WYDZIAŁ
EKONOMII I FINANSÓW

Studia Ekonomiczne, Prawne i Administracyjne

Nr 4/2025

UNIWERSYTET
RADOMSKI

WYDZIAŁ
EKONOMII I FINANSÓW

Studia Ekonomiczne, Prawne i Administracyjne

Nr 4/2025

UNIWERSYTET
RADOMSKI

Studia Ekonomiczne, Prawne i Administracyjne Nr 4/2025
Patronat wydania: Polskie Towarzystwo Ekonomiczne Oddział w Radomiu,
WEiF URad., ul. Chrobrego 31, 26-600 Radom

ISSN 2450-3940

Wyd. I

Spis treści

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.017

Leszek Tarasiński[1]

PRZYCZYNY PODEJMOWANIA BEZPOŚREDNICH INWESTYCJI ZAGRANICZNYCH W ŚWIETLE WYBRANYCH TEORII JEDNOCZYNNIKOWYCH

Streszczenie

W artykule omówiono wybrane zagadnienia teoretyczne objaśniające zagadnienie przyczyn podejmowania bezpośrednich inwestycji zagranicznych. Praca stanowi kolejny – drugi – fragment czteroczęściowego cyklu poświęconego wybranym aspektom teoretycznym związanym z bezpośrednimi inwestycjami zagranicznymi.

Słowa kluczowe: globalizacja, bezpośrednie inwestycje zagraniczne.

Wstęp

Zaprezentowany w części pierwszej (czteroczęściowego cyklu artykułów) model OLI trzeba uznać za kompleksowo tłumaczący kwestię przyczyn podejmowania bezpośrednich inwestycji zagranicznych, widzianych w perspektywie historycznej. W istocie daje on odpowiedź na zasadnicze pytanie: dlaczego te inwestycje są podejmowane. Źródłem wiedzy na ten temat były wcześniej sformułowane hipotezy i modele, a J.H. Dunning twórczo zintegrował je ze sobą. Wszakże, wskazując na trzy podstawowe przesłanki (przewagi), których wystąpienie skutkuje BIZ (czyli stworzeniem produkcji międzynarodowej), nie wchodzi szczegółowo i szeroko w obszar rozważań dotyczących skutków z tego wynikających dla poszczególnych państw i gospodarki światowej, ale daje dostatecznie ważny pretekst do nich. W przypadku każdej z przewag da się zwrócić uwagę na coś więcej, niż tylko ich kapitalne znaczenie dla samej decyzji o potrzebie podjęcia BIZ. Zagłębiając się w ich istotę, można dostrzec, że jest też obecny ich globalny kontekst związany z rozprzestrzenianiem się w całości gospodarki światowej – np. poprzez innowacyjne produkty – nowoczesnych technologii i zarządzania, umiejętności marketingowych itp.

[1] Doktor nauk ekonomicznych, Wydział Ekonomii i Finansów, Uniwersytet Radomski im. Kazimierza Pułaskiego, leszek.tarasinski@urad.edu.pl.

W przypadku przewagi lokalizacji mamy niemal wprost odwołanie się do osiągnięć teorii handlu międzynarodowego. W podobny sposób uzasadniającej przesłanki i skutki wynikające z handlu światowego, jak czynią to potencjalni inwestorzy zagraniczni, rozważający lokalizacje swoich nowych zagranicznych przedsięwzięć gospodarczych. Zatem do stwierdzenia o pełnieniu przez paradygmat OLI roli koncepcji rzetelnie objaśniającej przyczyny podejmowania BIZ trzeba dodać, że zarazem model ten ma swój znaczny potencjał rozwojowy – zachęca bowiem do wejścia szerzej w problematykę skutków BIZ, rozumianych jako efekt wzmagania się coraz bardziej pod wpływem BIZ oddziaływań prorozwojowych, w rezultacie systematycznie zwiększania się międzynarodowej wymiany gospodarczej. T. Ozawa, autor bardzo oryginalnej i popularnej zarazem tzw. *teorii dynamicznych przewag komparatywnych*, niewątpliwie inspirowanej eklektyczną teorią J.H. Dunninga, tak to ujął: „Jedną z luk w światowej literaturze poświęconej międzynarodowemu biznesowi jest brak dynamicznego podejścia do jego roli w rozwoju ekonomicznym”[2].

Refleksje wyrażone powyżej podnoszą niewątpliwie walor modelu OLI jako prezentującego duży potencjał poznawczy ze względu na jego eklektyczny charakter, który sprawia, że teoria ta jest otwarta na nowo powstające koncepcje i może być systematycznie ulepszana[3]. Zarazem wyraźnie wskazują na potrzebę „rozszerzenia” perspektywy rozważań teoretycznych[4]. Nie należy jednak zapominać o konieczności omówienia koncepcji, które – stanowiąc integralną część dorobku teoretycznego ekonomii w zakresie zjawiska BIZ w całej perspektywie historycznej badań tychże – może nie tyle, że pełnią funkcję stricte teorii bazowych dla modelu OLI (te omówiono w pierwszej część niniejszego cyklu), ale są równie interesujące poznawczo, oraz bez trudu mogłyby mieć charakter komplementarny wobec teorii, na których Dunning w swojej eklektycznej teorii się oparł. Zważywszy na – z jednej strony – organizację myślenia o istocie BIZ, zaproponowaną przez model OLI (tzn. ujmującą BIZ kompleksowo w kształt trzech przewag), oraz – z drugiej strony – na fakt, że hipotezy cząstkowe – każda z nich, podnosi niewątpliwie jakiś ważny (choć zazwyczaj pojedynczy) aspekt produkcji międzynarodowej – bez trudu da się skojarzyć z którąś z przewag modelu OLI. Widać wyraźnie możliwość włączenia tych hipotez w paradygmat OLI. Z tego względu należy potraktować niektóre z cząstkowych teorii (omówionych w dalszej części artykułu) jako pozostające w domniemanym związku z paradygmatem OLI. Skądinąd w tym właśnie wyraża się nasz optymizm, zawarty w zaprezentowanej wcześniej opinii, że teoria Dunninga jest otwarta na nowo powstające koncepcje i może być systematycznie ulepszana.

---

[2] T. Ozawa, *Foreign direct investment and economic development*, Transnational Corporation, February 1992, vol. 1, No. 1, s. 27.

[3] A. Zorska, *Ku globalizacji? Przemiany w korporacjach transnarodowych i w gospodarce światowej*, Wydawnictwo Naukowe PWN, Warszawa 1998, s. 80.

[4] Wyrazem tego jest m.in. struktura niniejszego cyklu, zakładająca jego cztery części.

Chociaż do tej pory często używano określenia „hipotezy cząstkowe", z pewnych względów niebawem zastąpimy to określenie mianem *teorii jednoczynnikowych*. Wyjaśnienie tego Czytelnik znajdzie poniżej.

1. Przyczyny podejmowania BIZ w ujęciu teorii jednoczynnikowych – perspektywa historyczna

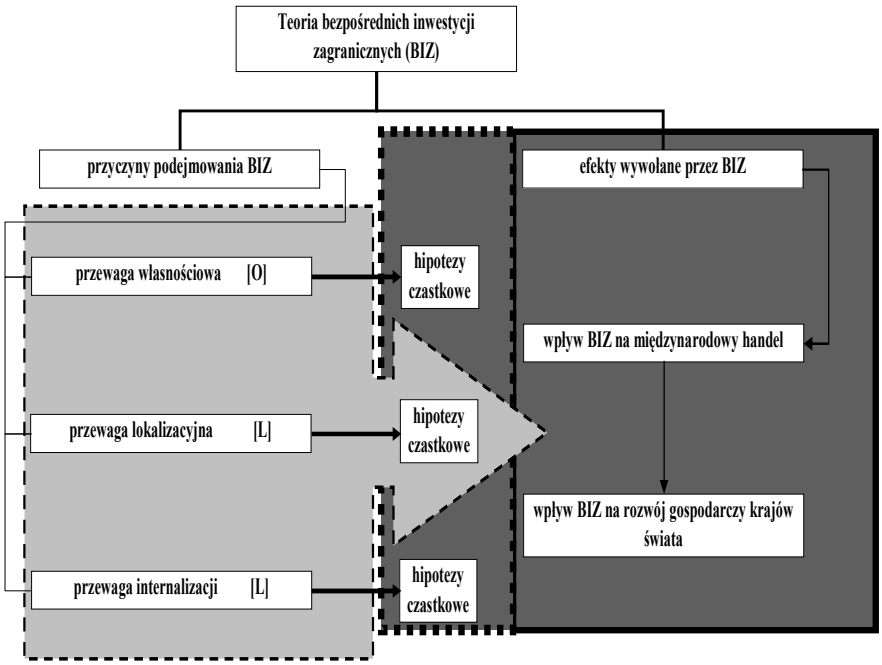
Zasadniczo treścią tego artykułu jest analiza, której przebieg polega na omówieniu najbardziej znanych cząstkowych hipotez dotyczących przyczyn podejmowania BIZ. Niektóre z tych hipotez akcentują mikro-, a inne makroekonomiczne aspekty produkcji międzynarodowej. Wg J. Misali można wyróżnić wiele sposobów podziału hipotez dotyczących BIZ, a wśród nich trzy zasadnicze typy teorii: a) dotyczące BIZ i inwestycji portfelowych, b) dotyczące zagranicznych inwestycji kapitałowych przedsiębranych w warunkach konkurencji doskonałej i jej braku, c) makroekonomiczne, mikroekonomiczne i mieszane. Autor ten swoją uwagę skupia wszakże na tej ostatniej kategorii teorii[5]. Skądinąd właśnie z tego powodu, że w eklektycznej teorii Dunninga liczne są zarówno mikro-, jak i makroekonomiczne akcenty, autor zalicza ją do grupy tzw. mieszanych teorii BIZ[6]. Obecne rozważanie będzie stanowiło swoiste „uzupełnienie" poprzedniej (zawartej w części pierwszej) prezentacji o kolejne koncepcje teoretyczne. Następnie – jak niebawem się okaże – z łatwością „wkomponujemy" je w treści poszczególnych przewag Dunninga. Udowodnimy w ten sposób duże zasługi tego autora jako badacza, który przekonująco integrując wybrane przez siebie koncepcje teoretyczne, stworzył model o dużym potencjale rozwojowym, tzn. w którym mają szanse zawrzeć się kolejne, na wskroś nowe wypowiedzi teoretyczne związane z BIZ.

Rozumiejąc i podzielając pogląd o sensowności wyjaśnienia przyczyn podejmowania BIZ, które w modelu OLI są zbiorem trzech przewag konkurencyjnych, potraktujemy go jako swoisty „konstrukt" – ramę, w której zawrzemy hipotezy cząstkowe (inaczej mówiąc, różne na przestrzeni czasu sformułowane teorie i modele BIZ). Ich słabością zazwyczaj było dość jednostronne patrzenie na BIZ. Zawarte w tytule niniejszego podrozdziału określenie „teorie jednoczynnikowe" wydaje się być w kontekście tych teorii o tyle adekwatne, o ile rzeczywiście koncepcje te zazwyczaj – jak niebawem się to okaże – koncentrowały się na jednym czynniku zmian. Powodowało to częstokroć albo szybką ich dezaktualizację, albo niemożność sprostania krytyce ze strony ujęć alternatywnych. Te ostatnie zresztą, podobnie jak te pierwsze, cechowała podobna słabość. W ten sposób mieliśmy do czynienia z dużym bogactwem teorii, z których żadna nie budziła pełnego zaufania.

Obecne rozważania teoretyczne będą zatem swoistą próbą dopełnienia do całości i w ten sposób – ostatecznie – stworzenia kompletnego obrazu hipotez teoretycznych

[5] J. Misala J., *Współczesne teorie wymiany międzynarodowej i zagranicznej polityki ekonomicznej*, SGH, Warszawa 2001, s. 214.
[6] Ibidem, s. 224.

BIZ, których związku z modelem Dunninga nie da się zaprzeczyć. Próbą, która zaowocuje w pełni poznaniem struktury modelu. Jednak – wziąwszy pod uwagę cytowaną już „lukę w światowej literaturze poświęconej międzynarodowemu biznesowi", „ramy" ulegną twórczemu poszerzeniu, w szczególności poprzez skierowanie zainteresowania na zagadnienie wpływu światowych BIZ na światowy handel i rozwój gospodarczy, w ten sposób dopełniając całości analizy przyczynowo – skutkowej o prezentację skutków BIZ [akurat ten wątek wypełni swą zawartością kolejne (3 i 4) części niniejszego cyklu, poświęconego teoriopoznawczym aspektom BIZ]. Schematycznie to zadanie badawcze można przedstawić, jak na rysunku poniżej.



Rys. 1. Teoria bezpośrednich inwestycji zagranicznych a model OLI
Źródło: Opracowanie własne

Jak pokazuje rys. nr 1, blok zagadnień teoretycznych ujętych przez Dunninga w formę paradygmatu OLI (symbolicznie zaznaczony jasnoszarym autokształtem strzałki blokowej z grotem skierowanym na prawo), z uwagi na fakt, iż zawartością swą dowodzi nader często faktycznie posługiwania się pojęciami, kategoriami i hipotezami o proweniencji makroekonomicznej (np. jak to ma miejsce w przypadku przewagi lokalizacyjnej, gdzie mowa jest o teoriach lokalizacji, będących stricte teoriami handlu międzynarodowego, czy modelu międzynarodowego cyklu życia

produktu. Model ten – chociaż przekonująco wskazuje na dostatecznie ważną przesłankę podjęcia bezpośredniej inwestycji zagranicznej, jaką jest przewaga amerykańskiej korporacji w dziedzinie innowacji i wprowadzania na rynek nowych i nowoczesnych produktów – jest przecież jedną z postaci tzw. neotechnologicznych teorii handlu międzynarodowego, które wyewoluowały z tradycyjnego modelu handlu międzynarodowego H-O-S[7]). Przywiązując do nich głównie wagę mikroekonomicznych przesłanek podejmowania BIZ, a nie rozwijając, czy też akcentując je jako stricte modele makroekonomiczne, w tym znaczeniu inspiruje do „wejścia" w obszar analizy makroekonomicznych efektów towarzyszących BIZ [stąd grot jasnoszarej strzałki blokowej skierowany jest na prawo, co symbolicznie ukazuje więź ze sobą z jednej strony przyczyn i skutków (na rysunku zaznaczonych jako blok o ciemnoszarym kolorze). Z drugiej strony nie sposób abstrahować od oczywistego w kategoriach prostej logiki związku przyczynowo-skutkowego paradygmatu OLI z nowoczesnym podejściem do zagadnienia rozwoju gospodarczego, w którym eksponuje się rolę BIZ jako czynnika prorozwojowych zmian w strukturze gospodarek krajów świata (w sensie: uczestniczących w procesie produkcji międzynarodowej, czyli otwartych na BIZ), prowadzących je ostatecznie do superwzrostu (jak to ujęte zostało w cytowanej już teorii T. Ozawy).

Przez przepływ kapitału rozumie się wszelki odnotowywany w bilansie płatniczym ruch kapitału przez granicę, którego podmiotami mogą być instytucje sektora publicznego oraz prywatnego. Znaczna część międzynarodowych przepływów kapitału przyjmuje postać bezpośrednich inwestycji zagranicznych, czyli kontrolowanego przez przedsiębiorstwo macierzyste za granicą komplementarnego pakietu czynników nakładczych, tj. kapitału akcyjnego, wiedzy i przedsiębiorczości[8].

Zgodnie z definicją opracowaną przez OECD, *bezpośrednią inwestycją zagraniczną* (BIZ) jest inwestycja dokonana przez rezydenta jednej gospodarki (inwestora bezpośredniego) w celu osiągnięcia długotrwałej korzyści z kapitału zaangażowanego w przedsiębiorstwo – rezydenta innej gospodarki (przedsiębiorstwo bezpośredniego inwestowania, zwane inaczej filią zagraniczną). Przedsiębiorstwem bezpośredniego inwestowania jest przedsiębiorstwo, w którym inwestor bezpośredni posiada co najmniej 10% akcji zwykłych (tzn. udziału w kapitale) lub uprawnienia do 10% głosów na walnym zgromadzeniu akcjonariuszy lub udziałowców)[9]. Kraj

[7] L. Tarasiński, *Międzynarodowa wymiana gospodarcza i konkurencyjność czynnikami gospodarczej restrukturyzacji i wzrostu dobrobytu. Implikacje dla Polski*, [w:] *Gospodarka XXI wieku. Wyzwania rozwojowe*, pr. zbiorowa pod red. M. Lament, J. Bukowskiej, CedeWu, Warszawa 2021, s. 21.

[8] E. Cyrson, *Korporacje wielonarodowe. Prawidłowości ekspansji zagranicznej*, PWN Warszawa 1981, s. 29.

[9] *Bilans płatniczy na bazie transakcji oraz Bilans aktywów pasywów Rzeczypospolitej Polskiej*, Narodowy Bank Polski, Warszawa, wrzesień 2003, s. 88; patrz także: *Bezpośrednie inwestycje zagraniczne na świecie i w Polsce: tendencje, determinanty i wpływ na gospodarkę*, raport UNCTAD i Ministerstwa Gospodarki RP, Warszawa 2002, s. 13.

pochodzenia bezpośredniego inwestora określa się mianem *kraju inwestującego* lub – częściej – *goszczonego*, zaś kraj, w którym inwestycji bezpośredniej się dokonuje, nazywamy *krajem przyjmującym* BIZ lub *krajem goszczącym*. Kapitał BIZ obejmuje kapitał podstawowy (akcyjny lub udziałowy), wnoszony w postaci pieniężnej lub jako raport rzeczowy, dopłaty do kapitału, reinwestowane zyski (mianem reinwestowanego zysku określamy przypadającą na inwestora bezpośredniego tę część zysku, która pozostaje w przedsiębiorstwie bezpośredniego inwestowania i jest przeznaczona na jego rozwój) oraz inne należności i zobowiązania związane z zadłużaniem się między przedsiębiorstwami powiązanymi kapitałowo (głównie kredyty inwestorów, tzw. *intercompany loans*)[10].

Istotą bezpośrednich inwestycji zagranicznych jest „transmisja do kraju goszczącego »spakowanego« kapitału, umiejętności menedżerskich i wiedzy technicznej"[11]. Z takiego ujęcia istoty BIZ wynika, że inwestycje te nie są transferem jednorodnego czynnika wytwórczego – kapitału pieniężnego – który może być alokowany i realokowany w dowolnym obszarze gospodarki. W rezultacie, w przeciwieństwie do międzynarodowych ruchów kapitału pieniężnego, takie inwestycje są przeniesieniem ponad granicami krajów wysoce zdywersyfikowanego pakietu aktywów – czynników wytwórczych, wśród których ruch kapitału pieniężnego ma znaczenie marginalne. Z tego też powodu nie mogą być – w przeciwieństwie do międzynarodowych przepływów kapitału pieniężnego – absorbowane przez całą gospodarkę i umożliwiać osiągnięcie równowagi ogólnej (w dwóch krajach, goszczonym i goszczącym)[12].

Bezpośrednie inwestycje zagraniczne jako forma przepływów kapitału ewoluują w kierunku coraz istotniejszej formy powiązań w skali światowej, zarówno między krajami wysoko rozwiniętymi, jak i rozwijającymi się. Ich obserwowany systematyczny wzrost umożliwia współpracę przemysłowo-handlową oraz wykształca relacje współzależności między różnymi krajami i ich grupami. Od początku procesu rozwoju bezpośrednich inwestycji zagranicznych zarysowała się prawidłowość,

---

[10] *Bilans płatniczy na bazie transakcji oraz Bilans aktywów pasywów Rzeczypospolitej…*, op. cit., s. 88.

[11] H. Johnson, *Survey of Issues*, P. Drysdale ed., „Direct Foreign Investment in Asia and Pacific", Australian National University Press, Canberra, 1972, s. 2, za: K. Kojima, *International Trade and Foreign Investment: Substitutes or Complements*, Hitotsubashi Academy 1975, s. 6.

[12] Chodzi o to, że inwestycje bezpośrednie, mające formę wyłącznie ruchów kapitału pieniężnego, (który następnie przekształca się w kapitał rzeczowy), są w jednakowym stopniu potrzebne wszystkim dziedzinom gospodarki narodowej, ponieważ w każdym procesie wytwórczym kapitał jest jego nieodzownym elementem składowym. Kapitał ten jest też – podobnie jak kredyt bankowy – potencjalnie dostępny wszystkim dziedzinom gospodarki kraju goszczącego, które zechcą zapłacić za niego wyższą cenę. Zupełnie inaczej jest z inwestycjami bezpośrednimi, w przypadku których kapitał pieniężny jest jedynie ich (nieistotną) częścią. Wówczas nie wszystkie, a tylko specyficzne podmioty gospodarki narodowej są w ogóle w stanie zaabsorbować takie inwestycje.

polegająca na tym, że najczęściej kraje wysoko rozwinięte były stroną eksportującą kapitał w tej formie do krajów o relatywnie niższym osiągniętym poziomie rozwoju, które weszły na drogę rozwoju przemysłowego później od krajów pierwszej generacji[13]. Poniekąd ma to związek z historycznie zdeterminowaną współczesną sytuacją finansową krajów wysoko rozwiniętych. Ukształtowała się ona bowiem jako produkt rozciągniętego na całe stulecia historycznego procesu międzynarodowych przepływów finansowych: od XIV w. począwszy, gdy centrum światowych finansów było zlokalizowane w miastach północnych Włoch (Wenecja, Florencja, Mediolan, Genua) poprzez wiek XVII i XVIII, gdy tę funkcję przejęła Holandia, tracąc ją następnie na rzecz londyńskiego City (wiek XIX), do którego na początku XX w. dołączyło centrum Wall Street z Nowego Jorku. Jesteśmy wreszcie w trzecim tysiącleciu, kiedy nie sposób nie zauważać wzrostu znaczenia centrów finansowych Dalekiego Wschodu – z japońskimi i chińskimi bankami i instytucjami finansowymi na czele[14]. Dla bezpośrednich inwestycji zagranicznych znaczącym był niewątpliwie moment (przełom XIX i XX w.), kiedy na arenie jako eksporter kapitału pojawiły się Stany Zjednoczone ze swoimi wielkimi przedsiębiorstwami, lokującymi swoje filie zagraniczne najpierw w Kanadzie i Ameryce Południowej, a następnie – w okresie między wojnami światowymi – także w Europie. Okres po II wojnie światowej to już niewątpliwie czas postępującej niezwykle dynamicznie globalnej ekspansji korporacji amerykańskich. Również w pozostałych światowych gospodarkach dokonywanie bezpośrednich inwestycji zagranicznych zaczęło się dynamicznie rozwijać, jakkolwiek z pewnym opóźnieniem, uwarunkowanym dystansem występującym między korporacjami amerykańskimi i np. europejskimi.

Bezpośrednie inwestycje zagraniczne stanowią niezmiernie ważny fragment światowej wymiany gospodarczej. Od 1985 r. począwszy ich wielkość systematycznie się zwiększa. Tego rodzaju prawidłowość zmian BIZ w ujęciu globalnym wynika z wielu uwarunkowań współczesnego świata. Postęp techniczny, zwłaszcza rewolucyjne zmiany w dziedzinach szeroko rozumianej komunikacji oraz przetwarzania i przenoszenia informacji sprawiają, że zarządzanie przedsiębiorstwem globalnym jest nie tylko możliwe, ale – wobec coraz powszechniejszego dostępu do informacji – efektywniejsze niż kiedykolwiek. Niezmiernie ważne są też szeroko rozumiane instytucjonalne uwarunkowania gospodarki światowej, w szczególności zaawansowanie procesów integracyjnych i uruchomienie pewnych procesów w dziedzinie polityki ekonomicznej. Po pierwszym okresie dynamicznego rozwoju BIZ, przypadającym na lata pięćdziesiąte i sześćdziesiąte XX wieku, liberalizacja przepływów kapitałowych została zahamowana w rezultacie przedsięwzięcia przez szereg krajów europejskich klauzul ochronnych (lata siedemdziesiąte). W istotnym stopniu dotyczyło to również BIZ. Związane to było ze skutkami ówczesnego kryzysu ekonomicznego, wywołanego spektakularnym wzrostem cen ropy naftowej

[13] J. Rutkowski, *Eksport kapitału*, PWN Warszawa 1972, rozdz. I i II.

[14] J. Rutkowski, *Światowe strumienie kapitałowe, rozprawy i studia*, t. (CC)126, Uniwersytet Szczeciński, Szczecin 1992, s. 11-47.

i pochodnych, przede wszystkim z niestabilnością międzynarodowych stosunków monetarnych i pogorszeniem się warunków gospodarowania w następstwie załamania się systemu stałych kursów walutowych z Bretton Woods. Do tych czynników zewnętrznych należy dodać przyczyny wewnętrzne, polegające głównie na braku koordynacji polityki ekonomicznej poszczególnych krajów – członków EWG – w zakresie takich celów, jak wolny handel, stabilność stosunków monetarnych między krajami i swoboda przepływu kapitału. Jednak w latach osiemdziesiątych proces liberalizacji przepływów kapitałowych zostaje ponownie uruchomiony, co wynikło z poprawy zewnętrznej pozycji wielu krajów europejskich. Spadło ryzyko wystąpienia kłopotów w bilansie płatniczym, a efektywność zewnętrznych regulacji dotyczących przepływów kapitałowych okazała się być niezadowalająca. Zrozumiano, że restrykcje wobec przepływów kapitałowych jedynie opóźniają powszechnie uświadamiane jako konieczne strukturalne dostosowania w poszczególnych gospodarkach. Jednocześnie, w warunkach zarysowania się silnej tendencji do deregulacji narodowych rynków finansowych, pojawiły się przesłanki do rozwoju rozległego, nieregulowanego eurorynku[15]. Te okoliczności w istotnym stopniu złożyły się na postęp integracji w ramach EWG, a następnie Unii Europejskiej, zdecydowanie sprzyjający BIZ. Z drugiej strony, dynamika integracji gospodarek europejskich wywołała zaniepokojenie przedsiębiorstw spoza Unii, u źródeł którego legło przekonanie o wzrastaniu znaczenia tego obszaru w świecie i obawa, że towarzyszące integracji zmiany instytucjonalne mogą utrudnić wejście na ten rynek w przyszłości[16]. Jednocześnie bardzo duże znaczenie dla dynamicznego rozwoju BIZ, notowanego w okresie ostatnich dwóch dekad, miały pewne procesy, zachodzące w zakresie polityki ekonomicznej. Przede wszystkim należy wskazać na masową prywatyzację i systematycznie postępującą deregulację poszczególnych gospodarek światowych, w szczególności rozwiniętych krajów Zachodu (np. Niemcy, Wielka Brytania, Francja) oraz – w początkach lat dziewięćdziesiątych – gospodarek Europy Środkowo-Wschodniej, w związku z rozpoczęciem przez nie transformacji systemowej[17].

Bezpośrednie inwestycje zagraniczne wyrażają istotę przedsiębiorstwa wielonarodowego – są elementem procesu przekształcania się firmy lokalnej w ogólnonarodową, a następnie w przedsiębiorstwo wielonarodowe (wielką korporację transnarodową – WKT). Proces ten polega na zanikaniu w działalności przedsiębiorstwa podziału na rynek wewnętrzny i zagraniczny, podobnie, jak zaniknął wcześniej podział na rynek lokalny i ogólnokrajowy. Przedsiębiorstwo to, osiągnąwszy stadium korporacji transnarodowej jest firmą narodową podejmującą za granicą bezpośrednie

---

[15] J. Witkowska, *Bezpośrednie inwestycje zagraniczne w warunkach stowarzyszenia i przyszłego członkostwa w WE*, [w:] *Biała Księga. Polska-Unia Europejska*, Wydawnictwo URM Biura ds. Integracji Europejskiej oraz Pomocy Zagranicznej, s. 16.

[16] A. Budnikowski, E. Kawecka-Wyrzykowska, *Międzynarodowe stosunki gospodarcze*, praca zbiorowa, PWE, Warszawa 1999, s. 135.

[17] Tamże, s. 134-137.

inwestycje zagraniczne i traktujące zagraniczną aktywność na równi z przeprowadzanymi przezeń operacjami krajowymi.

Bezpośrednie inwestycje zagraniczne podejmowane przez WKT mają na celu albo zapewnienie sobie dostaw tańszych surowców naturalnych (tzw. pionowo zintegrowane WKT), albo – najczęściej – uruchomienie za granicą produkcji wyrobów, w których wytwarzaniu i marketingu wyspecjalizowały się w kraju (integracja pozioma). Pierwszy typ inwestycji zagranicznych jest przykładem ekspansji WKT obecnie rzadko występującym i ma charakter zdecydowanie historyczny niż perspektywiczny (BIZ tego typu stopniowo zanikają, a swój najlepszy okres przeżywały w czasie przed II wojną światową). Natomiast inwestycje bezpośrednie będące przejawem pogłębiania się integracji poziomej WKT cechuje szczególnie duża dynamika rozwojowa. W przeciwieństwie do korporacji o integracji pionowej, inwestycje bezpośrednie będące przejawem integracji poziomej cechuje wysoki poziom technologiczny, znaczne umiejętności menedżerskie i marketingowe, w związku z czym są one szczególnie mile widziane przez kraje goszczące[18].

Rozważając podstawowe motywy podejmowania BIZ, należy wyróżnić:

- chęć osiągnięcia wyższego zysku, w sytuacji występowania różnic stóp zysku w kraju macierzystym i potencjalnym kraju goszczącym. Ze względu na bariery natury technicznej, ryzyko i towarzyszący BIZ kontekst polityczny różnica ta musi być na tyle istotna, aby kompensowała z nadwyżką te niedogodności[19];
- nadpodaż kapitału, występującą w warunkach krótkookresowego podwyższania się stopnia wolnych mocy wytwórczych w gospodarce kraju macierzystego. Wolna, niewykorzystana część kapitału w naturalny dla siebie sposób poszukuje produktywnych zastosowań;
- wykorzystanie przewagi technologicznej, która wobec wyczerpania się możliwości ekspansji w kraju macierzystym, stwarza szansę na osiągnięcie dużych zysków za granicą tym większe, im większe jest „rozwarcie" będącej wyrazem przewagi luki technologicznej[20];

[18] Tamże, s. 31-33.

[19] Bezpośrednim inwestycjom zagranicznym towarzyszy wyższe ryzyko oraz większe koszty komunikacji niż krajowej działalności. W tych warunkach przedsiębiorca musi oczekiwać większych niż w kraju macierzystym przychodów od kapitału zainwestowanego za granicą. Inwestor podejmujący działalność za granicą oczekuje również wyższych przychodów niż lokalni konkurenci w kraju goszczącym, ponosi bowiem koszty, których lokalne firmy nie mają (związane ze zdobyciem i wykorzystaniem wiedzy o obcym środowisku). Tak więc przedsiębiorstwa zagraniczne liczą na wyższe zyski, dodatkowo uzasadniając to swoją wyższością techniczno-technologiczno-organizacyjną, wspartą potencjałem wysokokwalifikowanych pracowników. Patrz: J. Górski, *Przemiany we współczesnej ekonomii burżuazyjnej*, praca zbiorowa, PWE, Warszawa 1987, s. 229-230.

[20] P. Bożyk, J. Misala, M. Puławski, *Międzynarodowe stosunki ekonomiczne*, op. cit., s. 153.

- rozszerzenie kontroli poprzez stwarzanie możliwości formowania się organizacji wielonarodowych. Lokalizacja produkcji w dwu (lub więcej krajach) zasadniczo jest zdeterminowana przez relatywną dostępność, jakość i cenę zasobów, koszty transportu, ustawodawstwo regulujące działalność obcego kapitału, zróżnicowanie poziomu rozwoju cywilizacyjnego pomiędzy krajem inwestora zagranicznego (goszczonym) a krajem goszczącym oraz stosunkiem społeczeństwa do kapitału zagranicznego[21]. Z drugiej strony, problem tzw. *internalizacji*, tzn. produkcji w różnych miejscach świata przez tę samą firmę (a nie przez firmy obce) wskazuje, że postępowało będzie wewnętrzne zespolenie firmy wielonarodowej, co należy również postrzegać jako istotny aspekt ekspansji bezpośrednich inwestycji zagranicznych. W tym wypadku podkreślić należy korzyści internalizacji wynikające przede wszystkim dla transferu technologii i integracji pionowej. Chodzi o to, że bardzo często technologia, jako nie poddająca się opisowi i „zapakowaniu" wiedza określonej grupy specjalistów, w tej postaci nie podlega po prostu sprzedaży. Poza tym niezmiernie dyskusyjna i trudna do rozwiązania jest kwestia egzekwowania praw własności w odniesieniu do wiedzy. Zatem firma, zamiast sprzedawać licencję, wybierze wariant zwiększania zysków poprzez założenie filii. Istotnym jest również to, że jeśli firma wytwarza produkt używany jako wkład do produkcji innej firmy, mogą wyniknąć liczne problemy koordynacji w obszarze np. zarządzania cenami czy ryzykiem – w tym wypadku integracja pionowa wiele z tych niedogodności usuwa albo przynajmniej pomniejsza ich znaczenie[22];
- implikacje, wynikające ze strategii współczesnych wielkich przedsiębiorstw, upatrujących szans własnego rozwoju w ekspansji na rynek światowy. Strategia globalna jako połączenie zbioru strategii lokalnych jest potrzebą najsilniej odczuwaną przez współczesne duże przedsiębiorstwa. Nie chodzi już tylko o produkcję dóbr i usług dostosowanych do potrzeb lokalnych (tzw. strategia multilokalna). Problem w tym, że niemal wszystkie gałęzie produkcji w jakimś zakresie są lub mogą być globalne. Kwestią do rozstrzygnięcia jest odpowiedź na pytanie: na ile globalny charakter ma dziedzina działalności danego przedsiębiorstwa? Przemysł, w którym pozycja konkurencyjna firmy w jednym kraju jest istotnie uzależniona od pozycji konkurencyjnej w innych krajach jest przemysłem globalnym[23]. Każdy rynek dóbr i usług w kluczowych gospodarkach światowych ma zagranicznych konkurentów. Nasilanie się zagranicznej konkurencji jest dostatecznie silnie oddziałującym na przedsiębiorstwa bodźcem w kierunku ich globalizacji, osiągnięcia takich rozmiarów i zdolności konkurowania, które zapewniłyby

[21] A. Budnikowski, E. Kawecka-Wyrzykowska, *Międzynarodowe…*, op. cit., s. 133.
[22] P.R. Krugman, M. Obstfeld, *Międzynarodowe stosunki gospodarcze*, Tom 1, PWN, Warszawa 1997, s. 126-127.
[23] M. Porter, *Strategia konkurencji*, PWE, Warszawa 1994.

> sukces. Jednocześnie rewolucja w dziedzinie komunikacji i informacji stwarza dodatkową zachętę dla przedsiębiorstw myślących kategoriami zarządzania globalnego biznesem, ponieważ sprawowanie kontroli w warunkach wysokiej efektywności przepływu informacji nie wydaje się czymś niewyobrażalnie trudnym[24].

Pierwsze próby teoretycznego uzasadnienia procesu rozwoju bezpośrednich inwestycji zagranicznych wywodzą się z *teorii międzynarodowych ruchów kapitału* (zwanych odtąd zamiennie teoriami stopy procentowej lub teoriami portfelowymi), wyjaśniających inwestycje portfelowe i – w dalszej kolejności – bezpośrednie[25] [zdaniem niektórych badaczy należy teorie te zaliczyć do grona *makroekonomicznych hipotez rozwoju BIZ*, albowiem wyraźnie bazują one na założeniach teorii obfitości zasobów (*model H-O-S*)][26]. W przypadku obu rodzajów inwestycji zwrócić należy jednak uwagę na podstawową różnicę występującą między nimi: inwestycje portfelowe jako wyłącznie płatności stanowiły jednorodny pakiet aktywów, generalnie nie kontrolowanych przez inwestora zagranicznego, podczas gdy inwestycje bezpośrednie były wysoce zdywersyfikowanym portfelem wszelkich (nie tylko finansowych) aktywów, nad którym sprawowano bezpośrednią kontrolę, polegającą na faktycznym decydowaniu przez korporację o sposobach wykorzystania czynników wytwórczych, zlokalizowanych za granicą. Pierwotnie twierdzono, iż właściwym – dla obu rodzajów inwestycji zagranicznych – motywem inwestowania są różnice w stopach procentowych między krajami. Przy takim wyjaśnieniu przyczyn długoterminowych międzynarodowych lokat kapitału transfer kapitału kończył się w momencie zrównania się krańcowych przychodów z kapitału w krajach goszczącym

---

[24] G.S. Yip, *Strategia globalna*, PWE, Warszawa 1996, s. 21-30.

[25] Trzeba zauważyć, że mówi się tu o teorii w liczbie mnogiej. W istocie bowiem – o ile mowa tu o pewnej uniwersalnej idei, wyjaśniającej motywy międzynarodowych przepływów kapitału – należy pamiętać, że przede wszystkim chodzi tu o szeroko rozumiany dorobek ekonomii klasycznej i neoklasycznej, w którym, tj. w każdym z poszczególnych przypadków (D. Ricardo, D. Hume`a, J.S. Milla, B. Ohlina, G. Haberlera, C. Iversona i innych) odnoszono się do kwestii przepływów kapitału. Ponadto warto również w tym miejscu podkreślić, że w czasie, kiedy teorie te były formułowane, w łącznych przepływach międzynarodowego kapitału pozycją zdecydowanie dominującą były inwestycje portfelowe. Do początku XX w. inwestycje portfelowe stanowiły niemal całość kapitału o charakterze lokat długoterminowych, a nieliczne inwestycje bezpośrednie, podejmowane głównie w przemyśle wydobywczym stanowiły raczej wyjątek niż regułę (w 1914 r. inwestycje portfelowe stanowiły 90% światowego eksportu kapitału długoterminowego. Patrz: J.H. Dunning, *Studies in International Investment*, London 1970, s. 2 i 26; M. Geldner, *Przyczynek do teorii zagranicznych inwestycji bezpośrednich*, MiO nr 193, SGPiS, Warszawa 1986, s. 65). Dlatego też dość często zamiennie dla teorii tych stosuje się jedno określenie: teoria portfelowa.

[26] J. Misala, *Współczesne teorie wymiany międzynarodowej i zagranicznej polityki ekonomicznej*, SGH, Warszawa 2001, s. 214.

i goszczonym[27]. Jednak, począwszy od końca I wojny światowej aż do czasów współczesnych, realia ekonomiczne dostarczały coraz więcej powodów do tego, by wyjaśnienie przyczyn ekspansji WKT w ramach teorii międzynarodowych ruchów kapitału uznać za nie w pełni wystarczające i nastręczające wątpliwości w szeregu kwestiach. W kontekście BIZ zawodność teorii międzynarodowych ruchów kapitału przejawiała się po prostu w niemożności wyjaśnienia na gruncie teorii wielu ważnych zjawisk z obszaru praktyki rozwoju BIZ. Warto zatrzymać się na chwilę przy najczęściej podnoszonych kwestiach. I tak, stosownym jest pytanie, dlaczego – skoro BIZ są wynikiem dążenia przedsiębiorstw z gospodarek obfitych w kapitał do eksportu kapitału na rynki, odczuwające jego względny niedostatek i, w związku z tym, zapewniające jego wyższą rentowność – eksport kapitału ma przyjąć formę BIZ, a nie np. pożyczki i/lub inwestycji portfelowej. Jest bowiem faktem, że o ile przed I wojną światową dominującą formą eksportu kapitału były inwestycje portfelowe, to później, zwłaszcza po II wojnie światowej, w łącznym eksporcie kapitału wyraźnie zaczynają przeważać bezpośrednie inwestycje zagraniczne. Innym ważnym, rzeczywistym problemem jest zjawisko tzw. inwestycji bezpośrednich „krzyżujących się". Obserwacja rozwoju BIZ wskazuje na pewną istotną ich prawidłowość: przedsiębiorstwa różnych krajów inwestują w tym samym czasie wzajemnie u siebie w podobnych dziedzinach wytwórczości, przy czym przepływy te mają miejsce nie tylko pomiędzy poszczególnymi parami krajów, lecz – przede wszystkim – odbywają się w ramach tej samej gałęzi[28]. W obliczu istnienia takiej tendencji można raczej podejrzewać, że motywem podejmowania inwestycji są tu nie tyle różnice ilościowe w wyposażeniu w kapitał, powodujące międzynarodowe zróżnicowanie stóp procentowych, ile różnice w jego jakości oraz inne czynniki. W takim razie tradycyjna teoria stopy procentowej (tzn. teoria portfelowa) nie daje wytłumaczenia dla tego przypadku BIZ.

Poważne wątpliwości wyrażane z punktu widzenia oceny przydatności teorii stopy procentowej do wyjaśnienia przyczyn BIZ nasuwa również ocena geograficznej struktury międzynarodowych przepływów BIZ. Z teorii tej bowiem wynika, że międzynarodowy dysparytet stóp procentowych powinien spowodować koncentrację BIZ w regionach słabo wyposażonych w kapitał –powinien on przepływać na linii kraje rozwinięte – kraje rozwijające się. Tymczasem gros przepływów BIZ ma miejsce w obszarze rozwiniętych gospodarek Północy, w szczególności w jej zachodniej części. Zatem przepływy te z pewnością nie są motywowane czynnikiem zapewnienia relatywnie wyższej rentowności lokatom kapitału.

---

[27] Iverson C., *Some Aspects of the Theory of International Capital Movements*, London 1936, za: J. Górski praca zbiorowa, *Przemiany we współczesnej myśli burżuazyjnej*, op. cit., s. 228.

[28] Prawidłowość ta jest zresztą przejawem ogólnej współczesnej tendencji charakteryzującej międzynarodowy podział pracy, tzn. systematycznego wzrostu znaczenia wymiany wewnątrzgałęziowej (i towarzyszącego tej tendencji zmniejszania się znaczenia wymiany międzygałęziowej).

Ciekawą konstrukcją teoretyczną o charakterze makroekonomicznym jest teoria obszarów walutowych R.Z. Alibera, w której podnosi się znaczenie istnienia różnych stref walutowych dla podejmowania BIZ, będących naturalnym skutkiem różnej siły poszczególnych walut świata na międzynarodowym rynku pieniężnym[29]. Dane przedsiębiorstwo utrzymuje swoje aktywa w określonej walucie. W rezultacie wniosków wynikających z obserwacji relatywnej siły waluty kraju inwestora (goszczonego) w porównaniu z siłą walut potencjalnych krajów lokaty (goszczących), uwzględniających dodatkowo również stopień ryzyka kursowego, podejmowane są inwestycje. Zazwyczaj pozycja waluty kraju inwestora jest lepsza i stabilniejsza, niż pozycja waluty kraju lokaty. W efekcie strumienie BIZ płyną z krajów o silnej walucie do krajów o słabej walucie. Zagraniczny inwestor wykorzystuje swego rodzaju premię walutową przy nabywaniu kredytów, akcji itp[30].

Zasygnalizowane wyżej problemy i pytania, na które odpowiedzi próżno by szukać w szczególności w teorii portfelowej, stanowią swego rodzaju świadectwo na istnienie sprzeczności pomiędzy kształtowaniem się BIZ a logiką tej teorii. Zrozumiałe zatem, że w tych okolicznościach zaczęto dostrzegać w bezpośrednich inwestycjach zagranicznych działanie innych czynników, niż znanych z teorii portfelowej determinant międzynarodowych przepływów kapitału. Coraz częściej w wyjaśnianiu przyczyn rozwoju BIZ odwoływano się do innych – niż tylko różnice w poziomie międzynarodowych stóp procentowych – czynników, wskazując na *know-how,* chęć ochrony rynków eksportowych, korzyści ze skali produkcji, przewagę technologiczną, innowacje, itp. Fakt, że w kolejnych interpretacjach teoretycznych zjawiska BIZ zaczęto uwzględniać te czynniki ma, poniekąd, swoje naturalne przyczyny. W istocie bezpośrednie inwestycje zagraniczne nie stanowią jednorodnego pakietu aktywów – są to inwestycje przedsiębiorcze, w przypadku których mamy do czynienia z szeregiem czynników, które stanowią przedmiot międzynarodowych transferów. Wśród nich kapitał jest tylko jednym z elementów zasobów produkcyjnych, przemieszczających się pomiędzy gospodarkami narodowymi. Z dużym prawdopodobieństwem inwestycje bezpośrednie mogą być podejmowane w ogóle bez transferu strumienia netto kapitału. Oznaczają natomiast z pewnością transfer kontroli nad zagranicznymi aktywami, bez jakiegokolwiek przemieszczania się kapitału przez granice państw[31].

Mnogość mankamentów, które ujawniły się w trakcie kolejnych prób weryfikacji teorii portfelowej jako adekwatnej konstrukcji teoretycznej w odniesieniu

---

[29] R. Aliber, *Teoria bezpośrednich inwestycji zagranicznych*, [w:] C.P.Kindleberger, red., *The International Corporation: A Symposium*, wydanie 5, MIT Press, Cambridge, MA, 17-34, 1970, cyt. za: J. Misala, *Współczesne teorie wymiany międzynarodowej i zagranicznej polityki ekonomicznej*, SGH Kolegium Gospodarki Światowej (wydruk komputerowy powielony), Warszawa 2000, s. 267.

[30] Tamże, s. 267-268.

[31] R.E. Caves, *International Corporations: The Industrial Economics of Foreign Investment*, „Economica", Vol. XXXVIII, No. 149, February 1971, s. 2-3.

do bezpośrednich inwestycji zagranicznych, zrodziła potrzebę sformułowania nowej teorii, która kompleksowo objaśniałaby różne, dyskusyjne kwestie. Trzeba dodać, że potrzebę pilną, albowiem po II wojnie światowej, zwłaszcza począwszy od 1950 roku, zjawisko BIZ zaczęło się nasilać, zdążając do znacznych, niespotykanych dotąd rozmiarów. Niewątpliwie na uwagę zasługują tu teoria przedsiębiorstwa, konkurencji i lokalizacji (które w większości są konstrukcjami teoretycznymi o charakterze mikroekonomicznym).

Jedną z podstawowych reguł, rządzących zachowaniem się przedsiębiorstwa działającego w warunkach rynku jest zasada maksymalizacji zysku. Przedsiębiorstwo kierujące się tą regułą, inwestując, będzie dążyło do zrównania krańcowej rentowności kapitału z jego kosztem krańcowym. W rezultacie istnienia międzynarodowego dysparytetu stóp zysku kapitał (mający formę BIZ) będzie przepływał z krajów charakteryzujących się niższą przeciętną stopą zysku do gospodarek, gdzie ta stopa jest wyższa. Tego rodzaju uzasadnienie źródeł istnienia bezpośrednich inwestycji zagranicznych było dość popularne w latach pięćdziesiątych XX w., ponieważ swoistego wsparcia dla tej hipotezy dostarczały obserwacje inwestycji bezpośrednich korporacji amerykańskich w Europie Zachodniej[32]. Hipoteza ta, jak widać, nie różni się znacząco od poglądów prezentowanych w teorii portfelowej (poza tym, że jej źródłem jest *neoklasyczna teoria przedsiębiorstwa*, a nie teoria kapitału, tzn. stopy procentowej). W tym sensie zatem ocena przydatności neoklasycznej teorii przedsiębiorstwa jest porównywalna z analogiczną oceną, którą wcześniej wystawiono teorii stopy procentowej. Nasuwa się też i taka refleksja, że walory neoklasycznej teorii przedsiębiorstwa, jako teorematu rzetelnie objaśniającego mechanizmy rządzące zachowaniem się przedsiębiorstwa wolnorynkowego, ujawniają się w całej pełni, ale w odniesieniu do przedsięwzięć quasidoskonale konkurencyjnych, czyli firm, w których – ze względu na ich niezmiernie małe rozmiary – z całą pewnością na próżno by szukać przesłanek do umiędzynarodowienia przez nie swojej aktywności.

Dyskusyjny charakter zaprezentowanej wyżej hipotezy ujawniły późniejsze zjawiska i tendencje, wobec których niemożliwym było utrzymanie jej jako stwierdzenia prawdziwego. Chodzi tu głównie o to, że mimo późniejszego wyrównania się stóp zysku (a nawet – krańcowo – odwrócenia się ich relacji na korzyść krajów – eksporterów BIZ), kierunek przepływu BIZ i ich struktura geograficzna nie uległy radykalnym zmianom. Niezależnie od tego, iż przy takim wyjaśnieniu motywów podejmowania BIZ nadal otwartą pozostawała kwestia, dlaczego w poszukiwaniu intratnych lokat kapitałowych preferowane są BIZ a nie inwestycje portfelowe. Ta logiczna niespójność sprowokowała nowe poszukiwania, które interpretatorów BIZ przywiodły do tzw. alternatywnych teorii przedsiębiorstwa. Przede wszystkim miało to związek z faktem, iż – generalnie – w koncepcjach tych podważano zasadę maksymalizacji zysku jako głównego celu działania firmy. Odmienność tych teorii w stosunku do teorii neoklasycznej przedsiębiorstwa wyrażała się – zasadniczo rzecz

[32] M. Geldner, *Przyczynek do teorii…,* op. cit., s. 67.

biorąc – w modyfikacji przez nie zasady maksymalizacji zysku. Zdawano sobie bowiem sprawę z tego, że poza celem zasadniczym, którym dla przedsiębiorstwa jest zysk, istnieją również cele pośrednie, których osiągnięcie z punktu widzenia maksymalizacji zysku jest kwestią niemniejszej wagi, niż koncentrowanie się wyłącznie na maksymalizowaniu zysków. W teoriach tych starano się pokazać, że do zysków prowadzi wiele dróg, spośród których jednym ze sposobów, wcale nie najważniejszym, jest ich maksymalizacja w każdym czasie (tzn. zarówno w krótkim jak i długim). Ukształtowanie się, w efekcie nasilania się wolnej konkurencji, nowych warunków gospodarowania, przede wszystkim zaś wyłonienie się z wielkiej zbiorowości firm niewielu zwycięzców, zasadniczo zmienia sposób widzenia kwestii kształtowania przyszłości firmy, czyli strukturę celów działalności. I właśnie w tym miejscu następuje, co zrozumiałe, zmiana stanowiska teoretycznego w stosunku do przedsiębiorstwa. Trzeba przyznać, że ilość zaproponowanych tu koncepcji teoretycznych jest dość imponująca. Jedną z pierwszych, niewątpliwie godną odnotowywania z uwagi na konsekwencje, które wynikły z niej dla dalszych poszukiwań wyjaśnienia BIZ, była tzw. *teoria menedżerska*[33]. Według niej wskutek wzrostu rozmiarów przedsiębiorstwa jego właściciele tracą kontrolę nad nim na rzecz menedżerów. Ostatecznie, skutkiem tego jest zmiana hierarchii celów przedsiębiorstwa: menedżerowie kierują się przede wszystkim zasadą maksymalizacji osobistych korzyści, które w ich przypadku przekładają się na maksymalizację wielkości sprzedaży, de facto – wielkości firmy, którą zarządzają (można ten cel określić inaczej jako dążenie do maksymalizacji stopy wzrostu). Od tych wskaźników przecież zależy ich wynagrodzenie (zgodnie z maksymą: duża firma – duże zarobki jej dyrektora, mała firma – małe zarobki). Jakie znaczenie może mieć ta zmiana w strukturze celów przedsiębiorstwa z punktu widzenia przedsiębrania właściwej strategii, której elementem, potencjalnie istotnym, są bezpośrednie inwestycje zagraniczne? Zwolennicy wyjaśnienia motywów BIZ utrzymanego w duchu tej teorii argumentują na rzecz dużego znaczenia BIZ jako środka realizacji założonych celów strategicznych przez firmę. W istocie podstawowym celem firmy jest jej ekspansja. Ekspansja firmy poprzez zakładanie przez nią licznych filii zagranicznych oznacza przecież w większym zakresie wykorzystanie korzyści skali, zwiększenie wielkości sprzedaży i umocnienie własnej pozycji na danym rynku, a więc – bynajmniej – jest niesprzeczna z interesem menedżerów. Porównując stanowisko teorii menedżerskiej (wyrażone w kwestii motywów podejmowania BIZ) z poprzednim poglądem, opowiadającym się za międzynarodowym zróżnicowaniem stóp zysku jako głównym czynniku kształtującym BIZ zauważyć należy, że w teorii menedżerskiej poddaje się w wątpliwość nie tylko, a raczej nie tyle samą zasadę maksymalizacji zysków przez WKT, ile w pewnym sensie rozszerza się jej interpretację. Zróżnicowanie stóp zysku może mieć miejsce, ale nie musi –

[33] A.A. Berle, G.C. Means, *The Modern Corporation and Private Property*, N.Y., 1968 (I wyd. 1932) oraz J.K. Galbraith, *The New Industrial State*, London 1967, za: M. Geldner, *Przyczynek do teorii*… op. cit., s. 68-69.

maksymalizacja sprzedaży w skali całej korporacji poprzez wzrost BIZ (których rentowność jest niekiedy, zwłaszcza na początku, niższa niż inwestycji krajowych) ostatecznie zapewnia jej maksymalny zysk i/lub umacnia pozycję konkurencyjną firmy, co jest równoznaczne z tworzeniem możliwości generowania zysków w przyszłości. Logika maksymalizacji zysku w WKT o wydłużonym horyzoncie czasu działania jest odmienna od logiki mającej na celu maksymalizację zysku w krótkim czasie w tym sensie, że „prymitywne robienie pieniędzy" przestało być celem WKT: etos zawodowy menedżerów został podporządkowany maksymalizacji zysku długookresowego poprzez wzrost rozmiarów firmy (czyli maksymalizację sprzedaży). Przy wydłużeniu horyzontu czasu w kalkulacji zysków cele maksymalizacji stopy wzrostu i zysku pokrywają się. Nie jest bowiem celem przedsiębiorstwa osiąganie największych rozmiarów sprzedaży, jeśli ostatecznie nie prowadzi to do maksymalizacji długookresowego zysku[34].

Jak widać, w WKT „niewidzialną rękę rynku" zastąpiła „widzialna ręka" menedżera, który, biorąc na siebie rolę „niewidzialnej ręki", włącza rynek w obszar swego planowania. Działalność firmy zostaje oparta na wieloletniej strategii, w której cena – jako zmienna w walce konkurencyjnej – przestaje być jej głównym narzędziem i traci na znaczeniu na rzecz jakości produktów, ich charakterystyk technicznych oraz inwestowania we wszelkie efektywne formy komunikacji z rynkiem (tzw. *marketing mix*). Taki właśnie charakter konkurencji w oligopolu stanowi główną determinantę przyśpieszenia procesów innowacyjnych w produkcji przemysłowej. Ta ewolucja reguł gry wielkich korporacji transnarodowych legła u podstaw koncepcji R. Vernona, tzw. *modelu międzynarodowego cyklu produktu*, będącej próbą wyjaśnienia procesu upowszechniania się innowacji w skali międzynarodowej. W istocie jest to jedna z ważniejszych i bardzo popularna zarazem teoria, tłumacząca determinanty bezpośrednich inwestycji zagranicznych. Jej głównych źródeł można doszukiwać się w poglądzie, zgodnie z którym duże rozmiary przedsiębiorstw i oligopolistyczna struktura rynku w sposób zasadniczy warunkują innowacje: koszty działalności innowacyjnej są na tyle znaczące, że tylko wielkie przedsiębiorstwa są w stanie je udźwignąć. By działalność ta była opłacalna, trzeba zapewnić jej odpowiednią, wielką skalę, przy czym przedsiębiorstwa muszą kontrolować rynek z takiej samej przyczyny, z jakiej wynalazca potrzebuje ochrony patentowej[35]. R. Vernon, uogólniając długoletnie obserwacje zachowań międzynarodowych korporacji amerykańskich, doszedł do wniosku, iż najlepszym sposobem osiągnięcia tych celów są BIZ. W modelu międzynarodowego cyklu produktu jego twórca dowodzi, że proces inwestowania przebiega wg pewnego schematu, w istocie objaśniającego proces rozpowszechniania się innowacji w skali międzynarodowej. Praprzyczyną tego procesu są warunki konkurencji niedoskonałej – polegającej na dominacji na poszczególnych rynkach wielkich przedsiębiorstw – panujące w oligopolu. Warunki zbytu produktów, które stwarza rozległy rynek oraz relatywnie

[34] Domańska E., *Kapitalizm menedżerski*, PWE, Warszawa 1986, s. 186-189.
[35] Tamże, s. 308.

wysoki dochód *per capita*, zapewniają szybki wzrost popytu na trwałe dobra konsumpcyjne. Firma, sprawując pełną kontrolę nad procesem moralnego starzenia się produktów, skutecznie wpływa na przyśpieszenie tempa wymiany tych produktów (stanowi to element strategii wielkich korporacji) i – w rezultacie – zwiększa tempo wzrostu popytu. Zachodzi tu sprzężenie zwrotne – dynamicznie zwiększające się przychody korporacji wskutek rosnącego popytu, generują wielkie sumy pieniędzy, przeznaczane przez nie na sferę badawczo-rozwojową i ostatecznie owocują kolejnymi innowacjami (nowymi produktami), które następnie jeszcze bardziej zwiększają przychody ze sprzedaży. Ponadto duża obfitość kapitału i wysokie koszty robocizny w porównaniu z zagranicą stanowią dodatkowy bodziec dla wszelkich innowacji substytuujących pracę ludzi pracą maszyn i w ten sposób dodatkowo napędzają popyt inwestycyjny, który mnożnikowo zwiększa popyt globalny i przychody ze sprzedaży w wielkich korporacjach. Najwięksi konkurenci w oligopolu zaczynają doceniać znaczenie nowego źródła zysków – innowacje technologiczne. W pierwszej fazie cyklu wytwarza się wiele odmian produktu nie standaryzowanego przy zastosowaniu względnie jednolitej technologii i zachowaniu znacznej elastyczności struktury produkcji – produkt wprowadza się na rynek wewnętrzny. Jest to okres tzw. dojrzewania produktu, czas, w którym motyw niższych kosztów produkcji generowanych w wypadku lokalizacji produkcji za granicą, nie jest najważniejszym czynnikiem kształtującym decyzje firmy. W tej fazie chodzi głównie o efektywną komunikację producenta z rynkiem, skutkującą decyzją o wyborze racjonalnej struktury produkcji. Z upływem czasu wzrastają rozmiary popytu krajowego, produkcja dóbr i zwiększa się stopień jej standaryzacji. Jednocześnie słabiej odczuwana jest potrzeba zachowania znacznej elastyczności struktury produkcji, bowiem produkt dojrzał do stadium produkcji masowej. Następnie produkt (produkty) staje się przedmiotem zyskownego eksportu (druga faza cyklu produktu), co poprzedzone jest organizacją komunikacji z potencjalnym odbiorcą dobra za granicą oraz tworzeniem sieci dystrybucyjnych. W tym wypadku może się jednak okazać, że pojawiły się zagrożenia dla eksportu w postaci wystąpienia ograniczeń w handlu międzynarodowym. Odpowiedzią firmy na to będzie dążenie do ochrony rynków eksportowych, które przyjmie postać bezpośredniej inwestycji zagranicznej, polegającej na założeniu za granicą własnej filii (produkt wkracza w trzecią fazę swojego cyklu). Odtąd produkt, jako wytwarzany w zagranicznej filii, trafia pod parasol ochronny wprowadzonych przez zagranicę ograniczeń w handlu (najczęściej ceł). Jednak z drugiej strony, silniej oddziałującym na zachowania firmy bodźcem – od chęci ochrony rynków eksportowych – jest umocnienie przewagi w dziedzinie innowacji poprzez znalezienie rentowniejszej niż krajowa lokaty (w postaci inwestycji bezpośredniej), przy czym im bardziej złożona jest innowacja, tym bardziej zasadną jest decyzja o dokonaniu inwestycji bezpośredniej. Kryterium tej decyzji stanowi, że inwestycje te są opłacalne, jeżeli oczekiwany strumień zysków ponad bieżące koszty eksploatacji filii zagranicznej przewyższa strumień zysków z eksportu (o wielkość odpowiadającą kosztowi uruchomienia filii zagranicznej) oraz zapewnia utrzymanie normalnej stopy zysku. Terenem

ekspansji stają się początkowo kraje wysoko rozwinięte o zbliżonym (do gospodarki kraju macierzystego korporacji) modelu gospodarki, aby następnie ich miejsce zajęły kraje o niższym poziomie rozwoju (czwarta faza cyklu). Jak się wydaje, przyczyn wejścia produktu w swoją czwartą fazę należy szukać w tym, że w miarę postępów w rozprzestrzenianiu innowacji na obszarze państw wysokorozwiniętych, mobilność i zdolności adaptacyjne firm pochodzących z tych państw sprawiają, że przewaga korporacji międzynarodowej w dziedzinie innowacji ulega zachwianiu. W obawie przed nasilaniem się tych negatywnych tendencji, korporacje, koncentrując się coraz bardziej na sposobach poprawy rentowności, na najwyższym stopniu standaryzacji produktu jego produkcję lokują w krajach gospodarczo słabo rozwiniętych, ale dysponujących znacznymi zasobami taniej siły roboczej. Filiom, ulokowanym w tych krajach najczęściej powierza się produkcję nie tyle kompletnych produktów, co wytwarzanie podzespołów (należy pamiętać, że w tej fazie poziom standaryzacji produkcji jest najwyższym z możliwych), co każe przypuszczać, że w przypadku tych gospodarek korzystny wpływ na nie BIZ jest zdecydowanie mniejszy niż w przypadku gospodarek, które włączają się do międzynarodowego cyklu życia produktu w jego fazie trzeciej. Związane jest to niewątpliwie z tym, że lokalne firmy w krajach rozwiniętych zachowują zdecydowanie bardziej aktywną postawę w procesie adaptacji i uczenia się; niejednokrotnie same, na własną rękę, prowadzą prace badawczo-rozwojowe, co w połączeniu z odpowiednio wysoką kulturą przedsiębiorczości gwarantuje dużą dynamikę rozwoju nowoczesnych gałęzi produkcji. W efekcie występująca na „wejściu" luka technologiczna i organizacyjna (między tą kategorią krajów goszczących i krajem goszczonym) maleje i struktury gospodarcze tych krajów istotnie upodabniają się do siebie[36)].

Fakt, że w poszukiwaniach wyjaśnienia motywów BIZ autorzy odwołali się m.in. do teorii menedżerskiej, która zakłada, iż podstawowym celem działalności firmy – ściślej rzecz biorąc WKT – jest maksymalizacja sprzedaży, wymownie świadczy o rezygnacji z kanonu konkurencji doskonałej i systematycznym „przemieszczaniu" się w kierunku mikroekonomicznej teorii (przedsiębiorstwa) konkurencji niedoskonałej. Właściwością konkurencji niedoskonałej jest przecież ograniczenie liczby uczestników rynku, tożsame ze wzrostem rozmiarów poszczególnych firm i zrozumiałym dążeniem przez nie do maksymalizacji sprzedaży. W istocie liczne, późniejsze teorie związane ze zjawiskiem BIZ, są w gruncie rzeczy sformułowanymi z punktu widzenia inwestycji bezpośrednich mikroekonomicznymi teoriami konkurencji niedoskonałej (monopolistycznej i oligopolistycznej).

Przedsiębiorstwo decydujące się na założenie zagranicznej filii ma świadomość konieczności poniesienia dodatkowych kosztów działania na odległość. Zatem, o ile zagraniczne filie WKT mimo tych kosztów są konkurencyjne w stosunku do przedsiębiorstw kraju goszczącego, muszą decydować o tym pewne przewagi konkurencyjne, dające mu względnie większą siłę monopolową. W *teorii przewagi własnościowej przedsiębiorstwa* [S. Hymer (1960), Ch.P. Kindleberger (1969),

36 Tamże, s. 300-313.

Caves R. (1971) oraz F.T. Knicker Brocker R.] jej twórcy głoszą, że istotną przesłanką umiędzynarodowienia produkcji przez przedsiębiorstwa jest dysponowanie określoną przewagą oraz możliwościami trwałego zawłaszczenia tejże. Warunkiem, by zawłaszczenie się powiodło jest, by przewaga była na tyle istotna, że jej wielkość będzie wystarczająca do neutralizacji z natury rzeczy lepszej pozycji wyjściowej firm kraju potencjalnej lokaty BIZ, oraz że umożliwi uprzedzenie podobnej strategii rywali z branży[37].

Zgodnie z *teorią zachowywania się przedsiębiorstw*, sformułowaną przez Y. Aharoni, punktem wyjścia decyzji o podjęciu BIZ jest ograniczoność informacji dotyczących szans rozwoju przedsięwzięcia zagranicznego oraz konsekwencji ich funkcjonowania[38]. Wobec tej niepewności zarządy firm skłonne są raczej przeceniać ryzyko związane z ekspansją zagraniczną. Jedynie silne bodźce zewnętrzne w postaci extra zachęt do lokowania filii wysyłane przez dany kraj goszczący (lub – dla odmiany – przedsiębranie przez ten kraj działań skutkujących powstaniem silnych barier dla handlu) skutkują zazwyczaj podjęciem decyzji o BIZ. Ten moment podjęcia decyzji zazwyczaj oznacza też wykształcenie się w firmie swoistego lobby popierającej aktywność międzynarodową[39].

Wśród teorii mikroekonomicznych BIZ wskazać trzeba również na *teorię zawłaszczalności* autorstwa S.P. Magee[40]. Wg niej istotnym problemem przedsiębiorstw – liderów w zakresie innowacyjności jest chęć skutecznego przeciwdziałania utracie innowacji na rzecz konkurentów-naśladowców. Przedsiębiorstwo ponosi duże nakłady związanie z finansowaniem sfery badawczo-rozwojowej swojej działalności, co skutkuje opracowywaniem nowoczesnych produktów, z dużym „wsadem" wiedzy technicznej. Jednak ta wiedza w znacznej części ma też charakter dobra publicznego. Zatem, zwłaszcza w przypadku najbardziej innowacyjnych produktów, gdy zawarta w produkcie wiedza techniczna ma niemal przełomowy charakter (jest w związku z tym bardzo złożona i początkowo trudna do przejęcia), a potencjalne zyski z tytułu monopolu pełnego są bardzo pokaźne, pojawia się *konflikt zawłaszczalności* między publicznym charakterem wiedzy technicznej a kształtowaniem się zysków firmy-innowatora. Z tego też powodu bardziej opłacalna jest internalizacja wiedzy zawartej w innowacyjnych produktach niż jej wykorzystanie poprzez rynek (tzn. drogą transakcji zewnętrznych)[41].

Zaprezentowane wyżej teorie stanowią pewien zestaw koncepcji, zdaniem autora niniejszego opracowania, ważnych z punktu widzenia teoretycznie uzasadnienia zjawiska BIZ. Siłą rzeczy jednak ich wybór – poza tym, że stosunkowo skromny

---

37 Misala J., op. cit., s. 221-222.

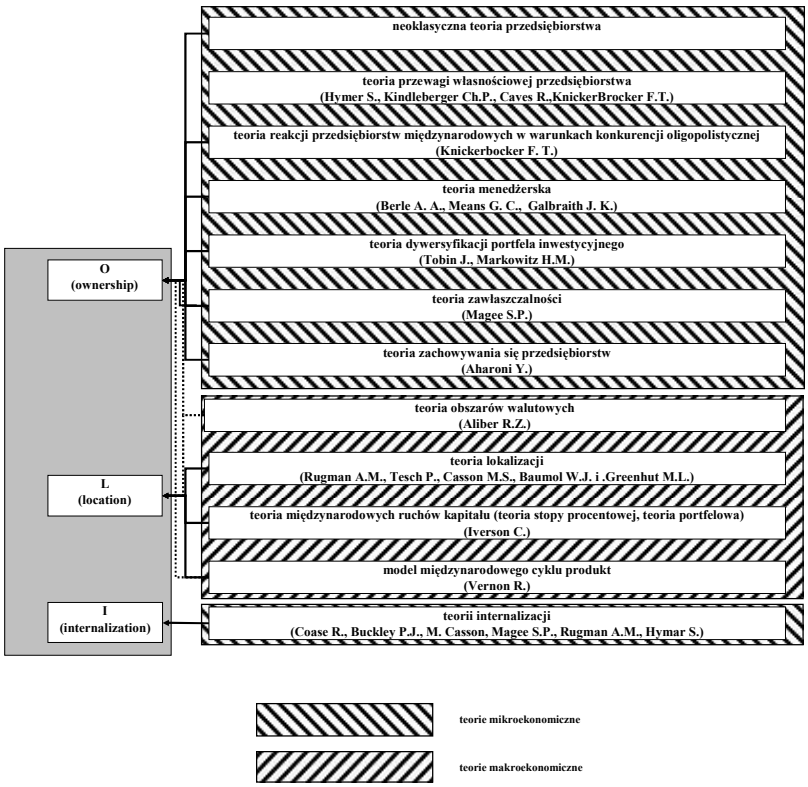
38 Aharoni Y., *The Foreign Investment Decision Process*, Plasting-Stoke Press, Boston 1966; cyt. za Misala J., op. cit., s. 220.

39 Tamże, s. 220.

40 Magee S.P., The Appriorability Theory of the Multinationals Corporation, „The Annals of the American Academy of AAPSS", 1977, No 458; cyt. za Misala J., op. cit. s. 224.

41 Misala J., op. cit., s. 224.

w swym zasięgu – obarczony jest subiektywizmem jego przekonań i doświadczeń. Dość powiedzieć, że jednak prezentacja powyższa, jak i ta zawarta w części pierwszej cyklu poświęconego teoriopoznawczym aspektom BIZ, stwarza możliwość syntezy całych dotychczasowych rozważań. Niech przyjmie ona postać ilustracji graficznej, na której – jak już to na wstępie niniejszego artykułu zasygnalizowano – dokonamy rozszerzenia modelu OLI, polegającego na przypisaniu poszczególnym przewagom zaprezentowanych jednoczynnikowych hipotez dotyczących BIZ.



Rys. 2. Model OLI a hipotezy dotyczące BIZ – perspektywa historyczna
Zródło: Opracowanie własne

Zgodnie z ideą schematu zaprezentowanego na rys. nr 2 model OLI rzeczywiście jest wypadkową – jak to wcześniej określono – teorią mieszaną, szeroko uwzględniającą historyczny dorobek rozważań poświęconych niezwykle ciekawemu i jakże będącemu „na czasie" zjawisku BIZ. Wykorzystana w prezentacji klasyfikacja hipotez, dzieląca ja na te o proweniencji mikro- i makroekonomicznej pokazuje, że zdecydowanie większa część teorii BIZ czerpie z dorobku mikroekonomicznej teorii przedsiębiorstwa konkurencji niedoskonałej i koncepcji doń zbliżonych (np. teoria menedżerska firmy). Zwraca uwagę, że z przewagą lokalizacji

powiązane są dwie koncepcje, które, będąc zaliczone do teorii makroekonomicznych, traktowane są zarazem jako kolejne wyjaśnienia źródeł przewagi własnościowej (tu w większości mamy do czynienia z modelami mikroekonomicznymi). Chodzi o teorię obszarów walutowych oraz model R. Vernona (międzynarodowego cyklu produktu). To może budzić pewne wątpliwości. A jednak w istocie – stanowi to treść pierwszej z koncepcji (teorii obszarów walutowych) – trudno nie zgodzić się z przesłaniem hipotezy, że motywem podjęcia BIZ przez WKT jest tzw. premia walutowa, zawłaszczana przez inwestującą WKT wskutek istnienia oddzielnych terenów walutowych i wynikającego stąd ryzyka zmiany kursu walut; to wszakże ma związek z dysponowaniem przez WKT unikalnym zasobem, jakim jest po prostu zarząd firmy, czyli jej personel o najwyższych kwalifikacjach, zdolny do podjęcia wyważonego ryzyka w aspekcie BIZ. Jednak makroekonomiczny charakter modelu nie budzi zastrzeżeń – przedmiotem bowiem jego zainteresowania była gospodarka światowa. Z kolei w modelu Vernona wiadomym jest, że produkt zaczyna swoje międzynarodowe „życie", ponieważ wynika to z faktu wiodącej roli firmy w dziedzinie innowacji i nowoczesnych technologii. Zatem z czegoś, co trudno byłoby nie uznać za element przewagi własnościowej. Z drugiej strony jednak model ten jest jedną z postaci tzw. *teorii neotechnologicznych*, które wyewoluowały z tradycyjnego modelu handlu międzynarodowego H-O-S, stricte koncepcji makroekonomicznej[42].

Podsumowanie

Niniejszy artykuł stanowi prezentację wybranych hipotez i modeli, w literaturze przedmiotu często określanych mianem teorii jednoczynnikowych, skupiających swoją uwagę na wybranych zjawiskach i procesach związanych z bezpośrednimi inwestycjami zagranicznymi. Koncepcje te legły u podstaw sformułowanej przez J.H. Dunning`a tzw. eklektycznej teorii produkcji międzynarodowej, stanowiąc fundament dla rozważań tego autora na temat istoty i doniosłości postulowanych przezeń przewag konkurencyjnych jako zasadniczych przesłanek podejmowania bezpośrednich inwestycji zagranicznych. Dzięki nim, oraz twórczo integrującego je w kompletną teorię podejścia J.H. Dunning`a, możliwe było holistyczne spojrzenie na kwestię przyczyn, ale też i skutków, jakie bezpośrednie inwestycje zagraniczne rodziły i nadal rodzą dla gospodarki światowej.

Bibliografia

1. Aharoni Y., *The Foreign Investment Decision Process*, Plasting-Stoke Press, Boston 1966.
2. Aliber, R., *Teoria bezpośrednich inwestycji zagranicznych*, [w:] Kindleberger, C.P., red., *The International Corporation: A Symposium*, wydanie 5, MIT Press, Cambridge, MA, 17-34, 1970.

[42] L. Tarasiński, op. cit., s. 21.

3. Berle A.A., Means G.C., *The Modern Corporation and Private Property*, N.Y., 1968 (I wyd. 1932).
4. *Bezpośrednie inwestycje zagraniczne na świecie i w Polsce: tendencje, determinanty i wpływ na gospodarkę*, raport UNCTAD i Ministerstwa Gospodarki RP, Warszawa 2002.
5. *Bilans płatniczy na bazie transakcji oraz Bilans aktywów pasywów Rzeczypospolitej Polskiej*, Narodowy Bank Polski, Warszawa, wrzesień 2003.
6. Bożyk P., Misala J., Puławski M., *Międzynarodowe stosunki ekonomiczne*, PWE Warszawa 1998.
7. Budnikowski A., Kawecka Wyrzykowska E., *Międzynarodowe stosunki gospodarcze*, praca zbiorowa, PWE, Warszawa 1999.
8. Budnikowski A., Kawecka-Wyrzykowska E., *Międzynarodowe stosunki gospodarcze*, PWE Warszawa 1999.
9. Caves R.E., *International Corporations: The Industrial Economics of Foreign Investment*, „Economica", Vol. XXXVIII, No. 149, February 1971.
10. Cyrson E., *Korporacje wielonarodowe Prawidłowości ekspansji zagranicznej*, PWN Warszawa 1981.
11. Domańska E., *Kapitalizm menedżerski*, PWE, Warszawa 1986.
12. Dunning J.H., *Studies in International Investment*, London 1970.
13. Galbraith J.K., *The New Industrial State*, London 1967.
14. Geldner M., *Przyczynek do teorii zagranicznych inwestycji bezpośrednich*, MiO nr 193, SGPiS, Warszawa 1986.
15. Górski J., *Przemiany we współczesnej ekonomii burżuazyjnej*, praca zbiorowa, PWE, Warszawa 1987.
16. Iverson C., *Some Aspects of the Theory of International Capital Movements*, London 1936.
17. Johnson H., *Survey of Issues*, Peter Drysdale ed., „Direct Foreign Investment in Asia and Pacific", Australian National University Press, Canberra, 1972.
18. Kojima K., *International Trade and Foreign Investment: Substitutes or Complements*, Hitotsubashi Academy 1975.
19. Krugman P.R., Obstfeld M., *Międzynarodowe stosunki gospodarcze*, Tom 1, PWN, Warszawa 1997.
20. Magee S.P., *The Appriorability Theory of the Multinationals Corporation*, „The Annals of the American Academy of AAPSS", 1977, No 458.
21. Misala J., *Współczesne teorie wymiany międzynarodowej i zagranicznej polityki ekonomicznej*, SGH Kolegium Gospodarki Światowej (wydruk komputerowy powielony), Warszawa 2000
22. Misala J., *Współczesne teorie wymiany międzynarodowej i zagranicznej polityki ekonomicznej*, SGH, Warszawa 2001.
23. Ozwa T., *Foreign direct investment and economic development*, Transnational Corporation, February 1992, vol. 1, No. 1.
24. Porter M., *Strategia konkurencji*, PWE, Warszawa 1994.
25. Rutkowski J., *Eksport kapitału*, PWN Warszawa 1972.

26. Rutkowski J., *Światowe strumienie kapitałowe, rozprawy i studia*, t. (CC)126, Uniwersytet Szczeciński, Szczecin 1992.
27. Tarasiński L., *Międzynarodowa wymiana gospodarcza i konkurencyjność czynnikami gospodarczej restrukturyzacji i wzrostu dobrobytu. Implikacje dla Polski*, w: *Gospodarka XXI wieku. Wyzwania rozwojowe*, pr. zbiorowa pod red. Lament M., Bukowska J., CedeWu, Warszawa 2021.
28. Witkowska J., *Bezpośrednie inwestycje zagraniczne w warunkach stowarzyszenia i przyszłego członkostwa w WE*, [w:] *Biała Księga. Polska-Unia Europejska*, Wydawnictwo URM Biura ds. Integracji Europejskiej oraz Pomocy Zagranicznej.
29. Yip G.S., *Strategia globalna*, PWE, Warszawa 1996.
30. Zorska A., *Ku globalizacji? Przemiany w korporacjach transnarodowych i w gospodarce światowej*, Wydawnictwo Naukowe PWN, Warszawa 1998.

REASONS FOR FOREIGN DIRECT INVESTMENT IN THE LIGHT OF SELECTED SINGLE-FACTOR THEORIES

Abstract

This article presents selected hypotheses and models, often referred to in the literature as single-factor theories, focusing on selected phenomena and processes related to foreign direct investment. These concepts underpin J.H. Dunning's so-called eclectic theory of international production, providing the foundation for his reflections on the nature and importance of the competitive advantages he postulated as fundamental premises for foreign direct investment. These concepts, combined with Dunning's creatively integrated approach into a comprehensive theory, provide a holistic perspective on the causes and consequences of foreign direct investment for the global economy.

Keywords: globalization, foreign direct investment.

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.018

Małgorzata Szczęk[1]

ROZWÓJ RYNKÓW UBEZPIECZENIOWYCH W KRAJACH EUROPY PÓŁNOCNEJ I POŁUDNIOWEJ

Streszczenie

Celem artykułu jest przeanalizowanie oraz porównanie poziomu rozwoju rynków ubezpieczeniowych w krajach Europy Północnej i Południowej, ze szczególnym uwzględnieniem czynników ekonomicznych, społecznych i instytucjonalnych wpływających na te różnice, a także wskazanie kluczowych barier oraz potencjału rozwojowego w obu regionach. Analizą objęto Szwecję, Finlandię i Norwegię oraz Włochy, Maltę i Grecję. W badaniu wykorzystano wskaźniki rozwoju rynku ubezpieczeniowego. Wyniki analizy wskazują na istotne różnice pomiędzy badanymi regionami, potwierdzając wyższy poziom rozwoju rynków ubezpieczeniowych w krajach Europy Północnej.

Słowa kluczowe: rynek ubezpieczeniowy; penetracja ubezpieczeniowa; gęstość ubezpieczeniowa; Europa Północna; Europa Południowa; sektor finansowy.

Wstęp

Współczesny rynek ubezpieczeniowy stanowi istotny filar gospodarki, odgrywając kluczową rolę w zarządzaniu ryzykiem, ochronie majątku oraz zapewnianiu stabilności finansowej obywatelom i przedsiębiorstwom. Europa, mimo wspólnego rynku i zbliżonych norm prawnych, charakteryzuje się znacznym zróżnicowaniem w zakresie rozwoju sektora ubezpieczeń. W niniejszym artykule porównano rynki ubezpieczeniowe w wybranych krajach Europy Północnej – znanych z wysokiego poziomu rozwoju ubezpieczeń społecznych i prywatnych – i państwach Europy Południowej, gdzie rynek ubezpieczeniowy rozwija się w odmiennym tempie i pod wpływem innych czynników kulturowych, ekonomicznych oraz społecznych.

[1] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, Finanse i Rachunkowość, II stopień.

Kontrast pomiędzy tymi częściami Europy rzadko jest przedmiotem analiz empirycznych, dlatego warto zbadać powyższe zagadnienie. Do analizy wybrano kraje położone na krańcach Europy – Szwecję, Finlandię i Norwegię na północy oraz Włochy, Maltę i Grecję na południu.

Głównym problemem badawczym podejmowanym w artykule jest określenie, jakie są różnice w rozwoju rynków ubezpieczeniowych w krajach Europy Północnej i Południowej oraz jakie czynniki determinują te rozbieżności. Artykuł opiera się na hipotezie, że rynki ubezpieczeniowe w krajach Europy Północnej charakteryzują się wyższym stopniem rozwoju, większym poziomem penetracji ubezpieczeń oraz silniejszą regulacją instytucjonalną w porównaniu do rynków Europy Południowej, co wynika głównie z różnic w poziomie rozwoju gospodarczego, stabilności systemów finansowych oraz świadomości ubezpieczeniowej społeczeństw.

Artykuł składa się z części teoretycznej, w której przedstawiono istotę rynku ubezpieczeniowego oraz podstawowe wskaźniki jego rozwoju, części analitycznej obejmującej porównanie rynków ubezpieczeniowych wybranych krajów Europy Północnej i Południowej na podstawie danych empirycznych, a także części końcowej zawierającej identyfikację czynników różnicujących rozwój rynków oraz wnioski z przeprowadzonej analizy.

1. Charakterystyka rynków ubezpieczeniowych

Rynek ubezpieczeniowy odgrywa istotną rolę w gospodarce, zapewniając ochronę przed różnego rodzaju ryzykiem oraz wspierając stabilność finansową społeczeństw. Dla zrozumienia jego znaczenia i funkcjonowania konieczne jest poznanie definicji, podstawowych funkcji oraz kluczowych wskaźników jego rozwoju. W rozdziale omówione zostaną również główne typy ubezpieczeń.

1.1. Definicja i funkcje rynku ubezpieczeniowego

Poprzez rynek ubezpieczeniowy rozumiana jest przestrzeń, w której działają firmy ubezpieczeniowe oraz ich klienci, zawierający umowy ubezpieczenia w celu zarządzania ryzykiem. Jest to część rynku finansowego, w ramach której ubezpieczyciele oferują ochronę przed nieprzewidzianymi zdarzeniami w zamian za składki ubezpieczeniowe[2].

W ramach swojego działania rynek ubezpieczeniowy pełni trzy podstawowe funkcje: ochronną, prewencyjną oraz finansową. Funkcja ochronna ma największe znaczenie – polega na zabezpieczeniu finansowym (poprzez wypłatę świadczeń) osób fizycznych i prawnych przed negatywnymi skutkami zdarzeń losowych, takich jak wypadki, choroby, szkody w mieniu czy utrata życia. Funkcja prewencyjna polega na podejmowaniu działań mających na celu uniknięcie lub zminimalizowanie ryzyka. Ubezpieczyciele często oferują niższe składki lub inne korzyści dla osób i podmiotów, które podejmują działania prewencyjne, np. instalują systemy alarmowe, regularnie przeprowadzają przeglądy techniczne pojazdów, czy dbają

[2] W. Ronka-Chmielowiec, *Ubezpieczenia*, Wydawnictwo C.H. Beck, 2016, s. 75.

o zdrowie. Rolą funkcji finansowej jest gromadzenie i przekazywanie środków finansowych w celu pokrycia strat wynikających z ubezpieczonych zdarzeń. Rynek ubezpieczeniowy tworzy ze składek od ubezpieczonych fundusze, które są wykorzystywane do wypłaty odszkodowań i świadczeń. To umożliwia redystrybuowanie ryzyka i kosztów związanych ze zdarzeniami losowymi, co pozytywnie wpływa na stabilność finansową osób i podmiotów.

1.2. Wskaźniki rozwoju rynku ubezpieczeniowego

Rozwój rynku ubezpieczeniowego znajduje odzwierciedlenie przede wszystkim w poszerzaniu oferty produktowej, większej dostępności ubezpieczeń dla klientów indywidualnych i instytucjonalnych, a także w systematycznym wzroście wartości składek gromadzonych przez zakłady ubezpieczeń. Świadczy to o rosnącym znaczeniu tego sektora w gospodarce oraz o wzmacniającej się świadomości ubezpieczeniowej społeczeństwa[3].

W celu zmierzenia stopnia rozwoju rynku ubezpieczeniowego w danym państwie, stosuje się trzy podstawowe wskaźniki[4]. Pierwszym z nich jest wartość składek przypisanych brutto z ubezpieczeń bezpośrednich wraz z analizą ich dynamiki, co pozwala ocenić tempo wzrostu sektora. Drugim wskaźnikiem jest gęstość ubezpieczeniowa, czyli wartość składek przypadająca na jednego mieszkańca, wskazująca na indywidualne zaangażowanie społeczeństwa w korzystanie z ubezpieczeń. Trzecią miarą jest wskaźnik penetracji ubezpieczeniowej, wyrażający stosunek składek do produktu krajowego brutto, który obrazuje udział sektora ubezpieczeniowego w gospodarce narodowej. Wymienione wskaźniki zostaną wykorzystane w późniejszej analizie rynków ubezpieczeniowych w wybranych krajach.

1.3. Główne typy ubezpieczeń

Ubezpieczenia klasyfikowane są m. in. ze względu na ich rodzaj. Jest to główny podział, według którego wyróżniamy: ubezpieczenia gospodarcze, ubezpieczenia zdrowotne i ubezpieczenia społeczne.

Ubezpieczenia gospodarcze dotyczą utraty mienia, zdrowia lub życia. Dzielą się na ubezpieczenia majątkowe oraz ubezpieczenia osobowe. W pierwszej z tych grup ubezpieczeń wyróżnia się ubezpieczenia rzeczowe (np. CASCO pojazdów, ubezpieczenie środków w transporcie, ubezpieczenie szkód rzeczowych spowodowanych

---

[3] Szerzej na temat czynników rozwoju rynku ubezpieczeniowego zob. M. Lament, S. Bukowski, *Wybrane determinanty rozwoju rynków ubezpieczeniowych krajów Unii Europejskiej w latach 1999-2019,* „Wiadomości Ubezpieczeniowe", 2022, 4, s. 61-74, S. Bukowski, M. Lament, *Impact of foreign capital on the insurance market development in the Visegrad Group countries*, „Journal of Management and Financial Sciences", 2019, 38, s. 33-45.

[4] T.H. Bednarczyk, *Ekonomiczne i instytucjonalne czynniki rozwoju ubezpieczeń*, „Wiadomości Ubezpieczeniowe", 2011, nr 4, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, s. 86, 87.

żywiołami) oraz ubezpieczenia majątkowe w ścisłym znaczeniu (ubezpieczenia ochrony prawnej). Ubezpieczenia osobowe dzielą się na życiowe, wypadkowe (tzw. następstw nieszczęśliwych wypadków) i chorobowe.

Kolejnym rodzaj to ubezpieczenie zdrowotne, dotyczące ryzyka utraty zdrowia lub życia. Jest ono oferowane przez NFZ, a jego posiadanie jest obowiązkowe. Oznacza to, że bezwzględnie podlegają mu pracownicy, osoby prowadzące działalność gospodarczą, osoby na umowach cywilnoprawnych, studenci i doktoranci, emeryci i renciści oraz osoby bezrobotne zarejestrowane w urzędzie pracy. Osoby nienależące do żadnej z wymienionych grup mogą być zgłoszone jako członkowie rodziny osoby ubezpieczonej[5].

Ubezpieczenie społeczne jest systemem świadczeń zapewniających pracownikom i ich rodzinom pomoc z publicznych funduszy składkowych w razie choroby, niezdolności do pracy, starości lub śmierci[6]. Przedmiotem tego ubezpieczenia objęty jest niezawiniony brak dochodu, powstały na skutek zdarzeń losowych, takich jak choroba, niezdolność do pracy, starość czy śmierć, lub też sytuacji rodzinnych, które nie mają charakteru losowego (np. urodzenie dziecka, opieka nad dzieckiem). Do ubezpieczeń społecznych zaliczane są: ubezpieczenia rentowe (mające charakter obowiązkowy), ubezpieczenia chorobowe (obowiązkowe i dobrowolne), ubezpieczenia emerytalne (obowiązkowe i dobrowolne) oraz ubezpieczenia wypadkowe (obowiązkowe)[7].

2. Europa Północna – profil rynku ubezpieczeniowego w wybranych krajach

Kraje Europy Północnej, takie jak Szwecja, Finlandia i Norwegia, należą do najbardziej rozwiniętych gospodarek nie tylko w Europie, ale i na świecie. Wysoki poziom dochodu narodowego, silne instytucje publiczne oraz powszechne zaufanie społeczne tworzą sprzyjające warunki dla dynamicznego rozwoju sektora ubezpieczeniowego. Charakterystyczne dla tych państw są również nowoczesne rozwiązania technologiczne, zaawansowana digitalizacja usług finansowych oraz rozbudowany system regulacji, które wspierają bezpieczeństwo i efektywność rynku.

Szwecja, Finlandia i Norwegia to jedne z najbardziej rozwiniętych krajów w Europie. Ubezpieczenia są tam powszechnie obecne w życiu społecznym, a ich funkcjonowanie ściśle powiązane jest z szerokimi systemami zabezpieczenia społecznego i silną obecnością państwa w sektorze usług publicznych. Rynek ubezpieczeń w Szwecji jest jednym z największych w krajach nordyckich. Znaczącą rolę odgrywają tam ubezpieczenia na życie, przewyższając średnią dla krajów europejskich[8].

[5] R. Garbiec, *Ubezpieczenia w teorii i praktyce*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2022, s. 10-12.
[6] *Encyklopedia popularna PWN*, Warszawa 1982, s. 815.
[7] R. Garbiec, *Ubezpieczenia w teorii…*, op. cit., s. 15-16.
[8] SAMPO GROUP, *The Swedish P&C insurance market*, „P&C insurance markets by country", 2025.

Ponadto, Szwecja jest największym rynkiem ubezpieczeń majątkowych i osobowych w krajach Europy Północnej. Posiada zarówno państwowy system ubezpieczeń społecznych, jak i prywatne firmy ubezpieczeniowe. Od 2011 roku w Szwecji obowiązuje system zabezpieczenia społecznego oparty na dwóch filarach: ubezpieczeniu rezydencyjnym, które przysługuje wszystkim osobom zamieszkującym na stałe w kraju i zapewnia gwarantowane świadczenia, oraz ubezpieczeniu uzależnionym od wysokości wynagrodzenia, które kompensuje utratę dochodów. System ten obejmuje zarówno mieszkańców Szwecji, jak i osoby pracujące na jej terytorium, niezależnie od obywatelstwa – posiadanie szwedzkiego paszportu nie jest wymagane, by podlegać ubezpieczeniu. Nadzór nad szwedzkim systemem zabezpieczenia społecznego, z wyjątkiem ubezpieczenia na wypadek bezrobocia, sprawuje Ministerstwo Zdrowia i Spraw Społecznych. Za jego realizację odpowiada przede wszystkim Szwedzka Agencja Ubezpieczeń Społecznych, która administruje większością świadczeń, poza emeryturami i rentami rodzinnymi. Te ostatnie są zarządzane przez Szwedzką Agencję ds. Emerytur. Zakres podstawowego ubezpieczenia obejmuje: ubezpieczenie chorobowe, rodzicielskie, emerytalne, renty rodzinne, odszkodowanie chorobowe, odszkodowanie z tytułu ograniczenia aktywności oraz z tytułu wypadku przy pracy i/lub chorób zawodowych[9].

Finlandzki rynek ubezpieczeniowy charakteryzuje się wysokim stopniem regulacji i szeroką ofertą, obejmującą zarówno ubezpieczenia społeczne, jak i prywatne. Finlandia posiada rozbudowany system ubezpieczeń społecznych, do których należą m.in. ubezpieczenia emerytalne, wypadkowe i zdrowotne. Istnieje tam również szeroki wybór prywatnych firm ubezpieczeniowych, oferujących różnorodne produkty i pakiety. System zabezpieczenia społecznego w Finlandii funkcjonuje w ramach nordyckiego modelu opieki, który gwarantuje każdemu mieszkańcowi kraju prawo do podstawowych świadczeń zapewniających minimalny dochód. Główne obszary objęte tym systemem to ochrona przed skutkami starzenia się, utraty zdolności do pracy, śmierci żywiciela rodziny, choroby, bezrobocia oraz z tytułu macierzyństwa i opieki nad dziećmi. System ten obejmuje wszystkich mieszkańców Finlandii i zapewnia im dostęp do emerytur podstawowych, świadczeń chorobowych, macierzyńskich oraz zasiłków rodzinnych. Osoby zatrudnione dodatkowo korzystają z przywilejów wynikających z zatrudnienia, takich jak emerytury pracownicze czy świadczenia z tytułu wypadków przy pracy. Ponadto, każdy mieszkaniec danej gminy ma zagwarantowany dostęp do publicznej opieki zdrowotnej i usług pomocy społecznej. Za organizację i nadzór nad fińskim systemem zabezpieczenia społecznego odpowiada Ministerstwo Spraw Społecznych i Zdrowia[10].

Rynek ubezpieczeń w Norwegii również cechuje się wysokim stopniem rozwoju i obejmuje zarówno sektor publiczny, jak i sektor prywatny. W kraju funkcjonuje powszechny system opieki zdrowotnej oraz państwowy system zabezpieczenia społecznego, który gwarantuje świadczenia w przypadku choroby, wypadków czy

[9] K. Szyszko-Głowacka, *Jak ubezpieczają się w Unii – Szwecja*, ZUS, 2016, s. 1.
[10] Ibidem.

emerytury. W kraju działa wiele prywatnych towarzystw ubezpieczeniowych, oferujących różnorodne produkty, w tym ubezpieczenia komunikacyjne, majątkowe, na życie oraz pakiety skierowane do przedsiębiorstw i ich pracowników. Wypłacaniem świadczeń społecznych, z wyjątkiem opieki zdrowotnej, zarządza Publiczny Urząd Pracy i Zabezpieczenia Społecznego, który podlega Dyrekcji Pracy i Zabezpieczenia Społecznego. Urząd ten zajmuje się również wypłacaniem świadczeń na rzecz dzieci. System ubezpieczeń społecznych w Norwegii jest finansowany zarówno ze składek ubezpieczeniowych, które odprowadzają pracodawcy oraz osoby ubezpieczone, jak i z wpływów podatkowych. W przypadku pracowników najemnych i osób prowadzących działalność gospodarczą, wysokość składek ustalana jest w oparciu o ich dochód brutto. System pomocy społecznej w pełni pokrywany jest ze środków pochodzących z podatków[11].

3. Europa Południowa – profil rynku ubezpieczeniowego w wybranych krajach

Kraje Europy Południowej wybrane do analizy pod kątem rozwoju rynków ubezpieczeniowych, to Włochy, Malta i Grecja. Różnią się one od rynków Europy Północnej pod względem struktury, poziomu rozwoju oraz funkcjonowania. Pomimo członkostwa w Unii Europejskiej oraz wdrażania wspólnych regulacji nadzorczych, region ten nadal zmaga się z pewnymi wyzwaniami ograniczającymi pełny rozwój sektora ubezpieczeniowego.

Włoski rynek ubezpieczeniowy jest największym wśród państw południowoeuropejskich. Dominującą pozycję mają ubezpieczenia na życie, szczególnie związane z produktami oszczędnościowymi i inwestycyjnymi. We Włoszech problematyką ubezpieczeń społecznych i ubezpieczeń z tytułu inwalidztwa i wypadków przy pracy zajmują się głównie INPS (Istituto Nazionale della Previdenza Sociale, odpowiednik polskiego ZUS) i INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortunni sul Lavoro, Krajowy Zakład Ubezpieczeń z Tytułu Wypadków przy Pracy). INPS stwierdza i ustala obowiązek ubezpieczeń, ustala uprawnienia do świadczeń i nalicza ich wysokość. Odnosi się to do świadczeń z tytułu ubezpieczeń społecznych oraz z tytułu opieki zdrowotnej. Ubezpieczenie w INPS i w INAIL jest obowiązkowe. Wypłaty dokonywane przez INAIL obejmują m. in. wypadki przy pracy, utratę zdrowia, inwalidztwo czy rehabilitację. INPS jest głównym organem ubezpieczającym pracowników, jednak istnieją również instytucje prowadzące obowiązkowe ubezpieczenia pracowników poszczególnych branż lub zawodów. Część świadczeń społecznych jest wypłacana przez władze gminy, w której ubezpieczony jest zameldowany[12]. Mimo rozbudowanego sektora ubezpieczeń, we Włoszech występuje luka ubezpieczeniowa. Od lat kraj mierzy się przede wszystkim z kryzysem klimatycznym. Według danych Europejskiego Banku Centralnego, w latach 1980-2020 tylko 5% strat spowodowanych przez katastrofy klimatyczne było ubezpieczone, podczas

[11] Komisja Europejska, *Twoje uprawnienia do zabezpieczenia społecznego w Norwegii,* 2012, s. 4-6.

[12] K. Szyszko-Głowacka, *Jak ubezpieczają się w Unii – Włochy*, ZUS, 2018, s. 1, 2.

gdy średnia europejska to 27%. Odszkodowania z tytułu trzęsień ziemi, osunięć czy powodzi wynoszą miliardy euro i stanowią duże obciążenie dla finansów Włoch, uszczuplając fundusze na inne potrzeby. Włoskie społeczeństwo obwinia firmy ubezpieczeniowe o wypłaty, które nie są warte składek. Niewielu Włochów nabywa ochronę, a najczęściej decydują się na ubezpieczenie dopiero w sytuacji wysokiego ryzyka. Wskutek tego tworzy się błędne koło mniejszych przychodów i większego ryzyka dla ubezpieczycieli, zmuszając ich do podnoszenia składek, co z kolei zniechęca innych do ubezpieczania się[13].

Malta jest niewielkim krajem, jednak odgrywa ważną rolę jako centrum usług finansowych i ubezpieczeniowych. Dzięki korzystnemu otoczeniu regulacyjnemu i podatkowemu, wiele międzynarodowych firm rejestruje tam swoje oddziały. Rynek lokalny pozostaje ograniczony pod względem liczby klientów, ale cechuje się wysoką aktywnością w obszarze reasekuracji i działalności transgranicznej. System zabezpieczenia społecznego na Malcie obejmuje: ubezpieczenie rentowe, emerytalne, w razie choroby i macierzyństwa, z tytułu chorób zawodowych i wypadków przy pracy oraz świadczenie dla bezrobotnych. W kraju istnieją dwa podstawowe systemy zabezpieczenia społecznego – system nieskładkowy i składkowy. Aby uzyskać uprawnienia w ramach pierwszego systemu, należy spełnić warunki związane z oceną zasobów finansowych, a w przypadku drugiego systemu – warunki składkowe. Składki obowiązkowe obejmują ryzyko związane ze starością, śmiercią, inwalidztwem, wypadkiem przy pracy i chorobą zawodową, a także świadczenia emerytalno-rentowe i uzupełniające. Obejmują również zasiłek na dzieci, pomoc społeczną i usługi świadczone w ramach systemu opieki zdrowotnej. Instytucją zarządzającą świadczeniami pieniężnymi jest Zakład Zabezpieczenia Społecznego obejmujący centralny urząd w Valletcie – stolicy kraju – oraz 24 biura okręgowe. Do zadań Zakładu Zabezpieczenia Społecznego należy przyznawanie zasiłków oraz udzielanie porad i informacji związanych z ubezpieczeniem społecznym. Ponadto instytucja zapewnia zasiłki składkowe, zasiłki nieskładkowe oraz opiekę nad klientem i współpracę międzynarodową. Zakład Zabezpieczenia Społecznego jest nadzorowany przez Ministerstwo Rodziny i Solidarności Społecznej. Świadczeniem usług opieki zdrowotnej i realizowaniem mechanizmu monitorowania i kontroli, a także promowaniem działań przyczyniających się do dobrego samopoczucia osób starszych i rozwoju opieki środowiskowej, zajmuje się Ministerstwo Energetyki i Ochrony Zdrowia[14]. Pomimo stabilnego otoczenia regulacyjnego i dużej liczby zarejestrowanych podmiotów działających transgranicznie, rozwój rynku ubezpieczeniowego na Malcie napotyka na kilka istotnych ograniczeń. Przede wszystkim, niewielki rozmiar lokalnego rynku i ograniczona liczba mieszkańców wpływają na niski wolumen składek krajowych i ograniczoną dywersyfikację oferty. Ponadto, niska

[13] „Gazeta Ubezpieczeniowa", *Włochy: Luka ubezpieczeniowa pochłania finanse państwa*, 2023.

[14] K. Szyszko-Głowacka, *Jak ubezpieczają się w Unii – Malta*, ZUS, 2018, s. 1, 2.

świadomość ubezpieczeniowa społeczeństwa oraz silna koncentracja na kilku rodzajach produktów, głównie obowiązkowych, takich jak OC komunikacyjne, ograniczają potencjał rozwoju segmentów dobrowolnych, np. ubezpieczeń zdrowotnych czy majątkowych. Wyzwaniem pozostaje również rozwój cyfrowych kanałów dystrybucji, które mimo postępu, nadal nie osiągnęły poziomu obserwowanego w bardziej rozwiniętych krajach UE.

Grecki sektor ubezpieczeń przez długi czas pozostawał słabo rozwinięty, z dominacją ubezpieczeń obowiązkowych. Kryzys gospodarczy mający początek w 2008 roku poważnie osłabił kondycję finansową ubezpieczycieli i spowodował spadek zaufania społecznego. Pomimo poprawy sytuacji makroekonomicznej, grecki rynek nadal cechuje się niskim poziomem penetracji ubezpieczeń i ograniczoną świadomością ubezpieczeniową. Obowiązkowe ubezpieczenie w Grecji obejmuje wszystkie osoby pracujące w tym kraju, bez względu na ich obywatelstwo. Od pierwszego dnia pracy mają one zapewnioną opiekę wszelkiego rodzaju, uprawnienia do świadczeń emerytalnych oraz innych świadczeń – m. in. z tytułu macierzyństwa, ciąży, bezrobocia. W Grecji istnieje wiele instytucji zabezpieczenia społecznego dla poszczególnych grup zawodowych, posiadających zróżnicowane uprawnienia, jednak głównymi instytucjami polityki społecznej są IKA-ETAM (Zakład Ubezpieczeń Społecznych) – największa instytucja ubezpieczeniowa, wypłacająca całość składek i świadczeń dla pracowników zatrudnionych na podstawie umowy o pracę – oraz OAED (Urząd ds. Zatrudnienia) – jednostka odpowiadająca za wypłatę zasiłków dla bezrobotnych i świadczeń rodzinnych dla wszystkich ubezpieczonych. Oprócz wspomnianych instytucji, w Grecji istnieją także fundusze ubezpieczeniowe dla specyficznych grup zatrudnionych, m. in. rolników, osób samozatrudnionych, przedstawicieli wolnych zawodów oraz urzędników administracji publicznej. Grecki system zabezpieczenia społecznego funkcjonuje w oparciu o model trójstronnego finansowania, w którym koszty pokrywają wspólnie pracownicy, pracodawcy oraz państwo. System ten jest dodatkowo wspierany przez roczne dotacje państwowe przeznaczone dla instytucji zabezpieczenia społecznego[15]. Jednakże, rozwój rynku ubezpieczeniowego w Grecji jest wciąż ograniczany przez szereg czynników o charakterze gospodarczym, społecznym i strukturalnym. Długotrwały kryzys finansowy, którego szczyt przypadał na lata 2008-2009, doprowadził do spadku dochodów gospodarstw domowych, wysokiego bezrobocia oraz utraty zaufania do instytucji finansowych, co przełożyło się na niski popyt na produkty ubezpieczeniowe[16]. Dodatkowo, niewielka świadomość ubezpieczeniowa społeczeństwa, dominacja ubezpieczeń obowiązkowych (głównie komunikacyjnych) oraz ograniczony rozwój ubezpieczeń dobrowolnych wpływają negatywnie na poziom penetracji ubezpieczeń. Bariery te potęgują również braki w infrastrukturze cyfrowej sektora oraz powolne tempo modernizacji usług ubezpieczeniowych.

[15] K. Szyszko-Głowacka, *Jak ubezpieczają się w Unii – Grecja*, ZUS, 2018, s. 1-3.

[16] Hist.pl, *Bankructwo Grecji – jak doszło do finansowego kryzysu?*, 2023. https://hist.pl/bankructwo-grecji-jak-doszlo-do-finansowego-kryzysu/ [dostęp: 15.12.2025].

4. Czynniki różnicujące rozwój rynków

Rozwój rynków ubezpieczeniowych w Europie Północnej i Południowej kształtowany jest przez szereg czynników ekonomicznych, instytucjonalnych i społecznych – takich jak poziom rozwoju gospodarczego, rola państwa, świadomość ubezpieczeniowa, stabilność finansowa oraz stopień innowacyjności sektora. Czynniki te mogą kształtować się w Finlandii, Szwecji i Norwegii inaczej, niż we Włoszech, w Grecji oraz na Malcie. W krajach północnych silne, sprawnie działające instytucje publiczne i nadzorcze wspierają rozwój sektora poprzez stabilne regulacje i nadzór. W południowej Europie słabsze struktury instytucjonalne i mniejsze wsparcie państwa ograniczają zaufanie i inwestycje w sektor ubezpieczeniowy. Kolejną różnicą jest to, że społeczeństwa północnoeuropejskie charakteryzują się wysokim poziomem świadomości finansowej i kultury samodzielnego zabezpieczania ryzyka, co przekłada się na większe zainteresowanie ubezpieczeniami. W krajach południowych nadal dominuje podejście oparte na oczekiwaniu wsparcia państwowego. Finlandia, Norwegia i Szwecja to kraje o stabilnej polityce fiskalnej i niskim poziomie zadłużenia, co zwiększa zaufanie do sektora finansowego. Z kolei w państwach Europy Południowej częste kryzysy zadłużeniowe, cięcia budżetowe i niestabilność makroekonomiczna negatywnie wpływają na sektor ubezpieczeń i skłonność społeczeństwa do długoterminowych zobowiązań. Ponadto, państwa skandynawskie są liderami w zakresie cyfryzacji usług finansowych, co przekłada się na większą efektywność i dostępność ubezpieczeń. W krajach południowych proces cyfryzacji przebiega wolniej, co stanowi barierę zwłaszcza dla młodszych grup odbiorców[17].

Choć oba regiony działają w ramach wspólnych regulacji unijnych, różnią się skalą rozwoju, stopniem innowacyjności oraz strukturą popytu na usługi ubezpieczeniowe. Podczas gdy w Europie Północnej ubezpieczenia są integralną częścią modelu społeczno-gospodarczego, w krajach południowych pełnią one bardziej ograniczoną funkcję. W celu zbadania różnic w rynkach ubezpieczeniowych wybranych krajów, należy przyjrzeć się wskaźnikom, takim jak: wskaźnik PKB, wartość składek przypisanych brutto z ubezpieczeń bezpośrednich, wskaźnik penetracji ubezpieczeniowej oraz gęstość ubezpieczeniowa.

Tabela 1. Wskaźnik PKB w krajach Europy Północnej w wybranych latach okresu 2015-2024

Wyszczególnienie	PKB w mld USD		
	2015	2020	2024
Finlandia	233,21	247,12	252,86
Szwecja	501,70	535,44	580,45
Norwegia	388,16	405	443,94

Źródło: *World Development Indicators*, The World Bank, https://databank.worldbank.org [dostęp: 15.12.2025]

[17] T.H. Bednarczyk, K. Bielawska, B. Jackowska, E. Wycinka, *Ekonomiczne i demograficzne uwarunkowania funkcjonowania i rozwoju ubezpieczeń*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2019, s. 83-86.

W ostatniej dekadzie wskaźnik PKB w Finlandii, Szwecji i Norwegii wzrastał, co przekłada się na ciągły rozwój gospodarczy tych krajów. Oznacza to, że rozwijał się każdy z sektorów w gospodarce, w tym sektor ubezpieczeniowy. Największe wartości PKB osiągało w Szwecji, co świadczy o największym stopniu rozwoju gospodarczego spośród wybranych państw Europy Północnej. Możliwe jest zatem, że spośród trzech analizowanych krajów, Szwecja posiada najlepiej rozwinięty rynek ubezpieczeniowy.

Tabela 2. Wskaźnik PKB w krajach Europy Południowej w wybranych latach okresu 2015-2024

Wyszczególnienie	PKB w mld USD		
	2015	2020	2024
Włochy	1845,43	1751,65	2029,01
Malta	11,34	14,38	19,22
Grecja	194,57	187,09	224,96

Źródło: *World Development Indicators*, The World Bank, https://databank.worldbank.org [dostęp: 15.12.2025]

Wybrane kraje Europy Południowej w latach 2015-2024 również charakteryzowały się wzrostem PKB, choć Włochy i Grecja odnotowały spadek wartości w 2020 roku. Był to efekt pandemii COVID-19, która wpłynęła w dużej mierze na sektor turystyczny, a kraje te są często wybieranymi kierunkami podróży. Z pewnością odbiło się to na zmniejszeniu popytu m. in. na polisy turystyczne, co w pewnym stopniu zahamowało rozwój włoskiego i greckiego rynku ubezpieczeniowego. Ponadto, wskaźnik PKB we Włoszech w latach 2015-2024 był wyjątkowo wysoki, a także o wiele wyższy, niż w krajach Europy Północnej. To świadczy o wysoko rozwiniętej gospodarce i może oznaczać, że spośród wybranych państw południa Włochy charakteryzują się najbardziej rozwiniętym rynkiem ubezpieczeniowym.

W poniższej tabeli ujęto wartość składek przypisanych brutto z ubezpieczeń bezpośrednich w krajach Europy Północnej, w ostatniej dekadzie. Ich wysokość w poszczególnych latach pozwala ocenić tempo rozwoju rynku ubezpieczeniowego.

Tabela 3. Wartość składek przypisanych brutto z ubezpieczeń bezpośrednich w krajach Europy Północnej w wybranych latach okresu 2015-2024

Wyszczególnienie	Wartość składek przypisanych brutto z ubezpieczeń bezpośrednich w mld EUR		
	2015	2020	2024
Finlandia	23,99	23,13	29,81
Szwecja	30,36	28,78	31,24
Norwegia	14,05	16,95	20,46

Źródło: Finance Finland, https://finanssiala.fi; OECD, https://oecd.org; Statista, https://statista.com [dostęp: 15.12.2025]

Rynki ubezpieczeniowe w każdym z krajów odnotowały wzrost składek przypisanych brutto w latach 2015-2024. W Finlandii i Szwecji wartości zmalały w roku 2020,

co było skutkiem kryzysu spowodowanego pandemią. Najmniejszy wzrost składek w badanej dekadzie wystąpił w Szwecji (niecały 1 mld) – najmniejsza dynamika zmian oznacza najwolniej rozwijający się rynek ubezpieczeniowy spośród wybranych krajów. Szwecja odznaczała się jednak najwyższą wartością składek już w 2015 roku – rynek ubezpieczeniowy w tym kraju był już wysoko rozwinięty. Finlandia i Norwegia charakteryzowały się podobnym wzrostem wysokości składek w latach 2015-2024, jednak w Norwegii był on wyższy. Ponadto, w 2020 roku również odnotowano wzrost, co czyni rynek tego kraju najszybciej rozwijającym się spośród wybranych, jednak z najniższą wysokością składek przypisanych brutto.

Tabela 4. Wartość składek przypisanych brutto z ubezpieczeń bezpośrednich w krajach Europy Południowej w wybranych latach okresu 2015-2024

Wyszczególnienie	Wartość składek przypisanych brutto z ubezpieczeń bezpośrednich w mld EUR		
	2015	2020	2024
Włochy	23,99	23,13	29,81
Malta	30,36	28,78	31,24
Grecja	14,05	16,95	20,46

Źródło: OECD, https://oecd.org; Statista, , https://statista.com [dostęp: 15.12.2025]

Dane przedstawione w tabeli 4 wskazują na zróżnicowany, lecz ogólnie rosnący poziom wartości składek przypisanych brutto w krajach Europy Południowej w latach 2015-2024. Największą skalą rynku ubezpieczeniowego charakteryzowały się Włochy, co wynika z wielkości gospodarki oraz dominacji ubezpieczeń na życie o charakterze oszczędnościowo-inwestycyjnym. Spadek wartości składek w 2020 roku był konsekwencją pandemii COVID-19, która ograniczyła popyt na produkty ubezpieczeniowe. Malta, mimo niewielkiego rynku krajowego, utrzymywała względnie stabilny poziom składek dzięki działalności transgranicznej sektora finansowego, natomiast Grecja odnotowała najniższe wartości, co potwierdza niski poziom rozwoju rynku i dominację ubezpieczeń obowiązkowych. Ogółem dynamika zmian wskazuje na stopniową odbudowę rynków południowoeuropejskich, jednak ich tempo wzrostu pozostaje niższe niż w krajach Europy Północnej.

Tabela 5 i tabela 6 zawierają dane dotyczące wskaźnika penetracji ubezpieczeniowej. Wskaźnik ten to relacja wartości składki przypisanej brutto (SPB) do produktu krajowego brutto (PKB), odzwierciedlająca znaczenie sektora ubezpieczeń w gospodarce.

Tabela 5. Wskaźnik penetracji ubezpieczeniowej w krajach Europy Północnej w latach 2015, 2020 i 2024 (%)

Wyszczególnienie	2015	2020	2024
Finlandia	9,8	10,3	10,9
Szwecja	10,5	10,8	11,2
Norwegia	7,6	8,1	8,4

Źródło: Opracowanie własne na podstawie danych OECD i Insurance Europe

Dane zawarte w tabeli 5 wskazują na wysoki i systematycznie rosnący poziom penetracji ubezpieczeniowej w krajach Europy Północnej w latach 2015-2024. Najwyższe wartości wskaźnika odnotowano w Szwecji, co potwierdza silną pozycję sektora ubezpieczeniowego w gospodarce oraz wysoką świadomość ubezpieczeniową społeczeństwa. Finlandia osiąga zbliżony poziom penetracji, natomiast Norwegia, mimo nieco niższych wartości, również charakteryzuje się stabilnym wzrostem. Wzrost wskaźników w okresie pandemii COVID-19 świadczy o dużej odporności rynków północnoeuropejskich na szoki gospodarcze.

Tabela 6. Wskaźnik penetracji ubezpieczeniowej w krajach Europy Południowej w latach 2015, 2020 i 2024 (%)

Wyszczególnienie	2015	2020	2024
Włochy	6,3	6,8	7,1
Malta	6,0	6,4	6,8
Grecja	1,9	2,2	2,4

Źródło: Opracowanie własne na podstawie danych OECD i Insurance Europe

Z analizy danych przedstawionych w tabeli 6 wynika, że kraje Europy Południowej charakteryzują się znacznie niższym poziomem penetracji ubezpieczeniowej w porównaniu z krajami północnymi. Najwyższe wartości wskaźnika odnotowano we Włoszech, co związane jest z dużą skalą rynku oraz istotnym udziałem ubezpieczeń na życie. Malta osiąga umiarkowany poziom penetracji, natomiast Grecja cechuje się najniższymi wartościami w całym badanym okresie. Pomimo stopniowego wzrostu wskaźników po 2020 roku, udział sektora ubezpieczeniowego w gospodarce krajów południowych pozostaje ograniczony.

Poniżej przedstawiono ostatni ważny wskaźnik – gęstość ubezpieczeniową, czyli stosunek kwoty składki przypisanej brutto do liczby mieszkańców. To jeden z podstawowych mierników popytu na ubezpieczenia wykorzystywanych w analizach porównawczych.

Tabela 7. Gęstość ubezpieczeniowa w wybranych krajach Europy w latach 2015, 2020 i 2024 (EUR na mieszkańca)

Wyszczególnienie	2015	2020	2024
Szwecja	4 300	4 800	5 200
Finlandia	3 900	4 200	4 600
Norwegia	3 200	3 600	3 900
Włochy	1 900	2 100	2 300
Malta	1 700	1 900	2 100
Grecja	900	1 000	1 100

Źródło: Opracowanie własne na podstawie danych Insurance Europe, OECD oraz Statista

Tabela 7 wyraźnie ukazuje znaczące różnice w poziomie gęstości ubezpieczeniowej pomiędzy krajami Europy Północnej i Południowej. W państwach północnych składka przypadająca na jednego mieszkańca jest kilkukrotnie wyższa niż w krajach

południowych, co świadczy o powszechności korzystania z ubezpieczeń oraz wyższych dochodach gospodarstw domowych. Najwyższe wartości odnotowano w Szwecji, natomiast najniższe w Grecji. Choć w krajach południowych obserwowany jest stopniowy wzrost gęstości ubezpieczeniowej, dystans pomiędzy analizowanymi regionami pozostaje znaczący.

Wnioski

Przeprowadzona analiza wykazała istotne różnice w poziomie rozwoju rynków ubezpieczeniowych w krajach Europy Północnej i Południowej. Rynki północnoeuropejskie charakteryzują się wyższą penetracją ubezpieczeniową, większą gęstością ubezpieczeń oraz stabilnym wzrostem wartości składek, co świadczy o ich wysokim stopniu dojrzałości i odporności na kryzysy gospodarcze. Z kolei rynki krajów Europy Południowej, mimo obserwowanego stopniowego rozwoju, nadal cechują się niższym poziomem zaangażowania społeczeństwa w korzystanie z ubezpieczeń oraz ograniczoną rolą sektora w gospodarce.

Na podstawie uzyskanych wyników można jednoznacznie stwierdzić, że postawiona w artykule teza badawcza została potwierdzona. Rynki ubezpieczeniowe w krajach Europy Północnej są bardziej rozwinięte niż w krajach Europy Południowej, co wynika przede wszystkim z wyższego poziomu rozwoju gospodarczego, stabilności systemów finansowych, silniejszych instytucji publicznych oraz większej świadomości ubezpieczeniowej społeczeństw.

Bibliografia

Literatura

1. Bednarczyk T.H., *Ekonomiczne i instytucjonalne czynniki rozwoju ubezpieczeń,* Polska Izba Ubezpieczeń.
2. Bednarczyk T.H., Bielawska K., Jackowska B., Wycinka E., *Ekonomiczne i demograficzne uwarunkowania funkcjonowania i rozwoju ubezpieczeń*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2019.
3. Bukowski S., Lament M., *Impact of foreign capital on the insurance market development in the Visegrad Group countries*, „Journal of Management and Financial Sciences", 2019, 38, s. 33-45.
4. *Encyklopedia popularna PWN*, Warszawa 1982, s. 815.
5. Garbiec R., *Ubezpieczenia w teorii i praktyce*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2022.
6. Gazeta Ubezpieczeniowa, *Włochy: Luka ubezpieczeniowa pochłania finanse państwa*, 2023.
7. Hist.pl, *Bankructwo Grecji – jak doszło do finansowego kryzysu?*, 2023. https://hist.pl/bankructwo-grecji-jak-doszlo-do-finansowego-kryzysu/ [dostęp: 15.12.2025].
8. Komisja Europejska, *Twoje uprawnienia do zabezpieczenia społecznego w Norwegii*, 2012.

9. Lament M., Bukowski S., *Wybrane determinanty rozwoju rynków ubezpieczeniowych krajów Unii Europejskiej w latach 1999-2019*, „Wiadomości Ubezpieczeniowe", 2022, 4, s. 61-74.
10. Ronka-Chmielowiec W., *Ubezpieczenia*, Wydawnictwo C.H. Beck, Warszawa 2016.
11. SAMPO GROUP, *The Swedish P&C insurance market*, „P&C insurance markets by country", 2025.
12. Szyszko-Głowacka K., *Jak ubezpieczają się w Unii – Szwecja*, ZUS
13. Szyszko-Głowacka K., *Jak ubezpieczają się w Unii (Finlandia)*, ZUS
14. Szyszko-Głowacka K., *Jak ubezpieczają się w Unii – Włochy*, ZUS, 2018.
15. Szyszko-Głowacka K., *Jak ubezpieczają się w Unii – Malta*, ZUS, 2018.
16. Szyszko-Głowacka K., *Jak ubezpieczają się w Unii (Grecja)*, ZUS.

Dane statystyczne

1. The World Bank, https://databank.worldbank.org [dostęp: 15.12.2025].
2. Finance Finland, https://finanssiala.fi [dostęp: 15.12.2025].
3. OECD, https://oecd.org [dostęp: 15.12.2025].
4. Statista, https://statista.com [dostęp: 15.12.2025].
5. Insurance Europe, https://www.insuranceeurope.eu/ [dostęp: 15.12.2025].

THE DEVELOPMENT OF INSURANCE MARKETS IN NORTHERN AND SOUTHERN EUROPE

Abstract

The aim of this article is to analyze and compare the level of development of insurance markets in Northern and Southern Europe, with particular emphasis on the economic, social, and institutional factors influencing these differences, as well as to identify key barriers and development potential in both regions. The analysis covers Sweden, Finland, Norway, Italy, Malta, and Greece. The study uses insurance market development indicators. The results of the analysis indicate significant differences between the regions studied, confirming the higher level of development of insurance markets in Northern European countries.

Keywords: insurance market; insurance penetration; insurance density; Northern Europe; Southern Europe; financial sector.

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.019

Julia Pękala[1], Katarzyna Tkacz[2], Aleksandra Ziomka[3]

ROZWÓJ BANKOWOŚCI MOBILNEJ A BEZPIECZEŃSTWO DANYCH KLIENTÓW

Streszczenie

W artykule omówiono rozwój bankowości mobilnej w Polsce oraz związane z nim wyzwania w zakresie bezpieczeństwa danych klientów. Przedstawiono główne zagrożenia oraz rozwiązania stosowane przez banki. Na przykładach wybranych instytucji finansowych wskazano, że skuteczna ochrona wymaga połączenia nowoczesnych technologii z edukacją użytkowników. Podkreślono, że dalszy rozwój bankowości mobilnej powinien opierać się na innowacyjnych zabezpieczeniach i świadomym korzystaniu z usług cyfrowych.

Słowa kluczowe: bank, bankowość mobilna, bezpieczeństwo danych.

WSTĘP

Dynamiczny rozwój technologii informacyjno-komunikacyjnych w ostatnich latach znacząco wpłynął na sposób funkcjonowania sektora finansowego. Jednym z najważniejszych przejawów tej transformacji jest bankowość mobilna, która umożliwia klientom dostęp do usług bankowych z dowolnego miejsca i o dowolnym czasie. Użytkownicy mogą realizować operacje finansowe, zarządzać kontem czy inwestycjami za pośrednictwem smartfona lub tabletu, co czyni bankowość mobilną niezwykle wygodnym i popularnym kanałem kontaktu z bankiem.

[1] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119676@student.uthrad.pl.
[2] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119679@student.uthrad.pl.
[3] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119681@student.uthrad.pl.

Upowszechnienie rozwiązań mobilnych przyniosło jednak również nowe wyzwania w zakresie bezpieczeństwa danych klientów. Wraz ze wzrostem liczby użytkowników rośnie liczba zagrożeń – od ataków phishingowych i malware, po wyłudzenia z wykorzystaniem socjotechniki. Dlatego współczesne instytucje finansowe stają przed koniecznością nieustannego doskonalenia systemów ochrony informacji, a także podnoszenia świadomości użytkowników w zakresie bezpiecznego korzystania z usług online.

Celem niniejszego artykułu jest analiza rozwoju bankowości mobilnej oraz ocena stosowanych przez banki mechanizmów zabezpieczających dane klientów. W pracy przedstawiono ewolucję usług mobilnych w Polsce, omówiono podstawowe zagrożenia towarzyszące korzystaniu z aplikacji bankowych, a także zaprezentowano konkretne przykłady rozwiązań stosowanych przez wybrane instytucje finansowe. Artykuł ma na celu ukazanie, że bezpieczeństwo bankowości mobilnej stanowi złożone zagadnienie technologiczno-organizacyjne, wymagające współdziałania banku i klienta w ramach wspólnego systemu ochrony.

1. Istota i rozwój bankowości mobilnej

Bankowość mobilna (ang. *mobile banking*, m-banking) stanowi jeden z kluczowych obszarów cyfrowej transformacji sektora finansowego. W najszerszym rozumieniu odnosi się do możliwości dokonywania operacji bankowych za pomocą telefonu komórkowego[4]. Bardziej szczegółowo definiowana jest jako usługa oferowana przez instytucje finansowe umożliwiająca dostęp do rachunku bankowego poprzez urządzenia mobilne posiadające dostęp do Internetu, w szczególności smartfonów i tabletów, z wykorzystaniem dedykowanych aplikacji, przeglądarek internetowych w wersji mobilnej lub komunikatów SMS/USSD[5]. Podsumowując przytoczone definicje, bankowość mobilna rozumiana jest jako platforma, która umożliwia dostęp do usług lub produktów bankowych za pośrednictwem urządzeń mobilnych[6]. Na podstawie definicji można wyróżnić jej kilka cech. Po pierwsze komunikacja na linii bank – klient realizowana jest za pośrednictwem Internetu mobilnego. Drugą cechą bankowości mobilnej jest interaktywność oraz dostęp w dowolnym czasie i miejscu. Bankowość mobilna może być realizowana za pośrednictwem różnych technologii – SMS, WAP, „lekkich" stron internetowych oraz aplikacji mobilnych. Wyróżniane są dwa rodzaje dostępu do usług lub produktów bankowych: pasywny i aktywny. W ramach dostępu aktywnego klient może realizować transakcje, np. zlecać przelewy, zakładać lokaty czy spłacać karty kredytowe. W dostępie pasywnym

[4] Z. Dobosiewicz, *Bankowość*, PWE, Warszawa 2011, s. 271-272.

[5] A. Janc, G. Kotliński, *Nowe technologie we współczesnym banku*, Akademia Ekonomiczna w Poznaniu, Poznań 2004.

[6] G. Uytterhoeven, *Financial services through mobile devices*, „Efma journal", nr 228, kwiecień-czerwiec 2011, s. 56.

klient nie ma możliwości realizacji transakcji, a jedynie posiada dostęp do informacji takich jak saldo, informacje o posiadanych kartach, historia transakcji itd.[7]

Pierwsze próby wykorzystania bankowości mobilnej miały miejsce w ubiegłym stuleciu, zasadniczo tuż przed rozwojem bankowości internetowej. Pod koniec lat 90. bankowość mobilna była nazywana bankowością SMS, ponieważ obsługiwana była głównie za pośrednictwem wiadomości SMS. Pierwsze usługi były bardzo ograniczone, był to np. SMS z zapytaniem o saldo konta. W 1999 roku wraz z wprowadzeniem protokołu WAP (Wireless Application Protocol) banki zaczęły oferować swoim klientom pierwsze platformy bankowości mobilnej. Pierwsza bankowość WAP pojawiła się w Norwegii w 1999 roku.

Do 2010 roku usługi bankowości mobilnej były oferowane za pośrednictwem SMS-ów i WAP. W 2007 roku Bank of Scotland ogłosił pierwszą na świecie aplikację bankowości mobilnej na smartfony. Co więcej, już w 2009 roku firma udostępniła swoim klientom darmową, pierwszą aplikację mobilną na iPhone'a oraz funkcję szybkich wyciągów tekstowych (SMS) na żądanie. Klienci mogli również sprawdzać aktualne saldo i ostatnie transakcje w czasie rzeczywistym.

W 2011 roku szkocki bank uruchomił pierwszą na świecie darmową, w pełni funkcjonalną aplikację bankową, dostępną na iPhone'y, Androida i Blackberry. Odbiór w społeczeństwie był pozytywny i w ciągu pierwszych sześciu miesięcy usługa przyciągnęła ponad milion użytkowników, którzy przelali za jej pośrednictwem ponad miliard funtów[8].

Bankowość mobilna w Polsce rozwijała się stopniowo, jedynie z lekkim opóźnieniem do państw Europy Zachodniej i początkowo związana była z dostępem do konta z wykorzystaniem krótkich wiadomości tekstowych SMS oraz technologii WAP. W 2000 r. Bank Zachodni WBK jako pierwszy uruchomił serwis w standardzie WAP, który umożliwiał aktywny dostęp do rachunku[9]. W tym samym czasie mBank uruchomił serwis aktywny w technologii SMS. Dużym krokiem w rozwoju bankowości mobilnej w Polsce był rok 2002, wówczas Raiffeisen Bank Polska – jako pierwszy bank na polskim rynku – udostępnił mobilną aplikację (SIM Application Toolkit). Na przestrzeni lat kolejne banki korzystały z tych rozwiązań. W 2005 r. powiadomienia SMS uruchomił Bank Millennium. Rok później mBank, MultiBank, Citi Handlowy oraz ING Bank Śląski wykorzystały także SMS do przesyłania haseł jednorazowych w celu autoryzacji transakcji w kanale internetowym (np. przelewów). W następnych latach w wyniku generowania wysokich kosztów i słabej funkcjonalności stopniowo wycofywano się z rozwiązań protokołu WAP[10]. W 2010 r. już tylko nieliczne banki

---

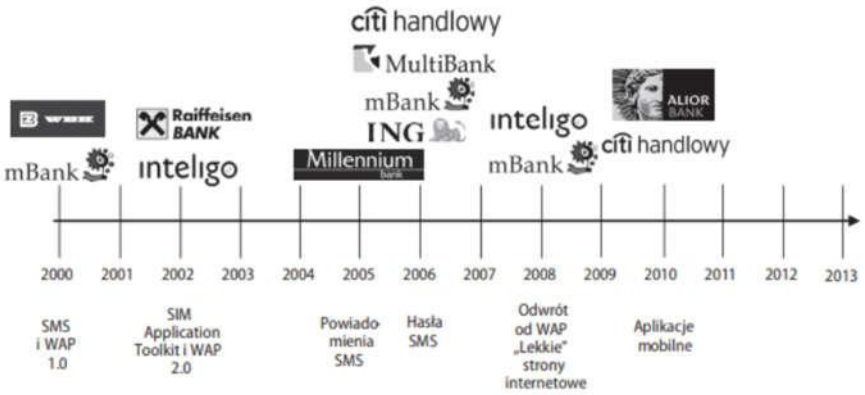
7 T. Hassa, *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce*, Szkoła Główna Handlowa w Warszawie, s. 41.

8 M. Kochańska, *Historia bankowości mobilnej*, https://whitehats.pwr.edu.pl/research/history-of-mobile-banking/ [dostęp: 30.09.2025].

9 Instytut Badań nad Gospodarką Rynkową, *Prognoza rozwoju rynku bankowego do 2016 r.* Gdańsk, kwiecień 2012, s. 231.

10 M. Kochańska, *Historia...*, op. cit.

posiadały serwisy WAP. Kamieniem milowym, który spowodował stworzenie rynku trwającego do dziś, było uruchomienie przez banki tzw. „lekkich" stron internetowych. W 2008 roku Inteligo, jako pierwsze w Polsce, uruchomiło taki serwis. Krótko potem kolejne banki korzystały z tego rozwiązania. W latach 2010/2011 można było się już spotkać z bankowością mobilną w wersji aplikacyjnej. Na przestrzeni dwóch lat już 12 banków na polskim rynku dawało możliwość korzystania z aplikacji bankowej. Obecnie serwis SMS (powiadomienia, autoryzacja lub zlecanie transakcji) oraz „lekkie" strony internetowe są codziennością na rynku. Należy zaznaczyć, że praktycznie wszystkie banki zapewniają przez wspomniane usługi aktywny dostęp do konta. Najważniejsze etapy rozwoju bankowości mobilnej w Polsce przedstawiono na rys. 1.



Rys. 1. Historia bankowości mobilnej w Polsce
Źródło: T. Hassa, *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce*, Szkoła Główna Handlowa w Warszawie, 2013, s. 43

Wraz z dynamicznym rozwojem bankowości mobilnej kluczowego znaczenia nabiera zagadnienie cyberbezpieczeństwa, które odnosi się do stanu zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają samej cyberprzestrzeni, jak i funkcjonowania w niej, a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji[11]. Bankowość mobilna, jako kanał w pełni cyfrowy, jest narażona na szerokie spektrum zagrożeń, takich jak ataki typu *phishing* i *smishing* czy złośliwe oprogramowanie. Zapewnienie odpowiedniego poziomu bezpieczeństwa wymaga wielowarstwowego podejścia. Banki stosują obecnie zaawansowane mechanizmy kryptograficzne, uwierzytelnianie wieloskładnikowe, ale również prowadzą działalność edukacyjną i uświadamiającą w tym zakresie.

[11] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne, Akademia Sztuki wojennej, 2019,* s. 12-13.

W kontekście dalszych rozważań szczególnego znaczenia nabierają kwestie bezpieczeństwa danych klientów, architektury aplikacji oraz zgodności z regulacjami prawnymi, co stanowi kluczowy obszar analizy w kolejnych częściach niniejszej pracy.

2. Zagrożenia dla klientów związane z bankowością mobilną

W literaturze przedmiotu wskazuje się, że bankowość mobilna podlega szerokiemu spektrum zagrożeń, które można klasyfikować w różny sposób – od ataków technicznych i luk programistycznych, po błędy ludzkie i niebezpieczne zachowania klientów. Celem niniejszego rozdziału jest przedstawienie i omówienie kluczowych zagrożeń związanych z korzystaniem z bankowości mobilnej.

Zjawisko *phishingu* jest jednym z najpowszechniejszych zagrożeń. Polega na otrzymywaniu wiadomości mailowych, SMS lub poprzez komunikatory internetowe, które wydają się autentyczne. Ich celem jest pozyskanie danych osobowych odbiorcy. Sprawcy podszywają się pod znane instytucje lub zaufane osoby w celu pozyskania haseł bankowych i loginów. *Phishing* określany jest jako „łowienie haseł" (ang. *Password harvesting phishing*)[12]. W Polsce rozpoznano również pokrewne zagrożenie, tzw. „na BLIKa". Przestępcy wykradają dane logowania swoich ofiar do kont na komunikatorach społecznościowych, a następnie podszywając się, piszą wiadomość do potencjalnej ofiary, która znajduje się w grupie znajomych i proszą o szybką pożyczkę. Przykładowo informują, że stoją w sklepie przy kasie i zapomnieli portfela, a terminal obsługuje płatności Blikiem. W rzeczywistości oszust może stać przed bankomatem i czekać na podanie kodu, który umożliwi mu wypłatę pieniędzy bez użycia karty debetowej. W temacie bankowości popularne są również połączenia telefoniczne od rzekomych pracowników banku, którzy informują o konieczności zweryfikowania danych do logowania. Sprawcy *phishingu* często wysyłają wiadomości SMS informujące o konieczności uiszczenia dodatkowej opłaty za przesyłkę zamówioną np. na portalu Allegro.pl lub za paczkę, która nie istnieje. Celem sprawców *phishingu* jest wykorzystanie błędów ludzkich, a nie sprzęt czy jego oprogramowanie[13].

Kolejne zagrożenie to Man-in-theMiddle (MITM). Ataki MITM polegają na manipulowaniu istniejącymi sieciami lub tworzeniu złośliwych sieci kontrolowanych przez cyberprzestępcę. Cyberprzestępcy działają jako „pośrednicy" między osobą wysyłającą i odbierającą informację, wyłudzając informacje, stąd nazwa „atak man-in-the-middle". Ataki te są powszechne zwłaszcza w publicznych sieciach Wi-Fi,

---

[12] K.Oleś, *Phishing, skimming jako przestępstwa bankowe. Charakterystyka i metody działania sprawców*, s. 220, https://www.researchgate.net/profile/Dawid-Pytel/publication/380519519_Model_kompetencji_menedzerskich_w_kontekscie_nowych_wyzwan_zarzadzania_zasobami_ludzkimi_w_branzy_kinowej/links/6640989a7091b94e93217248/Model-kompetencji-menedzerskich-w-kontekscie-nowych-wyzwan-zarzadzania-zasobami-ludzkimi-w-branzy-kinowej.pdf#page=220, [dostęp: 30.09.2025].

[13] Ibidem, s. 222-225.

które często są niezabezpieczone, więc nie można wiedzieć, kto monitoruje lub przechwytuje ruch internetowy.

Skimming jest zagrożeniem, którego celem są karty płatnicze. Skimming wywodzi się z angielskiego słowa *skim* oznaczającego „zbierać", zatem definiowany jest jako „bezprawne skopiowanie informacji zapisanych na pasku magnetycznym umieszczonym na karcie płatniczej oraz przechwycenie zabezpieczającego kodu PIN bez wiedzy i zgody posiadacza lub użytkownika w celu wykonania duplikatu karty, służącego do obciążenia rachunku bankowego posiadacza"[14]. Najgroźniejszą odmianą *skimmingu* jest tzw. *skimming* bankomatowy, którego celem są bankomaty, a dokładniej modyfikacja (nielegalna) tych urządzeń w celu pozyskania danych. Na bankomatach montowane są urządzenia skanujące/skimmer, które kopiują dane znajdujące się na drugiej ścieżce paska magnetycznego. Informacje od razu są wysyłane do przestępcy znajdującego się w okolicy. Innych sposobem na modyfikację bankomatu jest instalacja bardzo małej kamerki lub nakładki na klawiaturę, które mają na celu wyłudzenie numeru PIN[15].

Niebezpieczeństwa w cyberprzestrzeni wynikają nie tylko z ataków technicznych. Zagrożenia stanowią również luki w oprogramowaniu w aplikacjach bankowych. Zaliczane są tutaj m.in. niewłaściwe projektowanie systemów lub niedostateczne testowanie aplikacji. Typowe przykłady obejmują brak odpowiedniego szyfrowania danych przesyłanych lub przechowywanych na urządzeniu mobilnym, podatności w interfejsach API umożliwiających komunikację aplikacji z serwerami bankowymi, a także zapisywanie wrażliwych informacji w pamięci urządzenia w sposób niezabezpieczony (np. w postaci jawnej). Błędy i słabości związane z oprogramowaniem stanowią „pokusę" dla przestępców do przejęcia danych uwierzytelniających lub manipulacji komunikacją między aplikacją a bankiem, co bezpośrednio zagraża poufności i integralności danych klientów.

Ostatnim ogniwem powodującym wyłudzenia są sami klienci i użytkownicy bankowości mobilnej. Nieostrożność lub brak świadomości zwiększa prawdopodobieństwo wystąpienia przestępstwa. Takie zachowania to m.in. instalowanie aplikacji z niepewnych źródeł, korzystanie z niezabezpieczonych sieci publicznych, stosowanie słabych lub powtarzalnych haseł, a także ignorowanie komunikatów i ostrzeżeń dotyczących bezpieczeństwa.

Zagrożenia związane z bankowością mobilną mają charakter wielowymiarowy i obejmują zarówno kwestie techniczne, wynikające z luk w oprogramowaniu czy zaawansowanych metod ataków cybernetycznych, jak i czynniki behawioralne związane z zachowaniami użytkowników. Analiza literatury wskazuje, że to właśnie połączenie niedoskonałości technologicznych z niskim poziomem świadomości klientów tworzy środowisko sprzyjające działalności cyberprzestępców. Z tego względu skuteczne przeciwdziałanie ryzyku w obszarze bankowości mobilnej wymaga podejścia

[14] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10(6), s. 104.

[15] K. Oleś, Phishing..., s. 224-226.

kompleksowego – obejmującego zarówno rozwój i wdrażanie nowoczesnych zabezpieczeń technicznych, jak i systematyczne działania edukacyjne skierowane do użytkowników końcowych. Tylko równoczesne wzmocnienie obu tych obszarów może zagwarantować stabilny i bezpieczny rozwój usług bankowości mobilnej w perspektywie długoterminowej.

3. Zabezpieczenia stosowane przez bank

Rozwój bankowości internetowej i mobilnej sprawił, że korzystanie z konta stało się niezwykle wygodne i szybkie, jednak równocześnie pojawiły się nowe zagrożenia związane z bezpieczeństwem danych i środków finansowych. Aby chronić klientów przed ryzykiem, banki wdrażają rozbudowane mechanizmy ochronne. Ich zadaniem jest nie tylko zabezpieczenie infrastruktury technicznej, ale również wsparcie użytkownika w codziennym korzystaniu z usług online.

Jednym z najważniejszych elementów ochrony jest szyfrowanie komunikacji pomiędzy klientem a serwerem banku. W tym celu stosuje się protokoły SSL/TLS, które zapewniają poufność i nienaruszalność przesyłanych informacji. Dzięki nim dane logowania, numery rachunków czy szczegóły przelewów nie mogą zostać przechwycone i wykorzystane przez osoby niepowołane. Każdy klient powinien upewniać się, że adres strony banku rozpoczyna się od „https://" oraz że w pasku przeglądarki widoczna jest ikona kłódki.

Kolejną warstwą zabezpieczeń jest wieloskładnikowa autoryzacja (MFA). Oznacza ona, że logowanie czy zatwierdzanie transakcji nie opiera się wyłącznie na haśle. Do uwierzytelnienia wykorzystuje się zazwyczaj co najmniej dwa elementy: coś, co klient wie (np. hasło, PIN); coś, co posiada (np. token, aplikację mobilną z kodami jednorazowymi, SMS-kod) oraz biometrie (np. odcisk palca, rozpoznanie twarzy czy głosu). Dzięki temu samo przejęcie hasła nie pozwoli przestępcy na dostęp do konta.

Popularnym rozwiązaniem są wciąż kody jednorazowe – wysyłane SMS-em, generowane przez tokeny sprzętowe lub aplikacje bankowe. Każdy z nich jest ważny tylko raz i przez krótki czas, co uniemożliwia ponowne użycie. Coraz częściej banki odchodzą od SMS-ów na rzecz aplikacji mobilnych, które oferują wyższy poziom ochrony.

Znaczącą rolę odgrywają również metody biometryczne. Dzięki nim klient może logować się do aplikacji lub zatwierdzać przelewy przy użyciu odcisku palca, skanu twarzy czy głosu. Biometria jest nie tylko bezpieczna, ale i wygodna, ponieważ eliminuje konieczność pamiętania skomplikowanych haseł.

Banki wdrażają także monitoring aktywności. Systemy analizują charakterystyczne wzorce działań – godziny logowania, zwyczajowe kwoty przelewów, miejsca dostępu. Jeśli wykryją nietypowe zdarzenia, np. przelew na wysoką kwotę wysłany za granicę czy logowanie z nieznanej lokalizacji, mogą automatycznie zablokować transakcję, ograniczyć dostęp do konta lub skontaktować się z klientem. W tym celu stosuje się również limity transakcyjne, które ograniczają maksymalne kwoty przelewów w określonym czasie.

Oprócz tego banki inwestują w systemy ochrony przed *phishingiem*. Weryfikują autentyczność witryn poprzez certyfikaty EV SSL, korzystają z filtrów blokujących fałszywe wiadomości i współpracują z dostawcami oprogramowania antywirusowego. Celem tych działań jest maksymalne utrudnienie oszustw polegających na podszywaniu się pod bank.

Nie bez znaczenia są również działania organizacyjne – banki regularnie prowadzą kampanie edukacyjne, które przypominają o konieczności ostrożności w sieci i aktualizowania oprogramowania. W sytuacjach zagrożenia uruchamiane są procedury kryzysowe, takie jak blokowanie kont, zatrzymywanie przelewów i bezpośredni kontakt z klientem.

Wszystkie te mechanizmy tworzą wielowarstwowy system bezpieczeństwa, którego zadaniem jest zminimalizowanie ryzyka kradzieży danych i pieniędzy. Na ochronę składają się zarówno rozwiązania techniczne – szyfrowanie, biometryka, analiza ryzyka – jak i inicjatywy edukacyjne. Warto jednak pamiętać, że skuteczność tych zabezpieczeń zależy nie tylko od banku, lecz także od samych klientów. Nawet najbardziej zaawansowane narzędzia nie ochronią użytkownika, który lekkomyślnie udostępni swoje dane lub zignoruje podstawowe zasady bezpieczeństwa.

4. Przykłady banków i stosowanych rozwiązań zabezpieczających

Wraz z dynamicznym rozwojem bankowości mobilnej w Polsce (ponad 23 mln aktywnych użytkowników w 2024 r.[16]) rośnie znaczenie ochrony danych klientów. Banki wdrażają zróżnicowane rozwiązania – zarówno technologiczne, jak i edukacyjne – które mają minimalizować ryzyko utraty środków i poufnych informacji.

4.1. PKO Bank Polski

PKO BP, lider rynku mobilnego, w aplikacji IKO i serwisie iPKO stosuje m.in. uwierzytelnianie dwuetapowe, autoryzację mobilną zamiast kodów SMS, logowanie biometryczne oraz możliwość ustawiania limitów transakcji[17]. Dane użytkownika są szyfrowane, a aplikacja wymaga każdorazowej autoryzacji przy operacjach finansowych[18].

4.2. BNP Paribas Bank Polska

BNP Paribas koncentruje się na wykorzystaniu analizy behawioralnej – system monitoruje sposób korzystania z telefonu (np. tempo pisania, ruchy dłoni) i w razie wykrycia anomalii blokuje transakcję[19]. Dodatkowo stosowane są zabezpieczenia

[16] Związek Banków Polskich, *Raport: Bankowość Mobilna 2024*, bnpparibas.pl [dostęp: 30.09.2025].
[17] PKO Bank Polski, *Bezpieczne logowanie do banku online,* pkobp.pl [dostęp: 30.09.2025].
[18] PKO Bank Polski, *Mobilna autoryzacja IKO*, iko.pkobp.pl [dostęp: 30.09.2025].
[19] PRNews, *BNP Paribas rozpozna oszusta po tym, jak trzyma smartfon*, prnews.pl [dostęp: 30.09.2025 r.].

biometryczne oraz natychmiastowe powiadomienia o operacjach[20]. Rozwiązania te łączą klasyczne mechanizmy (PIN, limity) z nowoczesnymi metodami analizy zachowań.

4.3. Santander Bank Polska

Santander promuje model bezpieczeństwa oparty na edukacji użytkownika. W poradniku *5 zasad bezpiecznego bankowania* bank wskazuje m.in. na konieczność unikania podejrzanych linków, stosowania silnych haseł, instalacji aplikacji wyłącznie z oficjalnych źródeł oraz aktualizacji systemu[21]. Wyróżnia się również szybka reakcja na zgłoszenia klientów i zachęta do samodzielnego monitorowania konta.

Wnioski

Polskie banki konsekwentnie integrują zaawansowane technologie (biometrię, autoryzację mobilną, szyfrowanie) z działaniami edukacyjnymi. Badania wskazują, że „postrzegane ryzyko" ma istotny wpływ na akceptację bankowości mobilnej[22], dlatego kluczowe jest nie tylko wdrażanie zabezpieczeń, lecz także budowanie świadomości użytkowników. Przykłady PKO BP, BNP Paribas i Santandera dowodzą, że skuteczna ochrona danych wymaga współdziałania banku i klienta w ramach wielopoziomowego systemu bezpieczeństwa.

Zakończenie

Bankowość mobilna stała się integralną częścią współczesnego systemu finansowego, a jej znaczenie rośnie wraz z postępującą cyfryzacją usług i potrzebą natychmiastowego dostępu do informacji finansowych. Analiza rozwoju tego sektora pokazuje, że polskie banki z powodzeniem wdrożyły nowoczesne rozwiązania technologiczne, które zapewniają klientom wygodę, szybkość i elastyczność w zarządzaniu finansami. Jednocześnie rozwój ten wiąże się z koniecznością stałego wzmacniania ochrony danych osobowych i finansowych.

Przedstawione w artykule przykłady działań PKO Banku Polskiego, BNP Paribas oraz Santander Bank Polska dowodzą, że skuteczne bezpieczeństwo w bankowości mobilnej wymaga wielopoziomowego podejścia – łączącego technologię, procedury organizacyjne i edukację użytkowników. Zastosowanie rozwiązań takich jak uwierzytelnianie wieloskładnikowe, biometria, szyfrowanie danych czy analiza behawioralna znacząco ogranicza ryzyko utraty środków i nieuprawnionego dostępu do informacji.

---

[20] BNP Paribas, *7 zasad bezpieczeństwa bankowości mobilnej*, bnpparibas.pl [dostęp: 30.09.2025].

[21] Santander Bank Polska, *5 zasad bezpiecznego bankowania*, santander.pl [dostęp: 30.09.2025 r.].

[22] P. Sikorski, *The usage of mobile banking applications in Poland – empirical results*, *ResearchGate*, 2019.

Wnioski płynące z opracowania wskazują, że dalszy rozwój bankowości mobilnej powinien opierać się na dwóch filarach: innowacyjnych technologiach bezpieczeństwa oraz świadomym, odpowiedzialnym użytkowniku. Tylko synergia tych elementów pozwoli utrzymać wysoki poziom zaufania klientów i zapewnić stabilny rozwój cyfrowych usług finansowych w przyszłości.

Bibliografia

1. Ataki typu „man-in-the-middle" (MITM), [online] https://www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html [dostęp: 30.09.2025].
2. BNP Paribas, *7 zasad bezpieczeństwa bankowości mobilnej*, bnpparibas.pl [dostęp: 30.09.2025].
3. Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne,* Akademia Sztuki Wojennej, Warszawa, 2019.
4. Dobosiewicz Z., *Bankowość*, PWE, Warszawa, 2011.
5. Hassa T., *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce,* Szkoła Główna Handlowa w Warszawie, 2013.
6. *Historia bankowości mobilnej*, http://komorkomania.pl/2010/04/02/historia-mobilnej-bankowosci [dostęp: 30.09.2025].
7. *Historia bankowości mobilnej – jak to się wszystko zaczęło?,* [online] https://finanteq.com/blog/fintech-trends/history-of-mobile-banking-how-it-all-started/#:~:text=The%20Bank%20of%20Scotland%20is,ATMs%20as%20early%20as%202004 [dostęp: 30.09.2025].
8. Instytut Badań nad Gospodarką Rynkową, *Prognoza rozwoju rynku bankowego do 2016 r.,* Gdańsk, kwiecień 2012.
9. Janc A., Kotliński G., *Nowe technologie we współczesnym banku*, Akademia Ekonomiczna w Poznaniu, Poznań, 2004.
10. Kochańska M., *Historia bankowości mobilnej*, https://whitehats.pwr.edu.pl/research/history-of-mobile-banking/ [dostęp: 30.09.2025].
11. Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10(6).
12. Oleś K., *Phishing, skimming jako przestępstwa bankowe. Charakterystyka i metody działania sprawców*, Dąbrowa Górnicza 2023, [online] https://www.researchgate.net/profile/Dawid-Pytel/publication/380519519_Model_kompetencji_menedzerskich_w_kontekscie_nowych_wyzwan_zarzadzania_zasobami_ludzkimi_w_branzy_kinowej/links/6640989a7091b94e93217248/Model-kompetencji-menedzerskich-w-kontekscie-nowych-wyzwan-zarzadzania-zasobami-ludzkimi-w-branzy-kinowej.pdf#page=220 [dostęp: 30.09.2025].
13. PKO Bank Polski, *Bezpieczne logowanie do banku online,* pkobp.pl [dostęp: 30.09.2025].
14. PKO Bank Polski, *Mobilna autoryzacja IKO*, iko.pkobp.pl [dostęp: 30.09.2025].
15. PRNews, *BNP Paribas rozpozna oszusta po tym, jak trzyma smartfon*, prnews.pl [dostęp: 30.09.2025].

16. Santander Bank Polska, *5 zasad bezpiecznego bankowania*, santander.pl [dostęp: 30.09.2025].
17. Sikorski P., *The usage of mobile banking applications in Poland – empirical results*, ResearchGate, 2019.
18. Uytterhoeven G., *Financial services through mobile devices*, „Efma Journal", nr 228, kwiecień–czerwiec 2011.
19. Związek Banków Polskich, *Raport: Bankowość Mobilna 2024*, bnpparibas.pl [dostęp: 30.09.2025].

THE DEVELOPMENT OF MOBILE BANKING AND CUSTOMER DATA SECURITY

Abstract

Paper discussed the development of mobile banking in Poland and the related challenges concerning customer data security. It presents the main threats and the solutions implemented by banks. Based on examples from selected financial institutions, it is shown that effective protection requires combining modern technologies with user education. The article emphasizes that the further development of mobile banking should be based on innovative security measures and responsible use of digital services.

Keywords: bank, mobile banking, security of information.

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.020

Ola Rdzanek[1], Zuzanna Sulima[2]

STRATEGIE I WYZWANIA CYBERBEZPIECZEŃSTWA W BANKOWOŚCI

Streszczenie

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

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

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

Wstęp

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

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

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

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

1. Źródła cyberzagrożeń

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Rodzaje cyberzagrożeń

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

3. Systemy i strategie ochrony w bankowości

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

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

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

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

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

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

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

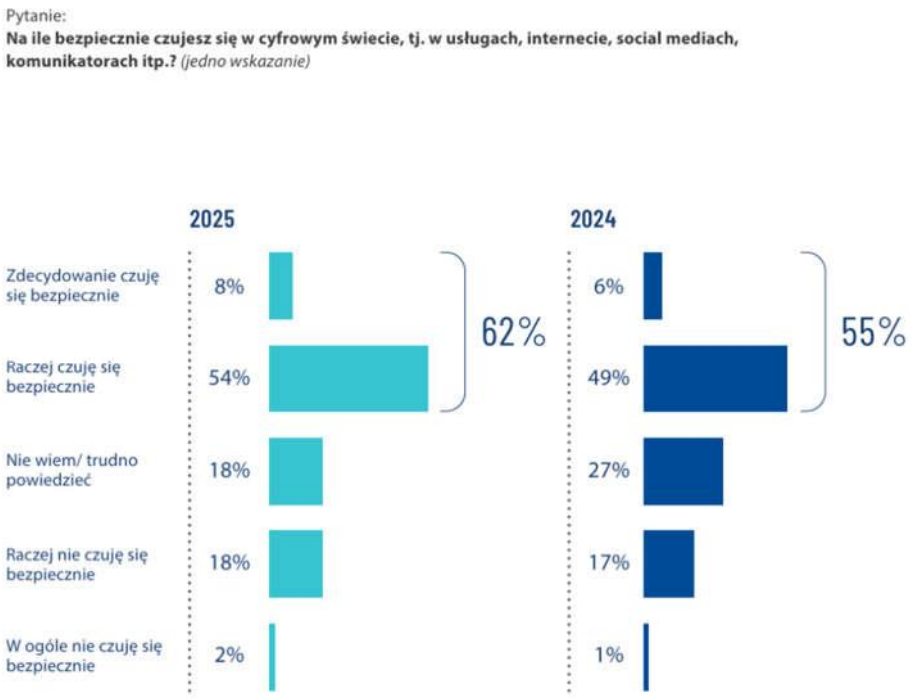
szyfrowanie połączeń, które uniemożliwia osobom trzecim podgląd przesyłanych danych. Skuteczne bezpieczeństwo bankowości opiera się więc na połączeniu technologii monitorujących i szyfrujących z odpowiedzialnym zachowaniem klienta[20].

4. Postawy Polaków wobec cyberbezpieczeństwa

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

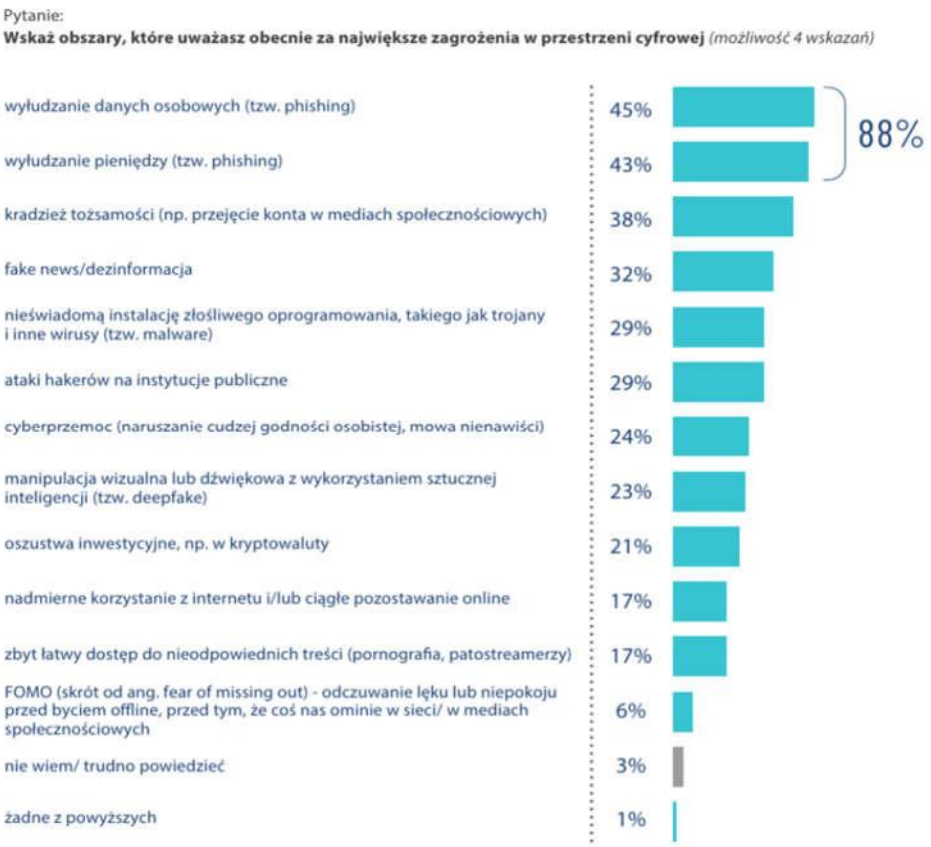
Poniżej przedstawiono wyniki badań Polaków na temat poczucia bezpieczeństwa w przestrzeni cyfrowej. W 2024 roku możemy zaobserwować, że 55% badanych nie odczuwa zagrożenia, natomiast 27% respondentów nie potrafi określić swojego odczucia, czy czuję się pewnie w omawianej kwestii, a pozostałe 18% ankietowanych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

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



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

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



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

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

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

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

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

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

5. Wyzwania, luki i kierunki rozwoju cyberbezpieczeństwa w bankowości

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

Podsumowanie

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

---

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

Bibliografia

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

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

CYBERSECURITY STRATEGIES AND CHALLENGES IN THE BANKING SECTOR

Abstract

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

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

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

Marta Zawisza[1]

CYBERBEZPIECZEŃSTWO W BANKOWOŚCI – UJĘCIE REGULACYJNE I WYZWANIA TECHNOLOGICZNE

Streszczenie

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

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

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

Wstęp

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

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

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

1. Cyberbezpieczeństwo – pojęcie, zakres i zasady

1.1. Pojęcie cyberbezpieczeństwa

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

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

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

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

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

Tabela 1. Pojęcie cyberbezpieczeństwa

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

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

1.2. Charakterystyka najczęstszych zagrożeń

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

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

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

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

Tabela 2. Rodzaj zagrożenia

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

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

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

Cd. Tabeli 2.

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

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

1.3. Zasady wpływające na bezpieczeństwo korzystania z bankowości internetowej

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

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

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

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

1.4. Wyzwania i trendy

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

---

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

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

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

2. Dyrektywy unii europejskiej i wymagania prawne

2.1. Dyrektywa CER

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

---

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

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

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

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

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

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

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

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

2.3. Dyrektywa o atakach na systemy informacyjne

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

2.4. Cyberprzestępcy a RODO

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

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

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

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

3. Cyberbezpieczeństwo a sztuczna inteligencja

3.1. *Zagrożenia technologii stosujących sztuczną inteligencję*

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

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

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

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

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

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

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

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

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

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

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

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

Podsumowanie

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

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

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

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

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

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

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

Bibliografia

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

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

CYBERSECURITY IN BANKING – REGULATORY FRAMEWORK AND TECHNOLOGICAL CHALLENGES

Abstract

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

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

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

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.022

Martyna Markowska[1]

ANALIZA ZMIENNOŚCI KURSÓW WALUTOWYCH W POLSCE W LATACH 2020-2025 NA PRZYKŁADZIE EUR/PLN I USD/PLN

Streszczenie

W artykule przedstawiono badanie dotyczące zmian kursów walutowych EUR/PLN i USD/PLN w Polsce w latach 2020-2025 za pomocą obliczeń średniego kursu, mediany, wariancji, odchylenia standardowego, wskaźnika zmienności oraz korelacji kursów. Wyjaśniono, czym jest waluta, kurs walutowy oraz ryzyko walutowe. Określono czynniki wpływające na kształtowanie się kursu walutowego.

Słowa kluczowe: waluta, kurs walutowy, ryzyko walutowe, kurs płynny, kurs stały, kurs pełzający, współczynnik zmienności, inflacja, pandemia COVID-19, EUR/PLN, USD/PLN.

Wstęp

Analiza zmienności kursów walutowych pozwala na zrozumienie, w jaki sposób różnorodne czynniki ekonomiczne, polityczne czy globalne wpływają na wahania wartości pieniądza. Kursy walutowe odgrywają kluczową rolę w gospodarce każdego kraju. Wpływają zarówno na handel zagraniczny, inwestycje kapitałowe, jak i na sytuację finansową przedsiębiorstw oraz konsumentów. Wahania kursu walutowego oddziałują na poziom cen importowanych dóbr, koszty kredytów w walutach obcych oraz konkurencyjność eksportu. Kursy walutowe w Polsce w latach 2020-2025 ulegały zmianom z powodu szeregu wyzwań gospodarczych takich jak: skutki pandemii COVID-19 powodujące zmienność rynków finansowych, wojna na Ukrainie, która wpłynęła na zachowania inwestorów i poziom zaufania do waluty krajowej, czy polityka monetarna Narodowego Banku Polskiego dotycząca zmian stóp procentowych czy inwestycji walutowych.

[1] Studentka kierunku finanse i rachunkowość – studia II stopnia, Wydział Ekonomii i Finansów, Uniwersytet Radomski im. Kazimierza Pułaskiego, e-mail: 115488@student.uthrad.pl.

Celem artykułu jest szczegółowa analiza zmienności kursów walutowych EUR/PLN i USD/PLN w Polsce w latach 2020-2025, z uwzględnieniem średnich wartości, odchyleń od średniej, procentowych zmian w poszczególnych okresach oraz ocena wpływu różnych czynników na kształtowanie się kursów walutowych. W artykule zastosowano narzędzia statystyczne umożliwiające wyznaczenie wskaźnika zmienności i dynamiki kursów, co pozwoli na rzetelny obraz ich kształtowania się w analizowanym okresie.

1. Teoria kursów walutowych

1.1. Istota kursów walutowych

Zrozumienie zjawiska kursów walutowych wymaga poznania podstaw związanych z takim zagadnieniem jak waluta. Waluta jest to oficjalny znak pieniężny będący prawnym środkiem płatniczym w określonych krajach i/lub ich grupach[2].

Kurs walutowy to stosunek, w jakim dokonywana jest wymiana określonej ilości danej waluty na jednostkę innej waluty. Jest jedną z najważniejszych cen w gospodarce światowej[3]. Kurs jest ceną, więc powinien bilansować popyt na waluty obce z podażą tych walut. Kursy walutowe kształtują się na rynku walutowym pod wpływem popytu na waluty i podaży walut obcych. Przy istniejącej swobodzie przepływu kapitału w skali minimum dwóch krajów, stosunek wymienny dwóch walut ustala się w obu krajach na poziomie wyznaczonym zgodnie z prawem jednej ceny. Każda zmiana kursu tych walut na jednym z rynków, powoduje ruch kapitału przez granicę w celu ujednolicenia kursów[4].

Kurs walutowy określa cenę, za którą w danym kraju kupujemy określony towar, jakim jest pieniądz obcej gospodarki narodowej. Każda gospodarka funkcjonuje w ramach własnego systemu cen, który odzwierciedla wartości nadawane różnym dobrom przez uczestników rynku. Kurs walutowy stanowi relację między dwoma takimi systemami cen, co sprawia, że różni się on istotnie od zwykłej ceny. Zmiana pojedynczej ceny w danym kraju nie prowadzi do zasadniczej zmiany całego krajowego systemu cen, nawet jeśli wywołuje pewne skutki przez powiązania między cenami. Każda zmiana kursu walutowego automatycznie oznacza zmianę relacji wymiennej między dwoma rynkami, których ten kurs dotyczy. Ta właściwość kursu jest rezultatem podwójnego charakteru wartościowanego w nim towaru, którym jest zazwyczaj dewiza[5].

---

[2] Infor.pl, 2024, https://www.infor.pl/slownik/biznes/5805933,waluta.html [dostęp: 24.12.2025].

[3] E. Bartov, G.M. Bodnar, *Firm Valuation, Earnings Expectations, and the Exchange-Rate Exposure Effect,* „The Journal of Finance", 1994, No. 5, s. 1758.

[4] P. Misztal, *Zabezpieczenia przed ryzykiem zmian kursu walutowego*, Wydawnictwo Difin, Warszawa, 2004, s. 16-17.

[5] R. Ślusarczyk, *Polityka bilansu banku centralnego a kurs walutowy,* Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków, 2018, s. 208-220.

Kurs walutowy jest ceną waluty obcej, wyrażoną w pieniądzu krajowym[6]. Określa, ile jednostek pieniądza krajowego płaci się za jednostkę waluty obcej[7]. Relacja pieniądza krajowego do walut obcych może być oparta na parytecie walutowym, co miało miejsce w historycznych systemach walutowych. Relacja ta może wynikać również ze stosunku podaży do popytu na krajowym rynku walutowym. Kurs walutowy dzielimy na kurs parytetowy i nieparytetowy. Kurs parytetowy występował w systemach walutowych, w których władze monetarne ustalały wartość pieniądza krajowego jako równą pewnej ilości wagowej złota[8]. Kurs nieparytetowy oznacza brak stałego odniesienia parytetowego. O poziomie kursu waluty krajowej decyduje wielkość podaży walut obcych w stosunku do popytu na te waluty.

Wyróżniamy dwa rodzaje kursów walutowych: kurs stały oraz zmienny. Kurs stały oznaczał stan, w którym w dłuższym okresie nie było równowagi i nie można było tego usunąć w inny sposób niż zmianą kursu walutowego[9]. Kurs zmienny (inaczej zwany płynnym) jest kształtowany głównie przez mechanizm rynkowy. O poziomie kursu zmiennego decyduje stosunek podaży do popytu na waluty obce w danym kraju[10]. Kurs stały ustalany jest przez władze monetarne, a kurs zmienny bez ingerencji władz państwowych. Wynika to z kształtowania się popytu i podaży na zagraniczne środki płatnicze[11].

M. Sołtysiak twierdzi, że kurs walutowy jest ceną jednostki pieniężnej danego kraju lub krajów, wyrażonej w pieniądzu innego kraju lub krajów. Kurs walutowy pełni wiele funkcji. Funkcja informacyjna informuje o cenie walut obcych. Funkcja cenotwórcza oznacza, że kurs walutowy przenosi zagraniczny układ cen na krajowy układ cen razem z wynikającymi z tego konsekwencjami dla gospodarki krajowej. Ta funkcja występuje w gospodarce rynkowej, gdy istnieje wymienialność walut. Może zostać ograniczona przez wprowadzenie ceł, opłat i podatków importowych. Funkcja współczynnika efektywności wymiany oznacza, że ceny oraz koszty są ustalane w różnych walutach. Funkcja regulatora wymiany – poziom kursów walutowych ma bezpośredni wpływ na liczbę i wartość zawieranych transakcji. Funkcja instrumentu polityki gospodarczej jest związana z podatnością na decyzje i działania

---

6 M. Jabłoński, K. Kalicki, *Rynek walutowy. Odesłania do tabel kursowych,* Wydawnictwo SCHOLAR, 2024, s. 34.

7 M. Chrzan, *Polityka kursu walutowego w Polsce w kontekście wejścia do strefy euro*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" nr 132, Wrocław, 2010, s. 66.

8 M. Janicka, *Międzynarodowe przepływy inwestycji. Zarys teorii i praktyki na tle ewolucji międzynarodowego systemu walutowego,* Wydawnictwo Uniwersytetu Łódzkiego, Łódź, 2022, s. 18.

9 M. Zaleska, *Podstawy biznesu: zarządzania i finansów – dla nauczycieli,* Wydawnictwo Difin, Warszawa, 2023, s. 25.

10 E. Drabowski, *Teorie kursu walutowego,* Państwowe Wydawnictwo Ekonomiczne, Warszawa, 1985, s. 13-16.

11 P. Siwior, A. Dobrzycka, *Przejście Polski z kursu sztywnego na kurs płynny złotego – perspektywa prawno-ekonomiczna,* „Studia Prawnoustrojowe", 2025, s. 311.

władz państwowych. Funkcja instrumentu gier finansowych oznacza, że zmiany poziomu kursów walutowych pozwalają na realizację różnych transakcji walutowych. Występuje również funkcja porównywalności gospodarek i dochodów państwa poprzez porównanie wartości wyrażonych w różnych walutach[12].

1.2. Czynniki kształtujące kurs walutowy

E. Drabowski podkreśla, że kurs walutowy jest zależny od wielu czynników. Czynniki te można klasyfikować według ich źródła (wewnętrzne i zewnętrzne), według czasu występowania (krótkookresowe, średniookresowe, długookresowe) oraz według sposobu oddziaływania (bezpośrednie, pośrednie i średnie). Poniższa tabela przedstawia wyszczególnienie tej klasyfikacji.

Tabela 1. Klasyfikacja czynników kształtujących kurs walutowy

Kryterium	Podział	Charakterystyka
Ze względu na pochodzenie	Czynniki wewnętrzne	Wynikają z sytuacji gospodarczej, politycznej i finansowej danego kraju. Oddziałują na popyt i podaż krajowej waluty oraz innych walut. Są pod kontrolą krajowej gospodarki, władz monetarnych i fiskalnych. Wyróżniamy: kondycję gospodarki krajowej – im lepsza sytuacja ekonomiczna tym większe zaufanie inwestorów do waluty, inflacja – niska inflacja powoduje umacnianie waluty, a wysoka osłabienie, wyższe stopy procentowe – zwiększają kapitał zagraniczny, co prowadzi do umocnienia waluty, duży deficyt i rosnący dług publiczny może prowadzić do osłabienia waluty, nadwyżka w bilansie płatniczym zwiększa popyt na walutę krajową, a deficyt zwiększa popyt na waluty obce, co prowadzi do deprecjacji, stabilność polityczna i prawna, oczekiwania uczestników rynku oraz poziom inwestycji krajowych – napływ kapitału wzmacnia walutę poprzez większy popyt.
Ze względu na pochodzenie	Czynniki zewnętrzne	Występują zarówno za granicą, jak i u partnerów gospodarczych. Są najsilniejsze, gdy występuje synchronizacja cyklu koniunkturalnego w gospodarce światowej. W fazach ożywienia i rozkwitu powoduje przegrzanie koniunktury, a w fazach depresji i kryzysu pogłębia stan bezrobocia i niewykorzystanie zdolności produkcyjnych. Dotyczą: wzrostu cen, zmiany warunków przepływu kapitału (zwiększenie lub zmniejszenie stóp procentowych i opodatkowania na rynkach kapitałowo-pieniężnych), warunków płatności (restrykcje ilościowe i walutowe), stanu bilansów płatniczych, wahań kursów walutowych, braku stabilizacji politycznej w głównych krajach, groźby konfliktów na skalę międzynarodową.
Ze względu na horyzont czasowy	Czynniki krótkookresowe	Przewidywanie dotyczące kształtowania się głównych determinant kursu w przyszłości. Wyróżniamy takie czynniki jak: stopa inflacji, stopa procentowa w kraju i zagranicą, ocena zyskowności lokat w różnych walutach, wnioski z wahań płynnego kursu walutowego w przeszłości, spekulacja walutowa, interwencje walutowe władz.

[12] M. Sołtysiak, *Rynek walutowy – pojęcia i ćwiczenia*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów, 2020, s. 36-37.

Cd. Tabeli 1.

Kryterium	Podział	Charakterystyka
Ze względu na horyzont czasowy	Czynniki średniookresowe i długookresowe	Do głównych determinant czynników średniookresowych i długookresowych zaliczamy: stan bilansu handlowego, przepływy kapitału, ocenę perspektyw lokat kapitałowych w gospodarce krajowej, politykę gospodarczą rządu, w tym politykę pieniężną i ograniczenia w handlu zagranicznym, relacje cen krajowych do cen zagranicznych, organizację handlu i płatności zagranicznych oraz stopę wzrostu gospodarczego.
Ze względu na sposób oddziaływania	Czynniki bezpośrednie	Czynniki bezpośrednio oddziałujące na kurs to takie, które nie wymagają zmian innych wielkości ekonomicznych np. deficyt bilansu płatniczego powoduje spadek kursu waluty krajowej. Oddziałują natychmiast poprzez rynek walutowy, popyt i podaż walut.
Ze względu na sposób oddziaływania	Czynniki pośrednie	Czynniki pośrednie wywołują zmiany innych wielkości ekonomicznych, które wpłyną na poziom kursu walutowego np. wzrost opodatkowania zagranicznych lokat kapitałowych spowoduje zahamowanie dopływu obcego kapitału, pogorszenie stanu bilansu płatniczego oraz deprecjację waluty krajowej. Wpływają na kurs walutowy poprzez kształtowanie fundamentów gospodarki, ale nie zmieniają go bezpośrednio w danym momencie. Ich działanie jest rozłożone w czasie.

Źródło: Opracowanie własne na podstawie: E. Drabowski, *Teorie kursu walutowego,* Państwowe Wydawnictwo Ekonomiczne, Warszawa 1985, s. 95-100

Czynniki określające poziom kursów walutowych można podzielić na dwie grupy: czynniki ekonomiczne i pozaekonomiczne. Poniższa tabela zestawia rodzaje czynników określających poziom kursów walutowych.

Tabela 2. Czynniki kształtujące poziom kursów walutowych

Czynniki ekonomiczne	Czynniki pozaekonomiczne
Czynniki strukturalne – poziom rozwoju i struktura gospodarki, poziom konkurencyjności gospodarki, sytuacja w bilansie płatniczym.	Czynniki polityczne – stopień stabilizacji politycznej, stopień ryzyka politycznego, szoki polityczne.
Czynniki techniczne – intensywność i struktura przemian technicznych, poziom rozwoju zaplecza technicznego funkcjonowania rynków.	Czynniki instytucjonalne – stosowane rozwiązania systemowe, stopień liberalizacji rynków, stosowana polityka pieniężna, fiskalna, częstotliwość i sposoby interwencji banku centralnego.
Czynniki koniunkturalne – stopa wzrostu produktu krajowego brutto, stopa inflacji, zmiany stóp procentowych.	Czynniki psychologiczne – oczekiwania społeczeństwa i poziom ryzyka finansowego.

Źródło: Opracowanie własne na podstawie: P. Bożyk, M. Puławski, *Międzynarodowe stosunki ekonomiczne*, PWE, Warszawa, 1999, s. 325

Kurs walutowy jest kształtowany przez szereg czynników gospodarczych, politycznych oraz finansowych. Dotyczy waluty krajowej i zagranicznej. Wahania kursów walutowych mogą być spowodowane zarówno natychmiastowymi zdarzeniami, jak i długoterminowymi trendami gospodarczymi. Kurs walutowy odzwierciedla równowagę między popytem a podażą, napływem kapitału, stopniem zaufania do gospodarki czy poziomem ryzyka postrzeganego przez uczestników rynku.

1.3. Ryzyko walutowe

W literaturze ryzyko walutowe określane jest również jako ryzyko kursowe. Występuje w przypadku pojawienia się wahań kursu jednej waluty w stosunku do innej. Źródłem tego ryzyka jest brak możliwości przewidzenia kierunku i skali wahań kursów walutowych. Może dotyczyć trzech obszarów aktywności gospodarczej podmiotów na rynkach międzynarodowych: transakcji bieżących, działalności długookresowej oraz rozliczeń finansowych i sprawozdawczości. Ryzyko walutowe można podzielić na trzy podstawowe rodzaje: ryzyko transakcyjne, ekonomiczne oraz przeliczeniowe.

Ryzyko transakcyjne jest krótkookresowe. Związane z zagrożeniem, że wartość transakcji denominowanej w walucie obcej zmieni się w wyniku wahań kursów walutowych od momentu zawarcia umowy do jej rozliczenia. Może dotyczyć zarówno wymiany waluty obcej na krajową w celu otrzymania płatności, jak i wymiany waluty krajowej na obcą w celu uregulowania zobowiązań[13].

Ryzyko transakcyjne dzieli się na:

1) ryzyko standardowe wynikające z różnicy między datą wystawienia faktury a datą realizacji płatności,
2) ryzyko powtarzające się (związane z przyszłymi płatnościami, do których nie są ustalone dokładne wartości ani termin realizacji płatności),
3) ryzyko warunkowe, które dotyczy ofert biznesowych składanych w walutach obcych.

Ryzyko ekonomiczne jest miarą wiarygodności rynkowej wartości przedsiębiorstwa na przyszłe zmiany kursów walut. Jest długoterminowe, strategiczne oraz konkurencyjne. Związane jest z nieprzewidzianą zmianą przyszłej wartości przepływów pieniężnych pod wpływem wahań kursów walut w długim okresie. Przedsiębiorstwo jest narażone na tego rodzaju ryzyko nawet jeśli aktualnie nie prowadzi rozliczeń w walutach obcych. Może to wynikać z konkurencji, ceny surowców czy globalnych warunków rynkowych. Przykładem ryzyka ekonomicznego może być: konkurencyjność przedsiębiorstwa – jeśli kurs waluty krajowej się wzmocni, produkty eksportera stają się droższe dla zagranicznych klientów, co może obniżyć sprzedaż, oddziaływanie na koszty produkcji – przedsiębiorstwo importujące surowce poniesie wyższe koszty, gdy waluta krajowa się osłabia, wpływ na przyszłą strategię – długotrwałe trendy kursowe mogą wymusić zmianę modelu biznesowego, lokalizacji produkcji lub strukturę rynków zbytu przedsiębiorstwa[14].

Ryzyko przeliczeniowe występuje, gdy wyrażone w walucie obcej pozycje bilansu lub rachunku zysków i strat danego przedsiębiorstwa wymagają przeliczenia na walutę krajową na koniec roku obrotowego. Jest to sytuacja, w której po dokonaniu przeliczenia umieszczonych w sprawozdaniu finansowym wartości aktywów

[13] N. Iwaszczuk, *Ryzyko w działalności gospodarczej: definicje, klasyfikacje, zarządzanie,* Wydawnictwo IGSMiE PAN, Kraków, 2021, s. 37.

[14] P. Misztal, *Zabezpieczenia przed ryzykiem…,* op. cit., s. 53.

i pasywów oraz przychodów i kosztów wyrażonych w walucie obcej, wystąpi różnica, powodująca powstanie zysku lub straty. Międzynarodowe standardy rachunkowości określają podstawowe metody ujmowania zmian wartości aktywów i pasywów, wynikających ze zmian poziomu kursów walutowych, w których są denominowane. Jest to metoda aktywów bieżących, metoda aktywów pieniężnych/niepieniężnych, metoda kursów bieżących[15]. Ryzyko przeliczeniowe występuje w aktywach i pasywach zagranicznych w sytuacji, gdy występuje przeliczenie środków trwałych, zapasów, należności lub kredytów denominowanych w obcej walucie na walutę krajową. W wyniku finansowym istnieje konieczność przeliczenia przychodów i kosztów zagranicznych jednostek zależnych do konsolidacji sprawozdań. Kapitały własne mogą ulec zmianie ze względu na zmiany kursów walutowych.

Pojęcie ryzyka zmian kursu walutowego rozumie się jako ryzyko zmiany przeliczonej na walutę krajową kwoty należności lub zobowiązań, która była ustalona w walucie obcej, w wyniku zmiany kursu waluty obcej w stosunku do waluty krajowej. Jest to prawdopodobieństwo pogorszenia sytuacji finansowej danego podmiotu na skutek nieprzewidzianej zmiany kursu walutowego[16]. Jednak w pewnych sytuacjach zmiany kursu mogą również przynieść korzyści finansowe i poprawić sytuację ekonomiczną podmiotu.

Ryzyko kursowe zależy od stopnia zmienności kursów walutowych – im większa zmienność, tym większe ryzyko. Ryzyko zmian kursu walutowego mierzy się jako odchylenie od parytetu siły nabywczej[17].

2. Analiza kursów walutowych

2.1. Metodologia badań

Dane empiryczne wykorzystane w badaniu pochodzą z Narodowego Banku Polskiego (NBP), który publikuje oficjalne średnie kursy walut obcych. Analizie poddano średnie kursy walut euro (EUR/PLN) oraz dolara amerykańskiego (USD/PLN). Zakres czasowy badania obejmuje lata 2020-2025. Pozwala to na określenie zmienności kursów walutowych w okresie istotnych wydarzeń gospodarczych takich jak pandemia COVID-19, wzrost inflacji czy napięcia geopolityczne. W badaniu wykorzystano miesięczne średnie kursy EUR/PLN i USD/PLN w latach 2020-2025, pobrane z oficjalnych danych NBP. Kursy wyrażają wartość w złotych polskich za jednostkę waluty obcej. Wykorzystanie danych miesięcznych ma na celu identyfikację trendów długookresowych oraz ograniczenie wpływu krótkookresowych wahań losowych.

---

[15] M. Sołtysiak, *Rynek walutowy – pojęcia…,* op. cit., s. 56-58.

[16] T. Krayenbuehl, *Cross-Border Exposures and Country Risk*, Woodhead, New York, 2001, s. 36-37.

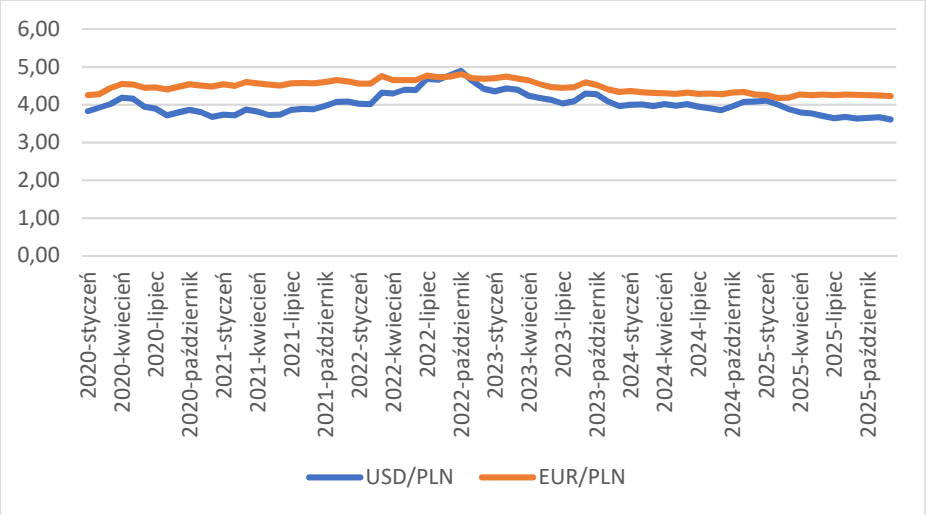
[17] K. Ahmady, *A Peace-Oriented Investigation of the Ethnic Identity Challenge in Iran (A Study of Five Iranian Ethnic Groups with the GT Method),* International Journal of Kurdish Studies, Turkey, 2022, s. 497.

Analiza zmienności kursów walutowych została przeprowadzona z wykorzystaniem podstawowych miar statystycznych oraz metod analizy zależności. Zastosowane metody obejmują: średnią arytmetyczną, medianę, wariancję, odchylenie standardowe, wskaźnik zmienności oraz współczynnik korelacji liniowej Pearsona.

2.2. Analiza poziomu kursów walutowych

Analiza poziomu kursów walutowych pozwala określić średni poziom kursu, jego medianę oraz zakres wahań w danym okresie. Określa kształtowanie się kursów USD/PLN i EUR/PLN w Polsce w latach 2020-2025. Badanie poziomu kursów walutowych umożliwia porównanie wartości obu walut w czasie, wskazanie okresów najwyższych oraz najniższych kursów oraz obserwację trendów rocznych i sezonowych.

Poniższy wykres zestawia średnie miesięczne kursy USD/PLN i EUR/PLN w Polsce w latach 2020-2025. Dane pochodzą z Narodowego Banku Polskiego.



Rys. 1. Średnie miesięczne kursy USD/PLN oraz EUR/PLN w latach 2020-2025
Źródło: Opracowanie własne na podstawie danych pochodzących ze strony https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025]

W latach 2020-2021 kursy obu walut były stosunkowo stabilne z niewielkim wzrostem w pierwszych miesiącach 2020 roku. USD/PLN wahał się w przedziale 3,68-4,19, natomiast EUR/PLN w przedziale 4,25-4,55. Zauważalny jest delikatny wzrost kursów w 2021 roku. W roku 2022 wystąpiły największe wahania oraz najwyższe wartości kursów w całym analizowanym okresie. USD/PLN osiągnął maksimum 4,89 w październiku 2022 roku, a EUR/PLN 4,81 w tym samym miesiącu. Wzrostu kursów walutowych może być spowodowany globalną niepewnością rynków oraz zwiększoną zmiennością walutową. W roku 2023 kursy wykazują

stopniowy spadek po ekstremach z 2022 roku, z okresowymi wahaniami w poszczególnych miesiącach. USD/PLN i EUR/PLN utrzymują się na średnim poziomie odpowiednio 4,2 i 4,54. W latach 2024-2025 obserwuje się tendencję spadkową kursu obydwu walut. USD/PLN spada do poziomu 3,61 w grudniu 2025 roku, natomiast EUR/PLN osiąga 4,23. Spadek kursów wskazuje na stabilizację po okresach wyraźnej zmienności w 2022 i 2023 roku.

Kurs USD/PLN jest bardziej zmienny niż EUR/PLN. Wykazuje wyraźniejsze wahania miesięczne oraz większe rozbieżności między minimalnymi oraz maksymalnymi wartościami w ciągu roku. EUR/PLN jest bardziej stabilny pomimo najwyższych wartości w 2022 roku. Obie waluty wykazują podobne trendy kierunkowe, co wskazuje na częściową synchronizację kursów w poszczególnych miesiącach.

W analizowanych latach kursy USD/PLN i EUR/PLN wykazują krótkoterminowe wahania, spadki w pierwszych miesiącach roku i wzrosty w drugiej połowie roku. Może być to związane z wynikiem czynników politycznych, gospodarczych lub wydarzeń globalnych, które mają wpływ na rynek walutowy.

Tabela 3 przedstawia zestawienie średniej arytmetycznej, mediany, wartości minimalne oraz maksymalne kursu dolara amerykańskiego względem złotego w latach 2020-2025. Są to roczne wartości.

Tabela 3. Roczne wartości kursu USD/PLN w latach 2020-2025

USD/PLN	2020	2021	2022	2023	2024	2025
Średnia arytmetyczna	3,90	3,86	4,46	4,20	3,98	3,76
Mediana	3,88	3,86	4,41	4,21	3,98	3,69
Min	3,68	3,72	4,02	3,97	3,85	3,61
Max	4,19	4,08	4,89	4,43	4,08	4,11

Źródło: Opracowanie własne na podstawie danych pochodzących ze strony https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025]

Średnia arytmetyczna oraz mediana pokazują ogólny poziom kursu USD/PLN w danym roku. W latach 2020-2021 kurs utrzymywał się w okolicach 3,86-3,90 co wskazuje na względną stabilność. W 2022 roku nastąpił gwałtowny wzrost średniego kursu do 4,46, a mediana wyniosła 4,41. Wartości minimalne i maksymalne wykazują zakres wahań kursów w poszczególnych latach. Największe wahania zanotowano w 2022 roku, gdzie wartość minimalna osiągnęła 4,02, a wartość maksymalna 4,89. Najbardziej stabilny był 2021 rok, w którym kursy mieściły się w przedziale 3,72-4,08. W latach 2024-2025 kurs USD/PLN wykazuje tendencję spadkową, osiągając najniższe średnie w całym okresie (4,76 w 2025 roku).

Tabela 4 prezentuje roczne zestawienie wartości kursu EUR/PLN w latach 2020-2025. W 2022 roku odnotowano najwyższy poziom kursów i największą zmienność EUR/PLN.

Tabbela 4. Roczne wartości kursu EUR/PLN w latach 2020-2025

EUR/PLN	2020	2021	2022	2023	2024	2025
Średnia arytmetyczna	4,44	4,57	4,69	4,54	4,31	4,24
Mediana	4,46	4,57	4,69	4,53	4,31	4,25
Min	4,25	4,50	4,55	4,33	4,27	4,18
Max	4,55	4,65	4,81	4,74	4,37	4,27

Źródło: Opracowanie własne na podstawie danych pochodzących ze strony https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025]

Średnia arytmetyczna i mediana kursu EUR/PLN pokazują trend stopniowego wzrostu od 2020 do 2022 roku. W 2022 roku odnotowano największą wartość średniej (4,69) oraz mediany (4,69). Wartości minimalne i maksymalne wskazują na zakres wahań kursu. W 2022 roku kurs EUR/PLN wahał się pomiędzy 4,55 a 4,81, co czyniło ten rok najbardziej dynamicznym pod względem zmienności. Od 2023 roku kurs EUR/PLN wykazuje tendencję spadkową, z najniższym poziomem średniej w 2025 r. (4,24).

Porównując EUR/PLN z USD/PLN, można zauważyć, że EUR/PLN jest bardziej stabilny i posiada mniejsze wahania w porównaniu do USD/PLN. Wskazuje to na wyższe ryzyko walutowe dolara.

2.3. Analiza zmienności kursów walutowych

Rynek walutowy charakteryzuje się wysoką dynamiką oraz wrażliwością na czynniki polityczne, makroekonomiczne oraz globalne. Analiza zmienności kursów walutowych stanowi jedno z kluczowych zagadnień analizy finansowej. Wpływa na decyzje inwestorów oraz reszty przedsiębiorstw prowadzących działalność międzynarodową oraz stabilność gospodarek narodowych. Analiza zmienności kursów walutowych pozwoli na ocenę stopnia ryzyka związanego z daną walutą. Im większa zmienność kursu walutowego, tym większa niepewność co do przyszłej wartości waluty. Prowadzi to do wyższego ryzyka walutowego.

Do obliczeń wykorzystano średnie arytmetyczne kursów miesięcznych USD/PLN i EUR/PLN dla lat 2020-2025. Tabela 5 przedstawia średnie z lat 2020-2025 USD/PLN i EUR/PLN wraz z odchyleniami standardowymi.

Tabela 5. Wyszczególnione dane kursów USD/PLN i EUR/PLN w latach 2020-2025

	USD/PLN	EUR/PLN
Średnia	4,03	4,46
Odchylenie stand.	0,26	0,17

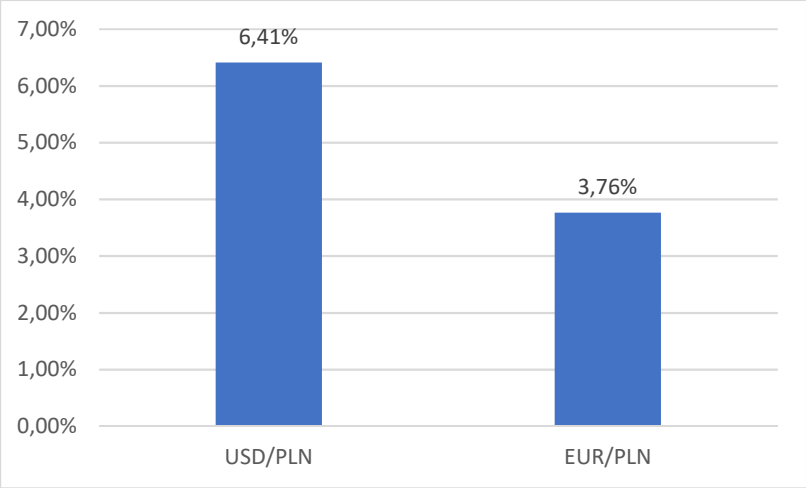
Źródło: Opracowanie własne na podstawie danych pochodzących ze strony https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025]

Odchylenie standardowe określa, jak poszczególne obserwacje odbiegają od średniej arytmetycznej. Im wyższa wartość odchylenia standardowego, tym większa zmienność

kursu walutowego i wyższe ryzyko. Zmienność kursów obliczono bezpośrednio z poziomów kursów walut, co pozwala uzyskać obraz rocznych wahań nominalnych. Jest to podejście uproszczone stosowane w analizach makroekonomicznych i zestawieniach statystycznych NBP. Średnia arytmetyczna kursu USD/PLN w latach 2020-2025 wynosi 4,03, a odchylenie standardowe 0,26. Oznacza to, że większość rocznych średnich kursów USD/PLN w latach 2020-2025 mieści się w przedziale między 3,77 a 4,29. Średnia arytmetyczna kursu EUR/PLN w latach 2020-2025 wynosi 4,46, a odchylenie standardowe 0,17. Oznacza to, że większość rocznych średnich kursów EUR/PLN w latach 2020-2025 mieści się w przedziale między 4,3 a 4,63. Zmienność jest mniejsza w przypadku EUR/PLN.

Kurs dolara wobec złotego cechował się relatywnie dużą zmiennością, większą od kursu euro wobec złotego. Oznacza to większe ryzyko walutowe i mniejszą stabilność. Przedsiębiorstwa i inwestorzy musieli zachować większą ostrożność przy transakcjach w dolarach niż w euro.

Rysunek 2 przedstawia współczynnik zmienności USD/PLN i EUR/PLN w Polsce w latach 2020-2025. Obliczony na podstawie średnich danych rocznych.



Rys. 2. Współczynnik zmienności kursów USD/PLN oraz EUR/PLN w latach 2020-2025

Źródło: Opracowanie własne na podstawie danych pochodzących ze strony https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025]

Współczynnik zmienności kursów walutowych jest relacją odchylenia standardowego do średniej. Zmienność względna kursu USD/PLN jest niemal dwukrotnie wyższa niż EUR/PLN. Współczynnik zmienności dolara względem złotego wynosi 6,41%, a euro względem złotego 3,76%. Oznacza to, że dolar amerykański był walutą bardziej ryzykowną i mniej stabilną w analizowanym okresie. Duże wahania wartości dolara mogły być spowodowane pandemią COVID-19, w trakcie której dolar pełnił rolę waluty

wyjścia z rynku, podczas gdy euro pozostawało relatywnie bardziej stabilne. Mogło być to spowodowane również wojną na Ukrainie, gdzie dolar silnie oddziaływał na globalne zmiany w rynkach finansowych, a euro było mniej wrażliwe, ponieważ Polska utrzymuje silne powiązania gospodarcze z Unią Europejską. Dodatkowo rynek USD/PLN jest bardziej podatny na spekulacje krótkoterminowe, ponieważ dolar jest globalną walutą. Euro jest często używane w transakcjach handlowych między Polską a Unią Europejską stąd przepływy charakteryzują się mniejszą zmiennością.

Do analizy korelacji kursów USD/PLN i EUR/PLN zastosowano współczynnik korelacji Pearsona. Współczynnik ten określa poziom zależności liniowej między zmiennymi losowymi[18]. Pozwala to na określenie w jakim stopniu zmiany jednego kursu są powiązane ze zmianami drugiego. Współczynnik korelacji Pearsona został obliczony na podstawie średnich rocznych kursów USD/PLN i EUR/PLN w latach 2020-2025. Wynosi on 0,75. Oznacza to, że między kursami USD/PLN i EUR/PLN występuje silna dodatnia korelacja. W analizowanym okresie wzrostom lub spadkom kursu dolara wobec złotego zwykle towarzyszyły podobne zmiany kursu euro wobec złotego. Obie waluty reagują na podobne czynniki makroekonomiczne wpływające na wartość złotego. Korelacja liczona na średnich rocznych kursach wskazuje na zależność długoterminową między walutami, korelacja miesięczna mogłaby ujawnić dodatkowe krótkoterminowe wahania. W niniejszej pracy skupiono się na ujęciu rocznym w celu analizy trendów makroekonomicznych.

Podsumowanie

Analiza kursów walutowych pokazuje złożoność rynku finansowego. Podlega on wpływom wielu czynników zarówno krajowych, jak i zagranicznych. Nawet pozornie stabilne waluty mogą doświadczać okresowych wahań. Zrozumienie mechanizmów kształtujących kursy walutowe pozwala na lepsze ocenienie ryzyka i podejmowanie racjonalnych decyzji ekonomicznych.

Analiza zmienności kursów walutowych USD/PLN i EUR/PLN wykazała, że kurs USD/PLN był bardziej zmienny niż EUR/PLN. Odchylenie standardowe dla dolara wynosiło 0,26, podczas gdy dla euro wynosiło 0,17. Oznacza to, że przeciętne roczne wahania kursu dolara wokół średniej wynosiły około +-0,26 zł, a euro +-0,17 zł. Najwyższą zmienność odnotowano w przypadku USD/PLN w 2022 roku, a dla EUR/PLN w 2023 roku. W porównaniu do dolara te wahania były stosunkowo niewielkie. Wyższa zmienność USD/PLN w analizowanym okresie może wynikać z globalnych czynników takich jak: decyzje amerykańskiego banku centralnego w sprawie stóp procentowych, reakcje inwestorów na sytuację makroekonomiczną w Stanach Zjednoczonych, kryzys pandemiczny COVID-19 czy napięciami geopolitycznymi. Stosunkowo stabilny kurs EUR/PLN wynikał z przewidywanych wymian handlowych Polski a Unią Europejską oraz łagodniejszą polityką Europejskiego Banku Centralnego.

[18] Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3033,pojecie.html [dostęp: 24.12.2025].

Bibliografia

1. Ahmady K., *A Peace-Oriented Investigation of the Ethnic Identity Challenge in Iran (A Study of Five Iranian Ethnic Groups with the GT Method),* International Journal of Kurdish Studies, Turkey, 2022.
2. Bartov E., Bodnar G.M., *Firm Valuation, Earnings Expectations, and the Exchange-Rate Exposure Effect, „The Journal of Finance"*, 1994, No. 5.
3. Bożyk P., Misala J., Puławski M., *Międzynarodowe stosunki ekonomiczne*, PWE, Warszawa 1999.
4. Chrzan M., *Polityka kursu walutowego w Polsce w kontekście wejścia do strefy euro*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" nr 132, Wrocław 2010.
5. Drabowski E., *Teorie kursu walutowego, wydanie II zmienione*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1985.
6. Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3033,pojecie.html [dostęp: 24.12.2025].
7. Infor.pl, https://www.infor.pl/slownik/biznes/5805933,waluta.html [dostęp: 24.12.2025].
8. Iwaszczuk N., *Ryzyko w działalności gospodarczej: definicje, klasyfikacje, zarządzanie,* Wydawnictwo IGSMiE PAN, Kraków 2021.
9. Jabłoński M., Kalicki K., *Rynek walutowy. Odesłania do tabel kursowych,* Wydawnictwo SCHOLAR, 2024.
10. Janicka M., *Międzynarodowe przepływy inwestycji. Zarys teorii i praktyki na tle ewolucji międzynarodowego systemu walutowego,* Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2022.
11. Krayenbuehl T., *Cross-Border Exposures and Country Risk*, Woodhead, New York 2001.
12. Misztal P., *Zabezpieczenia przed ryzykiem zmian kursu walutowego*, Wydawnictwo Difin, Warszawa 2004.
13. Narodowy Bank Polski, https://nbp.pl/statystyka-i-sprawozdawczosc/kursy/archiwum-tabela-a-csv-xls/ [dostęp: 24.12.2025].
14. Siwior P., Dobrzycka A., *Przejście Polski z kursu sztywnego na kurs płynny złotego – perspektywa prawno-ekonomiczna,* „Studia Prawnoustrojowe", 2025.
15. Słownik Języka Polskiego, *Waluta*, https://sjp.pl/waluta [dostęp: 24.12.2025].
16. Ślusarczyk R., *Polityka bilansu banku centralnego a kurs walutowy,* Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2018.
17. Sołtysiak M., *Rynek walutowy – pojęcia i ćwiczenia*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2020.
18. Zaleska M., *Podstawy biznesu: zarządzania i finansów – dla nauczycieli,* Wydawnictwo Difin, Warszawa 2023.

ANALYSIS OF EXCHANGE RATE VOLATILITY IN POLAND BETWEEN 2020 AND 2025: THE CASE OF EUR/PLN AND USD/PLN

Abstract

This article presents a study on the fluctuations of the EUR/PLN and USD/PLN exchange rates in Poland between 2020 and 2025 using calculations of the average rate, median, variance, standard deviation, volatility index, and correlation of exchange rates. It explains what currency, exchange rate, and currency risk are. Factors influencing the determination of the exchange rate are also identified.

Keywords: currency, exchange rate, floating exchange rate, fixed exchange rate, crawling peg, volatility index, inflation, COVID-19 pandemic, EUR/PLN, USD/PLN.

Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
DOI https://doi.org/10.24136/sepia.2025.023

Beata Siczek[1]

ANALIZA RYNKU UBEZPIECZEŃ NA ŻYCIE W POLSCE W LATACH 2019-2023

Streszczenie

Celem artykułu jest analiza rynku ubezpieczeń na życie w Polsce w latach 2019-2023. W części teoretycznej omówiono definicję, cechy oraz funkcję ubezpieczeń na życie, a także charakterystykę najważniejszych produktów, takich jak ubezpieczenia klasyczne, rentowe oraz ubezpieczenia związane z ubezpieczeniowym funduszem kapitałowym. W części empirycznej przeprowadzono analizę danych statystycznych dotyczących rynku ubezpieczeń na życie w Polsce, w szczególności wartości składki przypisanej brutto, wypłaconych świadczeń i odszkodowań, kosztów działalności ubezpieczeniowej, lokat oraz wyników finansowych zakładów ubezpieczeń. Do oceny zmienności danych wykorzystano podstawowe miary statystyczne, takie jak średnia arytmetyczna, odchylenie standardowe oraz współczynnik skośności. Przeprowadzona analiza wykazała, że w badanym okresie rynek ubezpieczeń na życie w Polsce podlegał znacznym zmianom, związanym m.in. z pandemią COVID-19 oraz sytuacją gospodarczą. Pomimo okresowych spadków wyników finansowych, sektor ten zachował stabilność i stopniowo odbudowywał swoją pozycję w kolejnych latach.

Słowa kluczowe: analiza finansowa, rynek ubezpieczeniowy, ubezpieczenia na życie.

Wstęp

Ubezpieczenia na życie stanowią istotny element systemu finansowego oraz ważne narzędzie zabezpieczenia ekonomicznego gospodarstw domowych. Ich podstawową funkcją jest ochrona finansowa ubezpieczonego lub jego bliskich na wypadek zdarzeń losowych, takich jak śmierć, choroba czy trwała niezdolność do pracy. Współcześnie ubezpieczenia na życie pełnią również funkcję oszczędnościową i inwestycyjną, stanowiąc element długoterminowego planowania finansowego.

[1] Studentka kierunku finanse i rachunkowość – studia II stopnia, Wydział Ekonomii i Finansów, Uniwersytet Radomski im. Kazimierza Pułaskiego, e-mail: 114092@student.urad.edu.pl.

Znaczenie ubezpieczeń na życie wzrosło szczególnie w ostatnich latach w związku ze zmianami społeczno-ekonomicznymi, takimi jak pandemia COVID-19, wzrost inflacji oraz zmiany demograficzne. Czynniki te wpłynęły na funkcjonowanie rynku ubezpieczeniowego oraz na poziom zainteresowania ochroną ubezpieczeniową. Celem artykułu jest analiza rynku ubezpieczeń na życie w Polsce w latach 2019-2023 ze szczególnym uwzględnieniem jego struktury, dynamiki oraz wyników finansowych zakładów ubezpieczeń. W opracowaniu przedstawiono podstawowe zagadnienia teoretyczne dotyczące ubezpieczeń na życie, charakterystykę głównych produktów oraz analizę wybranych wskaźników ekonomicznych, takich jak składka przypisana brutto, wypłacone świadczenia, koszty działalności oraz wyniki finansowe. W pracy wykorzystano literaturę z zakresu finansów i ubezpieczeń, akty prawne regulujące działalność ubezpieczeniową oraz dane statystyczne publikowane przez Polską Izbę Ubezpieczeń i Komisję Nadzoru Finansowego.

1. Pojęcie i istota ubezpieczeń na życie

W literaturze przedmiotu występuje wiele definicji ubezpieczenia, jednak większość z nich odnosi się do ubezpieczeń w szerokim znaczeniu, obejmując zarówno ubezpieczenia osobowe, jak i majątkowe. W związku z tym pełne określenie specyfiki ubezpieczeń na życie wymaga interpretacji poszczególnych elementów zawartych w tych definicjach.

Według E. Stroińskiego ubezpieczenie na życie jest instrumentem rozłożenia skutków finansowych ryzyka, które może wystąpić u niektórych osób, lecz zagraża wszystkim ubezpieczonym, a jednocześnie stanowi narzędzie przemieszczania w czasie oraz pomnażania środków finansowych osób zawierających umowę ubezpieczenia. Definicja ta podkreśla zarówno ochronny, jak i oszczędnościowy charakter ubezpieczeń na życie[2].

Z prawnego punktu widzenia istota ubezpieczenia wynika z umowy ubezpieczenia. Zgodnie z art. 805 § 1 Kodeksu cywilnego ubezpieczyciel zobowiązuje się do spełnienia określonego świadczenia w przypadku zajścia zdarzenia przewidzianego w umowie, natomiast ubezpieczający zobowiązuje się do opłacania składki[3]. W ubezpieczeniach na życie świadczenie polega najczęściej na wypłacie sumy pieniężnej, renty lub innego świadczenia w razie śmierci ubezpieczonego, dożycia określonego wieku albo wystąpienia innych zdarzeń przewidzianych w umowie[4]. Stronami umowy są ubezpieczyciel oraz ubezpieczający, natomiast w przypadku ubezpieczeń na wypadek śmierci występuje także uposażony, czyli osoba uprawniona do otrzymania świadczenia[5].

[2] E. Stroiński, *Ubezpieczenia na życie. Teoria i praktyka*, Poltext, Warszawa 2003, s. 17-18.
[3] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 1964 r. nr 16, poz. 93, art. 805 §1).
[4] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 1964 r. nr 16, poz. 93, art. 805 §2).
[5] E. Kucka, *Ubezpieczenia gospodarcze i społeczne*, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, Olsztyn 2009, s. 311.

Ubezpieczenia na życie spełniają podstawowe funkcje charakterystyczne dla ubezpieczeń gospodarczych. Najważniejszą z nich jest funkcja ochronna, polegająca na zapewnieniu wsparcia finansowego w przypadku wystąpienia zdarzenia losowego. Drugą istotną funkcją jest funkcja prewencyjna, której celem jest ograniczanie ryzyka poprzez odpowiednie regulacje prawne, warunki umowy oraz ocenę ryzyka przed zawarciem ubezpieczenia. Trzecią funkcją jest funkcja akumulacji kapitału, polegająca na gromadzeniu środków finansowych ze składek ubezpieczeniowych oraz ich inwestowaniu przez zakłady ubezpieczeń w celu zapewnienia możliwości wypłaty świadczeń w przyszłości[6].

Ubezpieczenia na życie mogą mieć charakter ochronny, oszczędnościowy lub mieszany. Ubezpieczenia ochronne zapewniają wypłatę świadczenia w przypadku wystąpienia określonego zdarzenia, natomiast ubezpieczenia oszczędnościowe i mieszane oprócz funkcji ochronnej umożliwiają także gromadzenie kapitału i jego wykorzystanie w przyszłości. Dzięki temu ubezpieczenia na życie stanowią ważny element systemu finansowego oraz istotne narzędzie zabezpieczenia ekonomicznego gospodarstw domowych[7].

2. Podstawowe produkty ubezpieczeń na życie

Ubezpieczenia na życie, zaliczane są do działu I według załącznika do ustawy o działalności ubezpieczeniowej. Obejmują szeroki zakres produktów o charakterze ochronnym, oszczędnościowym oraz inwestycyjnym[8]. Ich zróżnicowanie wynika z odmiennych potrzeb ubezpieczających, którzy oczekują zarówno zabezpieczenia finansowego w przypadku zdarzeń losowych, jak i możliwości gromadzenia kapitału w długim okresie.

Do podstawowych form ubezpieczeń na życie zalicza się ubezpieczenia klasyczne, ubezpieczenia posagowe, ubezpieczenia z ubezpieczeniowym funduszem kapitałowym, ubezpieczenia rentowe, a także ubezpieczenia chorobowe i wypadkowe oraz grupowe.

Do grupy ubezpieczeń klasycznych należą przede wszystkim ubezpieczenia na całe życie, ubezpieczenia terminowe, ubezpieczenia na dożycie oraz ubezpieczenia mieszane. Ubezpieczenie na całe życie zapewnia ochronę od momentu zawarcia umowy aż do śmierci ubezpieczonego, a świadczenie wypłacane jest osobie uposażonej

---

[6] M. Szczepańska, *Ubezpieczenia na życie. Aspekty prawne*, Oficyna, Warszawa 2008, s. 24. Zob też: S. Bukowski, M. Lament, *Market structure and financial effectiveness of life insurance companies,* European Research Studies Journal, 2021, 24(2B), 502-514, M. Lament, S. Bukowski, *Business model impact on the financial efficiency of insurance companies,* European Research Studies Journal, 2021, 24(s4), 237-247.

[7] E. Stroiński, *Ubezpieczenia na życie...*, op. cit., s. 31.

[8] Załącznik do ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, Dz.U. z 2024 r. poz. 000.

wskazanej w umowie. Produkty te często łączą funkcję ochronną z możliwością gromadzenia kapitału, ponieważ część składki może być przeznaczona na tworzenie wartości wykupu[9].

Ubezpieczenie terminowe zapewnia ochronę przez określony czas, wskazany w umowie. Świadczenie wypłacane jest jedynie w przypadku śmierci ubezpieczonego w okresie trwania ochrony. Tego rodzaju ubezpieczenia mają zazwyczaj charakter ochronny i charakteryzują się niższą składką w porównaniu z ubezpieczeniami o charakterze oszczędnościowym. Są one często wykorzystywane jako zabezpieczenie kredytów lub zobowiązań finansowych[10].

Ubezpieczenie na dożycie ma przede wszystkim charakter oszczędnościowy i polega na wypłacie określonej sumy pieniężnej po upływie ustalonego okresu lub po osiągnięciu przez ubezpieczonego określonego wieku. W przypadku śmierci ubezpieczonego w trakcie trwania umowy świadczenie może być wypłacone osobie uposażonej lub umowa może wygasnąć, w zależności od warunków kontraktu[11]. Połączeniem funkcji ochronnej i oszczędnościowej jest ubezpieczenie mieszane, w którym świadczenie wypłacane jest zarówno w przypadku śmierci ubezpieczonego w trakcie trwania umowy, jak i w razie dożycia końca okresu ubezpieczenia. Produkty te należą do najbardziej rozpowszechnionych form ubezpieczeń na życie[12].

Można również wyróżnić ubezpieczenia posagowe i zaopatrzeniowe dzieci, które mają charakter oszczędnościowo-ochronny. Celem tych ubezpieczeń jest zgromadzenie środków finansowych przeznaczonych na przyszłe potrzeby dziecka, takie jak edukacja, rozpoczęcie samodzielnego życia czy zabezpieczenie materialne po osiągnięciu pełnoletności. W tego rodzaju ubezpieczeniach osoba dorosła zawiera umowę na rzecz dziecka i opłaca składki przez określony czas, natomiast wypłata świadczenia następuje po osiągnięciu przez dziecko ustalonego wieku lub po upływie okresu wskazanego w umowie[13]. Ubezpieczenia posagowe i zaopatrzeniowe mogą również zawierać element ochronny, polegający na przejęciu obowiązku opłacania składek przez zakład ubezpieczeń w przypadku śmierci lub trwałej niezdolności do pracy osoby opłacającej składkę. Dzięki temu zapewniona jest ciągłość gromadzenia kapitału, a dziecko otrzymuje świadczenie niezależnie od zdarzeń losowych dotyczących ubezpieczającego. Produkty tego typu łączą funkcję ochronną z funkcją

---

9 M. Szczepańska, *Ubezpieczenia na życie…*, op. cit., s. 255-256.

10 P. Lizak*, Ubezpieczenia na życie. Zarys charakterystyki umów ubezpieczenia na życie*, KNF, Warszawa 2022, s. 10.

11 A. Olearczuk, *Tradycyjne ubezpieczenia indywidualne*, [w:] O. Doan (red.), *Ubezpieczenia życiowe*, Poltext, Warszawa 1996, s. 66-67.

12 P. Lizak*, Ubezpieczenia na życie…*, op. cit., s. 29.

13 Z. Biskupski, *Ubezpieczenia emerytalne i na życie. Część 2*, Gazeta Ubezpieczeniowa 2003, nr 36, s. 16

długoterminowego oszczędzania i stanowią szczególną formę zabezpieczenia finansowego rodziny[14].

Szczególną kategorię stanowią ubezpieczenia na życie związane z ubezpieczeniowym funduszem kapitałowym, określane jako unit-linked. W tego rodzaju produktach składka dzielona jest na część przeznaczoną na ochronę ubezpieczeniową oraz część inwestycyjną, lokowaną w wybrane fundusze kapitałowe. Wysokość świadczenia zależy od wartości zgromadzonych jednostek uczestnictwa, co oznacza, że ryzyko inwestycyjne w znacznym stopniu ponosi ubezpieczający. Produkty te charakteryzują się dużą elastycznością, ponieważ umożliwiają zmianę strategii inwestycyjnej w trakcie trwania umowy, jednak ich konstrukcja jest bardziej złożona niż w przypadku tradycyjnych polis[15].

Istotną grupę stanowią także ubezpieczenia rentowe, których celem jest zapewnienie regularnych świadczeń pieniężnych w określonym czasie lub przez całe życie ubezpieczonego, co czyni je ważnym elementem zabezpieczenia dochodów po zakończeniu aktywności zawodowej. W zależności od konstrukcji umowy wyróżnia się renty terminowe oraz renty dożywotnie. Renta terminowa wypłacana jest przez określony czas, natomiast renta dożywotnia zapewnia świadczenie aż do śmierci ubezpieczonego, co oznacza przejęcie przez zakład ubezpieczeń ryzyka długowieczności. Istotne znaczenie ma również moment rozpoczęcia wypłat – renta może mieć charakter natychmiastowy lub odroczony, w którym najpierw następuje okres gromadzenia kapitału. Ze względu na wysokość świadczeń wyróżnia się renty stałe oraz zmienne, dostosowywane do zmian ekonomicznych. Ubezpieczenia rentowe mogą obejmować jedną lub więcej osób, np. w formie renty na dwa życia[16]. W praktyce często zawierają również dodatkowe opcje, takie jak gwarancja minimalnego okresu wypłaty czy zabezpieczenie środków dla uposażonych.

Uzupełnieniem podstawowej ochrony w ubezpieczeniach na życie są ubezpieczenia wypadkowe i chorobowe, które najczęściej występują w formie umów dodatkowych. Ich celem jest rozszerzenie zakresu ochrony o zdarzenia związane ze zdrowiem i zdolnością do pracy ubezpieczonego[17].

Ubezpieczenia wypadkowe obejmują przede wszystkim następstwa nieszczęśliwych wypadków, takie jak trwały uszczerbek na zdrowiu, niezdolność do pracy lub śmierć ubezpieczonego. W przypadku wystąpienia zdarzenia świadczenie wypłacane jest w formie jednorazowej lub jako procent sumy ubezpieczenia, zależny od stopnia uszczerbku na zdrowiu. Zakres ochrony może być zróżnicowany i często uzależniony od przyczyny zdarzenia oraz okoliczności jego powstania.

---

[14] W. Ronka-Chmielowiec, *Ubezpieczenia*, C.H. Beck, Warszawa 2016, s. 307-309.

[15] M. Szczepańska, *Charakter prawny ubezpieczenia na życie z ubezpieczeniowym funduszem kapitałowym,* „Wiadomości Ubezpieczeniowe" 2005, nr 5-6, s. 4.

[16] E. Kucka, *Ubezpieczenia gospodarcze*…, op. cit., s. 330-334.

[17] T. Sangowski, *Vademecum pośrednika ubezpieczeniowego*, SAGA Printing, Poznań 1996, s. 204.

Ubezpieczenia chorobowe koncentrują się natomiast na zabezpieczeniu finansowym w przypadku wystąpienia choroby, w szczególności poważnych schorzeń. Obejmują one m.in. wypłatę świadczeń w przypadku diagnozy określonych chorób, pokrycie kosztów leczenia lub rekompensatę utraconych dochodów w wyniku czasowej lub trwałej niezdolności do pracy. Szczególną popularnością cieszą się ubezpieczenia tzw. ciężkich chorób, obejmujące m.in. nowotwory, zawał serca czy udar mózgu[18] . Rozwój tych produktów związany jest ze zmianami demograficznymi oraz rosnącymi kosztami leczenia, co sprawia, że ubezpieczenia wypadkowe i chorobowe odgrywają coraz większą rolę w systemie zabezpieczenia finansowego ludności.

Ubezpieczenia na życie mogą być zawierane w formie indywidualnej lub grupowej, przy czym ubezpieczenia grupowe stanowią istotny segment rynku. Obejmują one większą liczbę osób, najczęściej pracowników przedsiębiorstw lub klientów instytucji finansowych, a umowa zawierana jest pomiędzy zakładem ubezpieczeń a podmiotem organizującym grupę[19]. Charakterystyczną cechą ubezpieczeń grupowych jest uproszczona procedura zawarcia umowy oraz ograniczona indywidualna ocena ryzyka, która często odbywa się na poziomie całej grupy. Dzięki temu możliwe jest objęcie ochroną szerokiego grona osób przy relatywnie niskiej składce. Zakres ochrony w ubezpieczeniach grupowych jest zazwyczaj szeroki i obejmuje nie tylko ryzyko śmierci, ale również zdarzenia takie jak choroba, wypadek czy niezdolność do pracy. Ubezpieczenia te pełnią ważną funkcję zabezpieczenia finansowego, m.in. jako element świadczeń pracowniczych lub zabezpieczenie kredytów[20].

3. Polski rynek ubezpieczeń na życie

3.1. Składka przypisana brutto

Składka przypisana brutto jest to całkowita wartość składek należnych zakładowi ubezpieczeń z tytułu zawartych umów ubezpieczenia w danym okresie, bez potrącania kosztów reasekuracji i innych wydatków. Na wysokość składki wpływa wiele czynników, takich jak wiek i stan zdrowia ubezpieczonego, zakres ochrony, suma ubezpieczenia, okres trwania umowy oraz szereg czynników wewnętrznych wynikających z działalności danego zakładu ubezpieczeń, jak również zewnętrznych (od niego niezależnych). Składka przypisana brutto stanowi jeden z kluczowych wskaźników opisujących dany rynek ubezpieczeń, ponieważ pokazuje całkowity potencjał przychodów z ubezpieczeń i pozwala ocenić wielkość i dynamikę działalności ubezpieczeniowej.

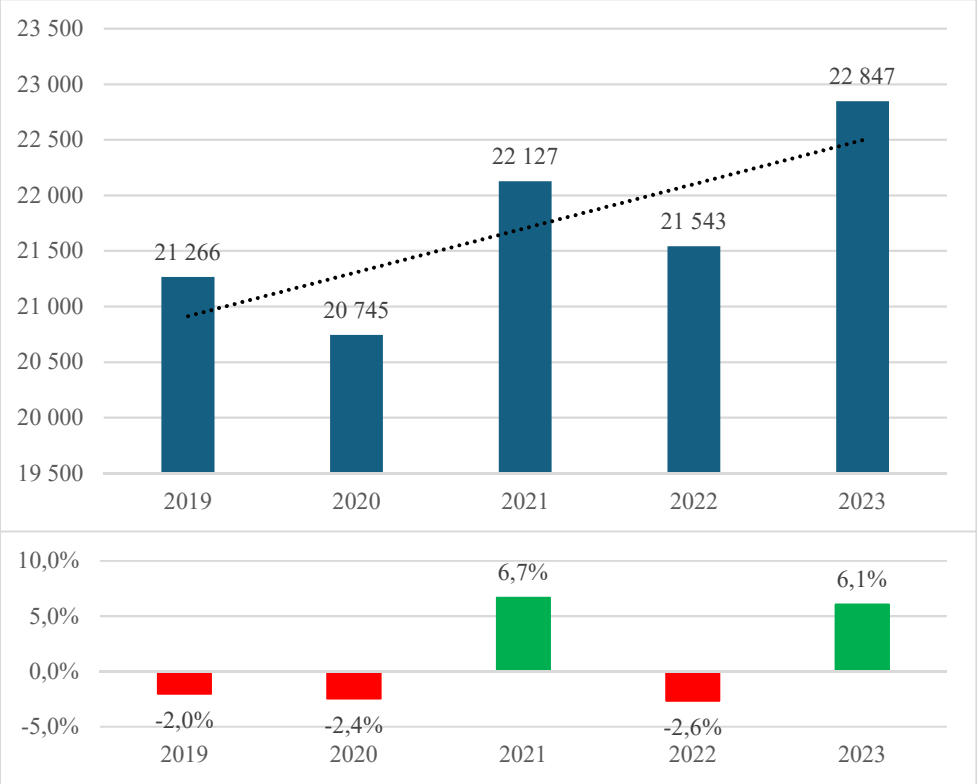
Na rysunku 1 przedstawiono wartość składek przypisanych brutto w segmencie ubezpieczeń na życie w Polsce w latach 2019-2023.

---

[18] E. Kucka, *Ubezpieczenia gospodarcze…*, op. cit., s. 335-337.

[19] J. Handschke, B. Kęszycka, E. Kowalewski, *Problematyka grupowych ubezpieczeń na życie w świetle znowelizowanych przepisów k.c. o umowie ubezpieczenia*, *Spór o intencje ustawodawcy*, „Wiadomości Ubezpieczeniowe" 2007, nr 7-8, s. 3.

[20] E. Kucka, *Ubezpieczenia gospodarcze…*, op. cit., s. 341-343.



Rys. 1. Wartość składki przypisanej brutto (mln zł) i dynamika jej zmian (%) w ubezpieczeniach na życie w latach 2019-2023

Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

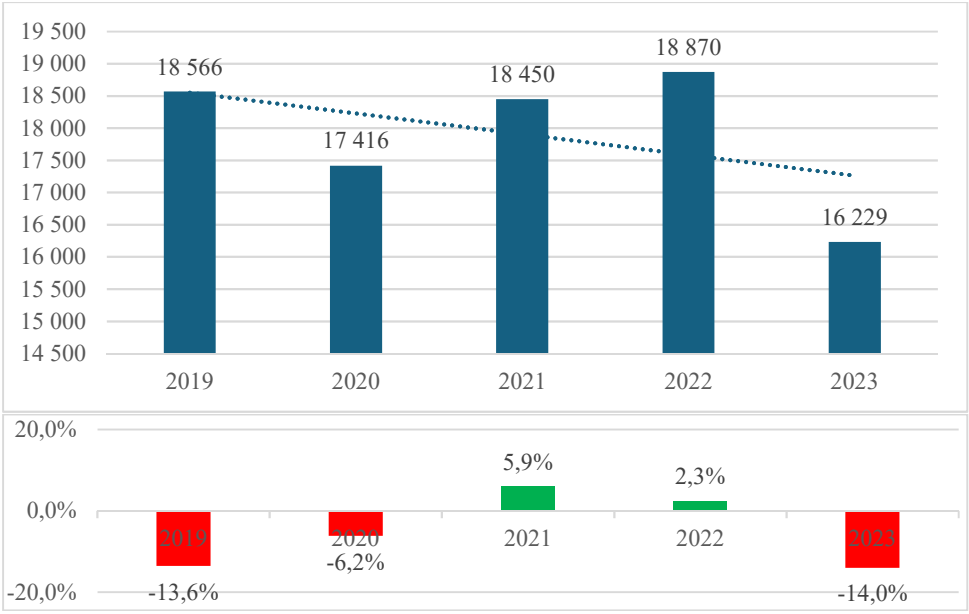
W 2019 roku wartość składki wynosiła 21 266 mln zł, natomiast już w roku 2020 odnotowano jej spadek do poziomu 20 745 mln zł, co stanowiło obniżenie o 2,4%. Spadek ten można powiązać z początkiem pandemii COVID-19, która wpłynęła na ograniczenie aktywności gospodarczej, niepewność finansową gospodarstw domowych oraz zmniejszenie skłonności do zawierania nowych umów ubezpieczeniowych. W roku 2021 nastąpiła istotna poprawa, wartość składki wzrosła do 22 127 mln zł, co przekłada się na wzrost o około 7% w porównaniu z rokiem poprzednim. Może to wskazywać na stopniową odbudowę zaufania do rynku finansowego oraz rosnące zainteresowanie ochroną ubezpieczeniową w obliczu niepewności zdrowotnej, spowodowanej trwającą ówcześnie pandemią. W kolejnym roku składka nieznacznie spadła do poziomu 21 543 mln zł (spadek o 2,6%), co może być wynikiem presji inflacyjnej, zmniejszenia realnych dochodów oraz rosnących kosztów życia, które mogły skłonić część klientów do rezygnacji z ochrony ubezpiecze-

niowej lub jej ograniczenia. Najwyższy poziom składki przypisanej brutto w analizowanym okresie osiągnięto w 2023 roku, wynosił on 22 847 mln zł, co stanowi wzrost o około 6% w stosunku do roku poprzedniego.

3.2. Odszkodowania i świadczenia

Świadczenia w ubezpieczeniach na życie to podstawowe formy wypłat, jakich towarzystwo ubezpieczeniowe dokonuje na rzecz ubezpieczonych lub uposażonych w przypadku zajścia określonego zdarzenia objętego umową ubezpieczenia (np. śmierci, poważnej choroby, inwalidztwa). Wysokość świadczenia w ubezpieczeniach na życie zależy przede wszystkim od sumy ubezpieczenia na jaką została zawarta umowa. Wypłaty z tytułu świadczeń i odszkodowań to jedno z głównych obciążeń finansowych towarzystw ubezpieczeniowych. Im wyższe wypłaty, tym potencjalnie mniejsze zyski dla zakładu ubezpieczeń.

Na rysunku 2 przedstawiono wartość świadczeń wypłaconych brutto w ubezpieczeniach na życie w Polsce w latach 2019-2023.



Rys. 2. Wartość świadczeń wypłaconych brutto (mln zł) i dynamika ich zmian (%) w ubezpieczeniach na życie w latach 2019-2023

Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

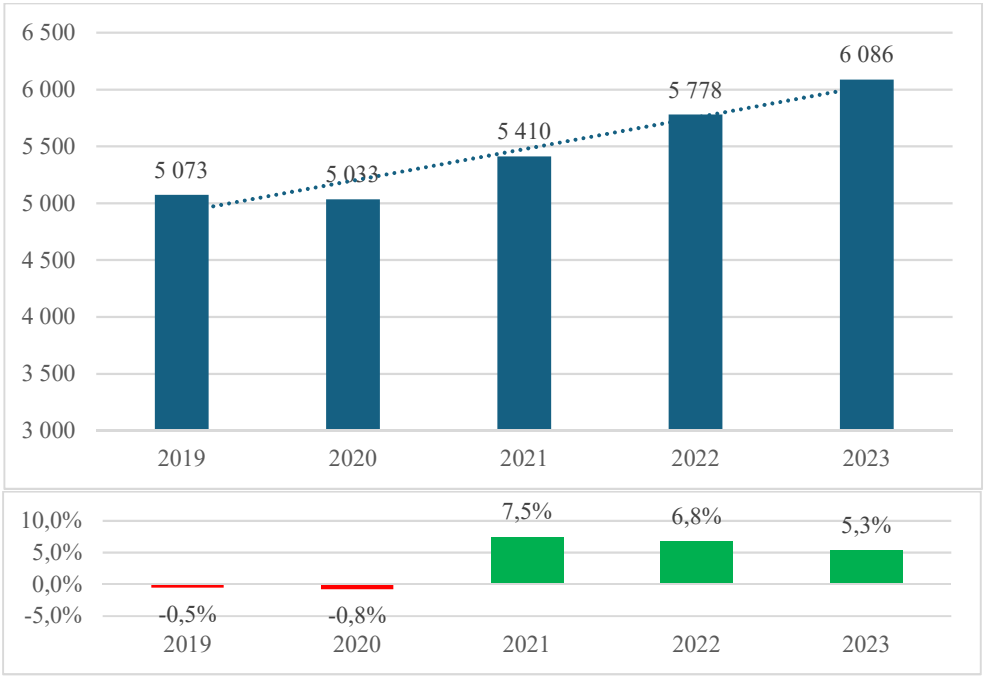
Na podstawie analizy danych z badanego okresu można zauważyć, że najniższą wartość świadczeń wypłaconych brutto zanotowano w 2023 roku, wynosiła ona 16 229 mln zł. Z kolei najwyższy poziom świadczeń przypadł na 2022 rok i wynosił 18 870 mln zł. Średnia roczna wartość tych świadczeń to 17 906 mln zł. Odchylenie

standardowe, wynoszące 1085,5 mln zł, wskazuje, że wartości roczne różniły się od średniej o średnio 1085 mln zł. Wartość współczynnika skośności (-0,8) sugeruje lekką lewostronną asymetrię, co oznacza, że w latach o niższych wartościach (np. 2023 rok) występowały większe odchylenia od średniej niż w latach o wyższych wartościach. W latach 2019-2023 wartość wypłaconych świadczeń brutto w ubezpieczeniach na życie w Polsce podlegała zauważalnym wahaniom, które odzwierciedlają zarówno zmieniające się uwarunkowania makroekonomiczne, jak i wpływ czynników zdrowotno-społecznych oraz regulacyjnych. W 2019 roku wartość wypłat wynosiła 18 566 mln zł, po czym w 2020 roku odnotowano spadek o 6,2% do poziomu 17 416 mln zł. Spadek ten może być powiązany z ograniczeniem aktywności gospodarczej i zmniejszeniem liczby nowo zawieranych umów w wyniku niepewności wywołanej pandemią COVID-19. Względnie niska liczba zgłoszonych roszczeń mogła również wynikać z ograniczonego dostępu do usług medycznych i diagnostyki w pierwszym etapie pandemii. W latach 2021-2020 nastąpił wzrost wartości wypłat odpowiednio o 5,9% i 2,3%. Wzrost ten może być wynikiem odłożonych roszczeń z okresów lockdownów oraz wzrostu liczby zgonów i pogorszeniu stanu zdrowia populacji w wyniku skutków pandemii. Dodatkowo, większa świadomość ryzyka wśród społeczeństwa mogła skutkować częstszym korzystaniem z ochrony ubezpieczeniowej. Rok 2023 przyniósł jednak gwałtowny spadek wartości wypłat o 14%, do poziomu 16 229 mln zł. Prawdopodobnie czynnikiem wpływającym na to zjawisko jest spadek liczby zgonów i hospitalizacji w porównaniu do lat pandemicznych, co skutkuje mniejszą liczbą roszczeń. Mimo krótkoterminowych wahań, rynek ubezpieczeń na życie w Polsce wykazuje tendencję malejącą pod względem wypłat świadczeń. Wpływ na to miały zarówno czynniki zewnętrze, takie jak pandemia i jej konsekwencje zdrowotne oraz gospodarcze, jak i zmiany strukturalne w ofercie produktowej oraz preferencjach konsumentów.

3.3. Koszty działalności ubezpieczeniowej

Koszty działalności ubezpieczeniowej w ubezpieczeniach na życie to ogół wydatków ponoszonych przez zakład ubezpieczeń w związku z prowadzeniem działalności ubezpieczeniowej w tym segmencie. Obejmują one w szczególności koszty pozyskiwania i obsługi umów ubezpieczenia (akwizycji), koszty administracyjne, koszty związane z likwidacją szkód oraz inne koszty operacyjne niezbędne do prawidłowego funkcjonowania przedsiębiorstwa ubezpieczeniowego. Koszty te wpływają bezpośrednio na wynik techniczny ubezpieczeń na życie i są istotnym elementem analizy efektywności działalności ubezpieczeniowej.

Na rysunku 3 przedstawiono wartość kosztów działalności ubezpieczeniowej w segmencie ubezpieczeń na życie w Polsce w latach 2019-2023.



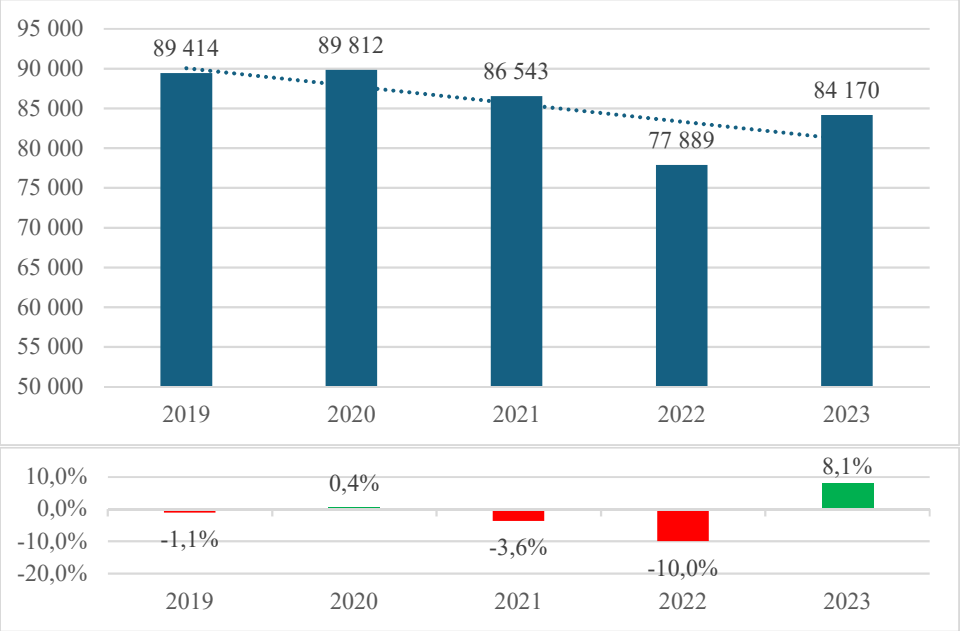
Rys. 3. Wartość kosztów działalności ubezpieczeniowej (mln zł) i dynamika ich zmian (%) w ubezpieczeniach na życie w latach 2019-2023
Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

W latach 2019-2023 wartość kosztów działalności ubezpieczeniowej w ubezpieczeniach na życie wykazywała umiarkowaną tendencję wzrostową. W roku 2019 koszty te wynosiły 5 073 mln zł. W kolejnym roku odnotowano niewielki spadek o 0,8%, co doprowadziło do zmniejszenia wartości do 5 033 mln zł. Wskazany spadek może być związany z efektem pandemii COVID-19, który zmusił zakłady ubezpieczeń do ograniczenia wydatków, w tym wydatków administracyjnych i marketingowych. Od 2021 roku obserwujemy wyraźne odbicie w górę – koszty wzrosły o 7,5% i osiągnęły poziom 5 410 mln zł. Wzrost ten można interpretować jako wynik powrotu rynku do normalnych warunków funkcjonowania po pierwszym szoku pandemicznym, a także rosnącej presji inflacyjnej, która wpływała na wzrost kosztów operacyjnych. Tendencja wzrostowa była kontynuowana w latach następnych. W 2022 roku koszty wynosiły 5 778 mln zł (wzrost o 6,8%), a w 2023 roku osiągnęły 6 086 mln zł (wzrost o 5,3%). Utrzymująca się dynamika wzrostu wskazuje na narastające obciążenia kosztowe w branży, związane m.in. z inflacją, koniecznością inwestycji w cyfryzację obsługi klienta oraz wyższymi kosztami zgodności z regulacjami prawnymi. Widoczna na wykresie linia trendu potwierdza, że mimo krótkoterminowych wahań, koszty działalności w sektorze ubezpieczeń na życie rosną.

3.4. Lokaty

Lokaty w ubezpieczeniach na życie to środki finansowe pochodzące m.in. ze składek ubezpieczeniowych, które zakład ubezpieczeń inwestuje w różne instrumenty finansowe w celu zapewnienia wypłacalności, pokrycia zobowiązań oraz osiągnięcia dodatkowych przychodów. Efektywne zarządzanie lokatami jest kluczowe dla rentowności zakładów ubezpieczeń na życie. Odpowiednio skonstruowany portfel inwestycyjny może nie tylko zwiększać zyskowność, ale też poprawiać płynność, stabilność finansową i konkurencyjność zakładu na rynku.

Na rysunku 4 przedstawiono wartość lokat w segmencie ubezpieczeń na życie w Polsce w latach 2019-2023.



Rys. 4. Wartości lokat (mln zł) i dynamika ich zmian (%) w ubezpieczeniach na życie w latach 2019-2023

Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

Na podstawie analizy danych z badanego okresu można zauważyć, że najniższy poziom wskaźnika odnotowano w 2022 roku i wyniósł on 77 889 mln zł. Z kolei najwyższa wartość miała miejsce w roku 2020, osiągając 89 812 mln zł. Średnia roczna wartość wyniosła 85 566 mln zł. Standardowe odchylenie równe 4865,1 mln zł wskazuje, że roczne wartości odbiegały od średniej o około 4865 mln zł. Ujemny współczynnik skośności (-0,8) świadczy o niewielkiej asymetrii lewostronnej, co sugeruje, że w latach z niższymi wartościami – jak 2022 – obserwowano większe odchylenia od średniej, niż w latach z wyższymi wynikami. Analiza danych pozwala

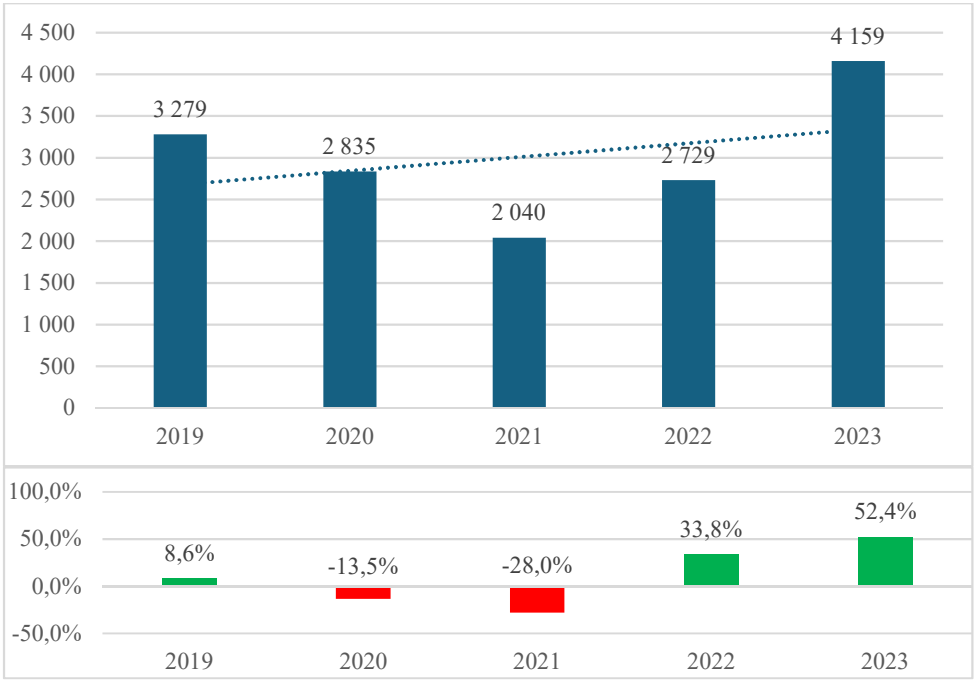
dostrzec istotne wahania w polityce inwestycyjnej zakładów ubezpieczeń, odzwierciedlające zarówno uwarunkowania rynkowe, jak i działania strategiczne podmiotów ubezpieczeniowych. W 2019 roku wartość lokat wynosiła 89 414 mln zł, co stanowiło solidny poziom bazowy dla dalszych obserwacji. W 2020 roku odnotowano nieznaczny wzrost o 0,4%, co może świadczyć o stabilności rynku mimo wybuchu pandemii COVID-19. Rok ten charakteryzował się wysokim poziomem niepewności ekonomicznej. W 2021 roku nastąpił spadek wartości lokat o 3,6%, co można powiązać z utrzymującym się niskim poziomem stóp procentowych oraz presją inflacyjną, wpływającą na realną stopę zwrotu z bezpiecznych instrumentów inwestycyjnych. Tendencja spadkowa pogłębiła się w 2022 roku, kiedy wartość lokat zmniejszyła się o kolejne 10%, osiągając poziom 77 889 mln zł. Rok ten charakteryzował się wysoką inflacją, napięciami geopolitycznymi oraz znaczną zmiennością na rynkach finansowych, co mogło skłonić zakłady ubezpieczeń do zmniejszenia struktury portfela inwestycyjnego lub zwiększenia płynności kosztem inwestycji długoterminowych. W 2023 roku nastąpił istotny wzrost wartości lokat o 8,1%, co pozwoliło osiągnąć poziom 84 170 mln zł. Zmiana ta może być wywołana poprawą warunków rynkowych – stabilizujących się stóp procentowych, zwiększenia rentowności obligacji skarbowych. Można również zakładać, że część podmiotów rozpoczęła proces odbudowy portfeli lokacyjnych.

3.5. Wynik finansowy

Wyniki finansowe w ubezpieczeniach na życie odnoszą się do kondycji ekonomicznej zakładów prowadzących działalność w tym segmencie. Obejmują one zarówno przychody, jak i koszty, a także wynik techniczny osiągany z tytułu prowadzenia działalności ubezpieczeniowej i inwestycyjnej. Wyniki finansowe są kluczowym wskaźnikiem efektywności funkcjonowania zakładów ubezpieczeń oraz ich zdolności do realizacji zobowiązań wobec ubezpieczonych[21]. Dobre wyniki finansowe świadczą o stabilności finansowej towarzystwa, jego zdolności do wypłaty świadczeń oraz możliwości oferowania atrakcyjnych warunków ubezpieczeń. Z kolei negatywne wyniki mogą wynikać m.in. z nieoptymalnej struktury portfela inwestycyjnego, wzrostu szkodowości, nadmiernych kosztów działalności lub niekorzystnych zmian demograficznych (np. starzenia się populacji). W przypadku ubezpieczeń na życie istotnym czynnikiem wpływającym na wynik są także zmiany stóp procentowych, które oddziałują na wartość zobowiązań długoterminowych, rentowność lokat.

Na rysunku 5 przedstawiono wartość wyników finansowych brutto w segmencie ubezpieczeń na życie w Polsce w latach 2019-2023.

[21] M. Lament, J. Piątek, *Rachunkowość zakładów ubezpieczeń i zakładów reasekuracji,* PWN, Warszawa 2023, s. 134.



Rys. 5. Wynik finansowy brutto (mln zł) i dynamika jego zmian (%) w ubezpieczeniach na życie w latach 2019-2923

Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

Z analizy danych za badany okres wynika, że najniższy poziom wyniku finansowego brutto odnotowano w 2021 roku – wyniósł on 2 040 mln zł. Najwyższy wynik osiągnięto natomiast w 2023 roku, kiedy to wyniósł 4 159 mln zł. Średnia roczna wartość kształtowała się na poziomie 3 008 mln zł. Odchylenie standardowe wynoszące 781,5 mln zł oznacza, że roczne wartości przeciętnie odbiegały od średniej o około 781 mln zł. Współczynnik skośności równy (0,4) wskazuje na niewielką asymetrię prawostronną, co sugeruje, że większe odchylenia od średniej występowały w latach z wyższymi wynikami, jak w 2023 roku. Rynek wykazuje wzrost. W latach 2019-2023 sektor ubezpieczeń na życie w Polsce charakteryzował się dużą zmiennością osiąganych wyników. W 2019 roku wartość brutto wyniosła 3 279 mln zł, natomiast w roku kolejnym spadła do poziomu 2 835 mln zł, co oznaczało spadek o 13,5%. Tendencja spadkowa pogłębiła się w 2021 roku, gdy wynik osiągnął najniższy poziom w badanym okresie – 2 040 mln zł, co oznaczało dalszy spadek o 28%. Spadki te można wiązać z niekorzystnymi warunkami gospodarczymi, w tym skutkami pandemii COVID-19, zwiększoną szkodowością oraz niższymi dochodami z działalności lokacyjnej. Począwszy od 2022 roku obserwuje się wyraźną poprawę sytuacji finansowej. Wynik finansowy brutto wzrósł do 2 729 mln zł,

co oznaczało dynamiczny wzrost o 33,8%. Tendencja ta została utrzymana i wzmocniona w 2023 roku, kiedy to sektor osiągnął wartość 4 159 mln zł, co stanowiło wzrost aż o 52,4% względem roku poprzedniego. Tak znacząca poprawa może wynikać z korzystniejszych warunków inwestycyjnych, wzrostu rentowności lokat, lepszej kontroli kosztów operacyjnych oraz odbudowy aktywności gospodarczej po okresie pandemii. Z powyższej analizy wynika, że mimo chwilowego załamania rentowności sektora w latach 2020-2021, zakłady ubezpieczeń na życie skutecznie zareagowały na kryzys i w kolejnych latach wykazały dużą zdolność adaptacyjną, co przełożyło się na odbudowę i umocnienie ich pozycji finansowej.

3.6. Struktura rynku

Struktura rynku w ubezpieczeniach na życie odnosi się do układu i charakterystyki podmiotów działających w tym segmencie sektora finansowego, a także do udziałów rynkowych, form dystrybucji produktów, typów ubezpieczeń oraz tendencji konsumenckich. Rynek ubezpieczeń na życie w Polsce charakteryzuje się dużą koncentracją, co oznacza, że istotna część składki przypisanej brutto skupia się w kilku największych towarzystwach ubezpieczeniowych. Dominującą rolę odgrywają spółki z kapitałem zagranicznym oraz instytucje powiązane z dużymi grupami bankowymi, które dysponują rozbudowanymi kanałami dystrybucji oraz zasobami inwestycyjnymi[22]. Ten kanał sprzedaży stał się kluczowy dla polis inwestycyjnych i oszczędnościowych. Równocześnie obserwuje się spadek liczby indywidualnych agentów ubezpieczeniowych, co wynika z cyfryzacji procesów i rosnącej roli kanałów online. Rynek ten jest regulowany i nadzorowany przez Komisję Nadzoru Finansowego, co zapewnia ochronę interesów konsumentów, a także stabilność finansową sektora.

W tabeli 1 przedstawiono strukturę rynku w segmencie ubezpieczeń na życie w Polsce w latach 2019-2023.

Tabela 1. Struktura rynku (%) w ubezpieczeniach na życie w latach 2019-2023

Zakład ubezpieczeń	2019	2020	2 021	2022	2023
PZU ŻYCIE SA	40,4	42,2	39,8	40,1	40,2
AVIVA ŻYCIE SA	9,1	9,5	9,5	11,8	11,4
NATIONALE NEDERLANDEN SA	7,2	7,9	7,6	7,6	9,8
OPEN LIFE SA	5,2	4,7	5,3	5,5	6,0
WARTA TUnŻ SA	4,6	4,7	4,9	5,2	5,3
COMPENSA ŻYCIE SA	4,2	4,5	4,8	4,6	4,2

[22] M. Lament, S. Bukowski, *Wybrane determinanty rozwoju rynków ubezpieczeniowych krajów Unii Europejskiej w latach 1999-2019,* „Wiadomości Ubezpieczeniowe", 2022, 4, 61-74; M. Lament, B. Jarolímová, *Foreign capital as a determinant of the non-financial reporting development in insurance companies of the Visegrad Group countries,* „Investment Management and Financial Innovations", 2021, 18(1), 203-214.

Cd. Tabeli 1.

Zakład ubezpieczeń	2019	2020	2 021	2022	2023
GENERALI ŻYCIE SA	4,2	3,7	3,7	4,0	4,1
METLIFE TUnŻ SA	4,0	3,4	3,3	2,9	2,6
AXA ŻYCIE SA	3,2	2,9	2,6	2,3	2,4
ALLIANZ ŻYCIE POLSKA SA	2,8	2,2	2,3	2,3	2,3
POZOSTAŁE	15,1	14,1	16,2	13,7	11,8

Źródło: Opracowanie własne na podstawie raportów rocznych Polskiej Izby Ubezpieczeń (2024, 2023, 2022, 2021, 2020)

Struktura rynku ubezpieczeń na życie w Polsce w latach 2019-2023 ukazuje wyraźną dominację kilku kluczowych podmiotów oraz utrzymującą się tendencją do koncentracji rynku. Na podstawie danych z tabeli 1, widoczna jest silna pozycja lidera – PZU Życie SA, którego udział rynkowy nie spadł poniżej 39,8% w żadnym z analizowanych lat. Taki poziom dominacji wskazuje na bardzo wysoki stopień zaufania klientów do największego krajowego ubezpieczyciela, ale też na jego efektywną strategię dystrybucyjną, szeroką ofertę i rozpoznawalną markę. Drugą największą firmą była AVIVA Życie SA, która w latach 2022-2023 po fuzji funkcjonowała już pod marką Allianz Życie. Udział tej firmy wzrósł z 9,1% w 2019 roku do 11,8% w 2022 roku, mimo niewielkiego spadku w 2023 roku do 11,4%. Allianz pozostaje drugą największą firmą w tym sektorze. Nationale Nederlanden SA, jako kolejny kluczowy podmiot, utrzymywał stabilny udział rynkowy (od 7,2% w 2019 roku do 9,8 % w 2023 roku). Pozostali ubezpieczyciele, tacy jak Open Life SA, Warta TUnŻ SA, Compensa Życie SA czy Generali, utrzymywali się na niższych poziomach udziałów rynkowych (od 2% do 6%). Systematyczny spadek obserwowano w kategorii „Pozostałe" – czyli suma udziałów mniejszych towarzystw. Ich łączny udział zmniejszył się z 15,1% w 2019 roku do zaledwie 11,8% w 2023 roku, co wskazuje na rosnącą konsolidację rynku i koncentrację kapitału w rękach największych towarzystw.

Rynek ubezpieczeń na życie w Polsce w analizowanym okresie (2019-2023) cechował się względną stabilnością udziałów największych podmiotów, wśród których dominującą pozycję nieprzerwanie zajmuje PZU Życie SA. Utrzymywanie silnej pozycji przez liderów rynku wpływa nie tylko na układ sił konkurencyjnych, ale również kształtuje ogólne warunki funkcjonowania sektora. Taka koncentracja może ograniczać przestrzeń dla mniejszych ubezpieczycieli, wpływając na poziom presji cenowej, zakres oferowanych produktów oraz tempo wdrażania innowacji. Z jednej strony stabilność liderów zapewnia przewidywalność i zaufanie konsumentów, z drugiej zaś może ograniczać dynamikę zmian i różnorodność oferty rynkowej. W związku z tym struktura rynku ma istotne znaczenie nie tylko z punktu widzenia ekonomicznego, ale również dla rozwoju jakościowego całego sektora.

Podsumowanie

Przeprowadzona analiza rynku ubezpieczeń na życie w Polsce w latach 2019-2023 pozwala stwierdzić, że sektor ten charakteryzował się stosunkowo wysoką odpornością na zmieniające się warunki gospodarcze. Pomimo negatywnego wpływu pandemii COVID-19 oraz rosnącej inflacji i niepewności ekonomicznej, rynek ubezpieczeń na życie utrzymał stabilność i zdolność do adaptacji. W części teoretycznej artykułu przedstawiono istotę ubezpieczeń na życie, ich funkcje oraz podstawowe rodzaje produktów oferowanych przez zakłady ubezpieczeń. Zróżnicowanie oferty – obejmujące zarówno produkty ochronne, oszczędnościowe, jak i inwestycyjne – wskazuje na rosnące znaczenie ubezpieczeń jako narzędzia zarządzania ryzykiem oraz długoterminowego planowania finansowego. Analiza danych statystycznych wykazała, że badany okres był czasem istotnych zmian w strukturze rynku. Szczególnie widoczne były wahania składki przypisanej brutto oraz wypłacanych świadczeń, które w dużej mierze wynikały z sytuacji epidemiologicznej oraz uwarunkowań makroekonomicznych. Jednocześnie sektor ubezpieczeniowy wykazał zdolność do odbudowy wyników finansowych w kolejnych latach. Wyniki analizy potwierdzają, że ubezpieczenia na życie pełnią ważną funkcję w systemie finansowym i społecznym, zapewniając ochronę finansową oraz wspierając proces akumulacji kapitału. W obliczu starzejącego się społeczeństwa oraz rosnącej niepewności ekonomicznej ich znaczenie będzie prawdopodobnie nadal rosło, co stwarza perspektywy dalszego rozwoju tego segmentu rynku.

Bibliografia

1. Biskupski Z., 2003, *Ubezpieczenia emerytalne i na życie. Część 2*, Gazeta Ubezpieczeniowa, nr 36.
2. Bukowski S., Lament M., 2021, *Market structure and financial effectiveness of life insurance companies,* „European Research Studies Journal", 24(2B), 502-514.
3. Handschke J., Kęszycka B., Kowalewski E., 2007, *Problematyka grupowych ubezpieczeń na życie w świetle znowelizowanych przepisów k.c. o umowie ubezpieczenia, Spór o intencje ustawodawcy*, „Wiadomości Ubezpieczeniowe", nr 7-8.
4. Kucka E., 2009., *Ubezpieczenia gospodarcze i społeczne*, Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, Olsztyn.
5. Lament J., Piątek J., 2023, *Rachunkowość zakładów ubezpieczeń i zakładów reasekuracji,* PWN, Warszawa.
6. Lament M., Bukowski S., 2022, *Wybrane determinanty rozwoju rynków ubezpieczeniowych krajów Unii Europejskiej w latach 1999-2019,* „Wiadomości Ubezpieczeniowe", 4, 61-74.
7. Lament M., Bukowski S., 2021, *Business model impact on the financial efficiency of insurance companies*, „European Research Studies Journal", 24(s4), 237-247.

8. Lament M., Jarolímová B., 2021, *Foreign capital as a determinant of the non-financial reporting development in insurance companies of the Visegrad Group countries, I*nvestment Management and Financial Innovations, 18(1), 203-214.
9. Lizak P., 2022, *Ubezpieczenia na życie. Zarys charakterystyki umów ubezpieczenia na życie*, KNF, Warszawa.
10. Olearczuk A., 1996, *Tradycyjne ubezpieczenia indywidualne*, [w:] O. Doan (red.), *Ubezpieczenia życiowe*, Poltext, Warszawa.
11. Raport roczny PIU 2023, Polska Izba Ubezpieczeń, Warszawa 2024.
12. Raport roczny PIU 2022, Polska Izba Ubezpieczeń, Warszawa 2023.
13. Raport roczny PIU 2021, Polska Izba Ubezpieczeń, Warszawa 2022.
14. Raport roczny PIU 2020, Polska Izba Ubezpieczeń, Warszawa 2021.
15. Raport roczny PIU 2019, Polska Izba Ubezpieczeń, Warszawa 2020.
16. Ronka-Chmielowiec W., 2016, *Ubezpieczenia*, C.H. Beck, Warszawa.
17. Sangowski T., 1996, *Vademecum pośrednika ubezpieczeniowego*, SAGA Printing, Poznań.
18. Stroiński E., 2003, *Ubezpieczenia na życie. Teoria i praktyka*, Poltext, Warszawa.
19. Szczepańska M., 2005, *Charakter prawny ubezpieczenia na życie z ubezpieczeniowym funduszem kapitałowym*, „Wiadomości Ubezpieczeniowe", nr 5-6.
20. Szczepańska M., 2008, *Ubezpieczenia na życie. Aspekty prawne*, Oficyna, Warszawa.
21. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U. z 1964 r. nr 16, poz. 93.
22. Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, (Dz.U. z 2024 r. poz. 000).

ANALYSIS OF THE LIFE INSURANCE MARKET IN POLAND IN 2019-2023

Abstract

The paper discussed the life insurance market in Poland in the years 2019-2023. The theoretical part presents the definition, features, and functions of life insurance, as well as the characteristics of the main products, such as traditional life insurance, annuity insurance, and unit-linked insurance. The empirical part includes an analysis of statistical data concerning the life insurance market in Poland, in particular gross written premiums, benefits and claims paid, operating costs, investments, and the financial results of insurance companies. Basic statistical measures, such as the arithmetic mean, standard deviation, and skewness coefficient, were used to assess data variability. The analysis shows that during the studied period the life insurance market in Poland underwent significant changes, mainly

due to the COVID-19 pandemic and economic conditions. Despite temporary declines in financial results, the sector remained stable and gradually recovered in subsequent years.

Keywords: financial analysis, insurance market, life insurance.