryteriów. W tym przypadku jest to zestaw kryteriów i subkryteriów (Prusak, Stefanów 2014). Każdy respondent porównywał parami poszczególne kryteria wykorzystując skalę od 1 do 9. Z uwagi na kompleksowość problemu oraz dostęp do ograniczonych danych, zdecydowano się na skonstruowanie kryteriów w obecnym kształcie. Mając wgląd w szczegółowe dane, nieudostępniane powszechnie przez banki, zestaw kryteriów mógłby być bardziej szczegółowy. To z kolei mogłoby pomóc w jeszcze bardziej wiarygodnej ocenie odporności banku. Oceny udzielone przez respondentów w drodze porównań parami zostały naniesione na macierze porównań AHP.

W następnym kroku przeprowadzono normalizację wartości macierzy i nadano wagi poszczególnym kryteriom w ramach zestawu dla każdego rodzaju przestępstwa. Do wyznaczenia wag kryteriów oceny odporności użyto procedury średniej arytmetycznej. Uśrednione wagi zostały zaprezentowane w tabeli 5.

Następnie przeprowadzono kontrolę poprawności porównań, która wykazała, że większość porównań przyjmuje wartości współczynnika zgodności CR powyżej 0,1, co może wskazywać na brak logiczności wyników (Prusak, Stefanów 2014). W takiej sytuacji można podjąć m.in. następujące działania:

- zrezygnować z badań – w tym przypadku byłoby to niemożliwe;
- poprosić ekspertów o ponowne wykonanie porównań – z uwagi na kompleksowość pierwotnego badania oraz fakt, że było finansowane z grantu, ponowne

wykonanie porównań zajęłoby dużo czasu i byłoby bardzo kosztowne. Jednocześnie nie byłoby gwarancji, że nowe wyniki osiągnęłyby wymóg CR<0,1;
- zmodyfikować pierwotne oceny i ponownie oszacować wartości współczynników wagowych oraz współczynnika zgodności – wymagałoby to spotkania z ekspertami i przeanalizowania udzielonych ocen i następnie kolektywne ich dostosowanie. Mając na uwadze poprzedni punkt oraz fakt, że badanie było anonimowe, to wyjście nie byłoby możliwe. Przydatnym narzędziem w tym celu byłaby analiza wrażliwości dokonanych wcześniej porównań. Przestrzega się jednak przed nadużywaniem takiego podejścia, ponieważ metoda AHP jest narzędziem, a nie celem samym w sobie;
- zmodyfikować model – po ponownym przeanalizowaniu modelu hierarchicznego uznano, że jego modyfikacja mijałaby się z celem prowadzonych badań. Model (zestaw kryteriów) musi zawierać wszystkie wymienione w nim dotychczas elementy, aby możliwie kompleksowo pokrywał aspekty odporności na przestępstwa finansowe;
- przyjąć wyniki ze świadomością, że rezultaty badań są obarczone błędami.

Mając na uwadze powyższe, zdecydowano o przyjęciu wyników ze świadomością, że rezultaty badań są obarczone błędami, a podejmowane na ich podstawie decyzje będą charakteryzowały się zwiększonym ryzykiem. W drugim etapie współpracy z respondentami poproszono o dodanie subkryteriów w poszczególnych kryteriach, jeśli uznają to za celowe. Okazało się jednak, że komentarze ani nie rozszerzyły, ani nie zmodyfikowały opracowanego zestawu kryteriów z pierwszej rundy. W związku z tym, zadecydowano o pozostawieniu zestawu kryteriów oceny odporności w niezmienionej formie. Tak stworzony zestaw kryteriów może stanowić podstawę do opracowania modelu oceny odporności banku na przestępstwa finansowe[4].

[4] Taki model oceny odporności banku jest głównym przedmiotem badań w rozprawie doktorskiej Autora.

Tabela 5. Kryteria i średnie wagi odporności dla pięciu rodzajów przestępstw finansowych

Kryteria i wagi [w %]									
Pranie pieniędzy	**Średnia waga (%)**	**Finansowanie terroryzmu**	**Średnia waga (%)**	**Korupcja**	**Średnia waga (%)**	**Cyber-przestępczość**	**Średnia waga (%)**	**Oszustwa kredytowe**	**Średnia waga (%)**
1. Proces KYC	19,01	1. Proces KYC	19,69	1. Procedury wewnętrzne	12,78	1. Standardy zarządzania	17,31	1. Procedury wewnętrzne	20,20
2. Procedury wewnętrzne	13,82	2. Procedury wewnętrzne	18,78	2. Whistleblo-wing	19,68	2. Ciągły monitoring	25,38	2. Whistleblo-wing	16,88
3. Whistleblo-wing	17,96	3. Whistleblo-wing	10,57	3. Zarządzanie ryzykiem	19,56	3. Kontrola dostępu	15,01	3. Zarządzanie ryzykiem	12,42
4. Zarządzanie ryzykiem	14,92	4. Zarządzanie ryzykiem	14,99	4. Szkolenia wewnętrzne	15,20	4. Zgodność i ra-portowanie	16,12	4. Szkolenia wewnętrzne	14,18
5. Szkolenia wewnętrzne	7,78	5. Szkolenia wewnętrzne	10,69	5. Dodatkowe dokumenty	10,19	5. Szkolenia wewnętrzne	15,50	5. Dodatkowe dokumenty	11,72
6. Dodatkowe dokumenty	6,69	6. Dodatkowe dokumenty	7,24	6. Wykrywanie	16,72	6. Budowanie świadomości klientów	10,68	6. Wykrywanie	15,31
7. Wykrywanie	14,20	7. Wykrywanie	15,01	7. Budowanie świadomości klientów	**5,86**			7. Budowanie świadomości klientów	9,29
8. Budowanie świadomości klientów	5,62	8. Budowanie świadomości klientów	**3,03**						

Źródło: opracowanie własne.

Podsumowanie

Przeprowadzone studia piśmiennictwa oraz badania własne pozwalają na sformułowanie kilku ocen i wniosków. Po pierwsze, brak jednoznacznej i ogólnie przyjętej definicji przestępstwa finansowego skutkuje kontrowersjami w jej identyfikacji, badaniu, typologii, a w konsekwencji prowadzi do kilku niepożądanych skutków. Przede wszystkim wywołuje kontrowersje w procesie rozpoznawania przejawów tego zjawiska, utrudnia lub uniemożliwia opracowanie. Po drugie, niejasności pojęciowo-zakresowe utrudniają opracowywanie odpowiedniego instrumentarium przeciwdziałania. Po trzecie, z perspektywy działalności bankowej wywołuje problemy zarządzania ryzykiem związanym z przestępczością finansową, zwłaszcza wobec wysokiej dynamiki rozwoju infrastruktury technicznej, technologii, a wręcz przestępczej innowacyjności. Wszystko to przemawia za zaawansowaniem prac nad uspójnieniem samego pojęcia przestępczości finansowej i przyjęciem jednoznacznej definicji.

Odporność na przestępstwa finansowe jest ważnym składnikiem ogólnie rozumianej odporności banków. Im bardziej odporny jest pojedynczy bank, tym bardziej odporny i stabilny sektor bankowy.

Przeprowadzona kwerenda literatury i źródeł wykazała brak zaawansowanych modeli oceny odporności banków na przestępstwa finansowe. Stanowiło to zasadniczą przesłankę dla opracowania autorskiego zestawu syntetycznych i szczegółowych kryteriów odporności banku. Zestaw ten opracowano na podstawie krytycznej analizy literatury i praktyki, a następnie poddano go ocenie ekspertów zatrudnionych w bankach. Przeprowadzony sondaż diagnostyczny pozwolił na zweryfikowanie adekwatności opracowanego zestawu kryteriów i jego użyteczności w praktyce. Wyniki sondażu uprawniają do ostrożnej acz pozytywnej oceny użyteczności modelu i wykorzystywania go w analizach i audycie odporności na przestępstwa finansowe nie tylko w instytucjach kredytowych.

Zaletą opracowanego modelu jest jego otwartość i elastyczność. W zależności od pozyskiwanych informacji i dostępu do baz danych model może być modyfikowany lub rozbudowywany. Jednocześnie w ocenie wiarygodności diagnozy odporności na przestępstwa finansowe trzeba mieć na względzie, że zaproponowany zestaw kryteriów i ich parametryzacja odpowiada w zasadzie zakresowi udostępnionych przez banki informacji oraz danych, w tym raportów ESG, CSR i innych materiałów symptomatycznie powiązanych z badaną tematyką.

Ramy artykułu nie pozwalają na zamieszczenie w nim *in extenso* wykorzystanych narzędzi badawczych, w tym zwłaszcza formularza ankietowego, który obejmuje *ca* 13 stron druku, który jest w dyspozycji autora.

Trudna do dokładnego oszacowania, ale niewątpliwie ogromna wartościowo i rosnąca skala przestępstw finansowych w ujęciu globalnym, a także podobna tendencja w Polsce stanowi silną przesłankę na rzecz rozwoju badań i doskonalenia instrumentarium przeciwdziałania im. Tym bardziej, że wysoce uprawdopodobniona jest teza głosząca, iż nakłady świata przestępczego na nielegalną działalność są większe i rosną szybciej niż te dedykowane ich zwalczaniu.

Bibliografia

ACFE, IIA, AICPA. (2007), *Managing the Business Risk of Fraud: A Practical Guide*, The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiners.

Akanni J.O., Akinpelu F.O., Olaniyi S., Oladipo A.T., & Ogunsola A.W. (2020), *Modelling financial crime population dynamics: optimal control and cost-effectiveness analysis*. „International Journal of Dynamics and Control", 8.

Amjad R.M., Rafay A., Arshed N., Munir M., & Amjad M.M. (2022), *Non-linear impact of globalization on financial crimes: a case of developing economies*, „Journal of Money Laundering Control", 25(2).

Appiah G., Amankwah-Amoah J., Liu Y.-L. (2020), Organizational Architecture, Resilience, and Cyberattacks, IEEE Transactions on Engineering, University of Kent.

Bahnsen A.C., Aouada D., Stojanovic A., & Ottersten B. (2016). *Feature engineering strategies for credit card fraud detection*, Expert Systems with Applications, 51.

Bhamra R., Dani S., Burnard K. (2011), *Resilience: the concept, a literature review and future directions*, „International Journal of Production Research", 49(18).

Birdi A. (2021), *Global Perspective of Financial Crimes*, Available at SSRN: https://ssrn.com/abstract=3917078.

Bojarski M. (red.). (2015), *Prawo karne materialne. Część ogólna i szczególna*, Warszawa: Wolters Kluwer.

Burnard E., et al. (2018), *Building organizational resilience: Four configurations,* IEEE Transactions on Engineering Management, 65(3).

Crichton M.T. (2009), *Enhancing organizational resilience through emergency planning: learnings from cross-sectoral lessons*, J. Contingencies and Crisis Management, 17(1).

Deloitte. (2019), *Financial Crime Compliance. It is no longer sufficient to 'go it alone'*, Deloitte Touche Tohmatsu India LLP.

Deloitte. (2022), *The effectiveness of financial crime risk management reform and next steps on a global basis*, The Institute of International Finance and Deloitte White Paper.

FATF. (2023), *Illicit Financial Flows from Cyber-Enabled Fraud*, Paryż: FATF.

Gundel S. (2005), *Towards a new typology of crises*, „Journal of Contingencies and Crisis Management", 13(3).

Houben R., Snyers A. (2018), *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament.

International Monetary Fund. (2001), *Financial System Abuse*, Financial Crime and Money Laundering – Background Paper, Washington DC: International Monetary Fund.

ISO. (2017), *International Standard. ISO 22316*, ISO copyright office, Geneva.

Jasiński W. (2014), *Nadużycia w przedsiębiorstwie*, Wydawnictwo Poltext, Warszawa.

Jung J., Lee J. (2017), *Contemporary Financial Crime*, „Journal of Public Administration and Governance", 7(2).

Kisiała W., Suszyńska K. (2018), *The resilience of regions to economic recession: the analysis of employment trends*. Acta Scientiarum Polonorum. Oeconomia, 17(3).

Mahanama, T., Shrivani, A., Rachev, S. T. (2021), *Global Index on Financial Losses Due to Crime in the United States*, „Journal of Risk and Financial Management", 14(7).

Mazur Z., Orłowska A. (2018), *Jak zaplanować i przeprowadzić systematyczny przegląd literatury*, Polskie Forum Psychologiczne, tom 23(2), Katolicki Uniwersytet Lubelski Jana Pawła II.

Morgan R.E. (2017), *Financial Fraud in the United States*, Washington DC: U.S. Department of Justice.

Patora K. (2024), *Relacje norm prawa Unii Europejskiej i prawa krajowego w zakresie ścigania przestępstw prania brudnych pieniędzy*. „Bezpieczny Bank", 94(1). https://doi.org/10.26354/bb.3.1.94.2024

Pilarczyk A. (2016), *Oszustwa pracowników banków w gospodarce opartej na wiedzy*, „Roczniki Ekonomii i Zarządzania", 44(2).

Płókarz R., Iwanowicz B., Iwanowicz T., Majewski P., Voss G., Wojtczak K. (2020), *Przestępczość finansowa. Bankowość. Ubezpieczenia. Przedsiębiorstwa. Tom I*, Warszawa: Difin.

Proczek M., Szczepańska P. (2017), *Nadużycia i oszustwa finansowe a działalność Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych*, „Studia Ekonomiczne", nr 319.

Prusak A., Stefanów P. (2014), *AHP – analityczny proces hierarchiczny. Budowa i analiza modeli decyzyjnych krok po kroku*, C.H. Beck.

Rajesh R. (2017), *Technological capabilities, and supply chain resilience of firms: A relational analysis using Total Interpretive Structural Modeling (TISM)*, Technological Forecasting & Social Change, 118.

Reurink A. (2019), *Financial fraud: A literature review*, Contemporary topics in finance: A collection of literature surveys.

Ryder N. (2015), *The financial war on terrorism: A review of counter-terrorist financing strategies since 2001*, Routledge.

Snyder H. (2019), *Literature review as a research methodology: An overview and guidelines*. „Journal of Business Research", Volume 104.

Suzumura T. et al. (2019), *Towards federated graph learning for collaborative financial crimes detection*, arXiv preprint arXiv:1909.12946.

Trozze A., Kamps J., Akartuna E.A., Hetzel F.J., Kleinberg B., Davies T., Johnson S.D. (2022), *Cryptocurrencies and future financial crime*, Crime Science 11, 1.

United Nations (2005), *Economic and financial crimes: challenges to sustainable development*, United Nations, The Eleventh United Nations Congress on Crime Prevention and Criminal Justice.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 Nr 88 poz. 553).

Wang F., Topalli V. (2022), *Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context*, „American Journal of Criminal Justice" (Ahead of print).

Wright E.G. (2017), *Follow the Money: Financial Crimes and Forfeiture in Human Trafficking Prosecutions*, US Att'ys Bull., 65, 79.

Xu R., Bao J. (2023), *Research on Financial Crimes Detection based on Big Data Technology*, Proceedings of the 2023 4th International Conference on Big Data and Social Sciences (ICBDSS 2023), Atlantis Highlights in Social Sciences, Education and Humanities 12.

Van Wegberg R.S. et al. (2017), *Discerning Novel Value Chains in Financial Malware. On the Economic Incentives and Criminal Business Models in Financial Malware Schemes*, „European Journal on Criminal Policy and Research", 23(4).