VOL. 77 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2025.77.13

Kamil Mroczka[*], *Marcin Groniewski*[**]

Krajobraz cyberbezpieczeństwa rynku finansowego w Polsce a poziom edukacji finansowej – perspektywa organu nadzoru nad rynkiem finansowym oraz jego interesariuszy

Cybersecurity in the Polish Financial Market and the Role of Financial Education: a Regulatory and Stakeholder Perspective

Słowa kluczowe: *cyberbezpieczeństwo, rynek finansowy, organ nadzoru, Komisja Nadzoru Finansowego, edukacja, edukacja finansowa*

Key words: *cybersecurity, financial market, supervisory authority, Polish Financial Supervision Authority, education, financial education*

Abstrakt: *Dynamiczny rozwój technologii informacyjno-komunikacyjnych (ICT) znacząco wpłynął na transformację społeczną i gospodarczą, w szczególności w sektorze finansowym. Coraz powszechniejsze wykorzystanie cyfrowych narzędzi przez instytucje finansowe niesie ze sobą zarówno korzyści, jak i nowe wyzwania, zwłaszcza w obszarze cyberbezpieczeństwa. Artykuł podejmuje problematykę wpływu edukacji finansowej – w szczególności jej komponentu związanego z cyberbezpieczeństwem – na bezpieczeństwo. Autorzy formułują tezę, że edukacja ta stanowi kluczowy element budowania odporności cyfrowej rynku finansowego, zwłaszcza w kontekście rosnącej liczby cyberzagrożeń, takich jak fałszywe oferty inwestycyjne rozpowszechniane w sieci. W celu weryfikacji postawionej hipotezy, przeanalizowano m.in. definicje cyberbezpieczeństwa i rynku finansowego, rolę Komisji Nadzoru Finansowego oraz wybrane regulacje prawne. Zastosowano metody badawcze o charakterze instytucjonalno-prawnym oraz empirycznym, w tym analizę danych i obserwację uczestniczącą. Wnioski zawarte w artykule wskazują na konieczność*

[*] ORCID ID: https://orcid.org/0000-0003-3809-3479; dr hab., MBA, Wydział Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. E-mail: ks.mroczka@uw.edu.pl.

[**] ORCID ID: https://orcid.org/0009-0002-0616-3516; doktorant, Prezes Zarządu Santander TFI. E-mail: magronie@gmail.com.

zintegrowanych działań edukacyjnych i regulacyjnych w celu zwiększenia odporności cyfrowej sektora finansowego w Polsce.

Abstract: *The rapid development of information and communication technologies (ICT) has significantly transformed both social and economic spheres, with the financial sector being one of the most impacted. The widespread adoption of digital tools by financial institutions brings undeniable benefits, but also introduces new challenges – particularly in the realm of cybersecurity. This article explores the role of financial education, with a special emphasis on cybersecurity awareness, as a key factor in strengthening the systemic financial security of the state. The central thesis posits that cybersecurity education is essential for building digital resilience, especially in light of increasing threats such as fraudulent investment offers distributed through social media, search engines, and online platforms. To verify this hypothesis, the study examines definitions of cybersecurity and the financial market, the role of the Polish Financial Supervision Authority (KNF), and the relevant legal framework. The research employs both institutional-legal and empirical methods, including data analysis and participant observation. The findings highlight the need for coordinated educational and regulatory efforts to enhance the digital resilience of Poland's financial market.*

Wprowadzenie

Termin cyberbezpieczeństwo zyskał istotne znaczenie w dyskursie publicznym, prawniczym i eksperckim, stając się trwałym elementem współczesnych debat i analiz. Dynamiczny rozwój technologii ICT stanowił istotny czynnik stymulujący wzrost gospodarczy oraz usprawnienie wielu procesów społecznych i politycznych. Z dobrodziejstw rozwoju technologicznego korzystamy praktycznie każdego dnia. Trudno dzisiaj wyobrazić sobie sytuację, w której istotne z perspektywy codziennego funkcjonowania procesy cofnęłyby się do czasów analogowych. W szczególności twierdzenie to odnosi się do funkcjonowania rynku finansowego. Klienci podmiotów tego rynku każdego dnia korzystają z aplikacji mobilnych, serwisów internetowych oraz innych narzędzi ICT wspierających procesy obsługi klienta. Często, poziom digitalizacji usług oferowanych przez dany podmiot jest decydujący o nawiązaniu, bądź utrzymaniu relacji z nim. Nakłady finansowe na digitalizację stale rosną. Procesy digitalizacji kolejnych sfer życia społecznego i gospodarczego znacząco przyspieszyły w wyniku globalnej pandemii COVID-19[1]. Objęły one również podmioty rynku finansowego, które już przed tym okresem były liderami cyfryzacji.

[1] Zob. szerzej: K. Mroczka, *Uwarunkowania i kierunki zmian w procesach decydowania publicznego na szczeblu samorządowym w związku z pandemią koronawirusa*, «Polityka i Społeczeństwo» 2020, nr 4(18).

Na potrzeby prowadzonych rozważań przyjęto następującą tezę badawczą: edukacja finansowa, której częścią jest edukacja w zakresie cyberbezpieczeństwa jest kluczowym czynnikiem przyczyniającym się do bezpieczeństwa finansowego państwa w wymiarze systemowym, dlatego że jednym z podstawowych zagrożeń są oferty fałszywych inwestycji dystrybuowane za pośrednictwem nośników reklamowych w popularnych serwisach społecznościowych, wyszukiwarkach czy serwisach internetowych[2].

W celu weryfikacji założonej tezy sformułowano następujące pytania badawcze: jak definiowane jest cyberbezpieczeństwo, zarówno w ujęciu teorii, jak i praktyki? Jak definiowany jest rynek finansowy? Jakie regulacje kształtują system cyberbezpieczeństwa rynku finansowego? Jakie zadania w tym systemie realizuje Komisja Nadzoru Finansowego? Jakie są główne zagrożenia dla bezpieczeństwa uczestników rynku finansowego w kontekście cyberbezpieczeństwa? Jakie działania należy podjąć aby zwiększyć odporność cyfrową rynku finansowego w Polsce?

W artykule zastosowano dwie główne metody badawcze. Po pierwsze zastosowano metodę instytucjonalno-prawną w celu zdefiniowania podmiotów odpowiedzialnych za cyberbezpieczeństwo oraz ich odpowiedzialności za ten obszar funkcjonowania państwa. Po drugie wykorzystano metody empiryczne, m.in. analizę danych ilościowych i jakościowych oraz obserwację uczestniczącą.

Konceptualizacja terminów: cyberbezpieczeństwo, rynek finansowy i edukacja finansowa

W piśmiennictwie słusznie podkreśla się, że pojęcie cyberbezpieczeństwa od samego początku „rodziło liczne wątpliwości w zakresie konkretnego znaczenia i nadania mu pewnych ram normatywnych. Podejmowane w literaturze przedmiotu próby definiowania cyberbezpieczeństwa nie miały kompleksowego charakteru, w zależności bowiem od dziedziny nauki uwypuklano aspekty informatyczne, społeczne, militarne czy funkcjonalne. Z tego też względu przedstawiciele doktryny podkreślali blankietowość tego terminu, przyjmując, że treść tego pojęcia jest zmienna, poddana ewolucji stosownie do zmian stosunków społecznych”[3].

---

2 *Raport roczny CSIRT KNF 2024*, Urząd Komisji Nadzoru Finansowego, Warszawa 2025, s. 4.

3 A. Szkurłat, *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, «internetowy Kwartalnik Antymonopolowy i Regulacyjny» 2020, nr 2(9), s. 55. Zob. także: C. Banasiński (red.), *Cyberbezpieczeństwo*, Warszawa

W ujęciu definicji legalnej cyberbezpieczeństwo, zgodnie z art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa, oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[4]. W doktrynie zwraca się uwagę, że terminowi „cyberbezpieczeństwo" ustawodawca krajowy nadaje znaczenie zbliżone do przyjętego w dyrektywie NIS[5] określenia „bezpieczeństwo sieci i systemów informacyjnych"[6]. Dyrektywa NIS precyzuje, że bezpieczeństwo sieci i systemów informatycznych oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych przez te sieci i systemy informatyczne.

Już pobieżna analiza przywołanych definicji prowadzi do wniosku, że krajowy ustawodawca pominął występujący w dyrektywie zwrot „przy danym poziomie zaufania", nadający charakter względny „odporności", co – zdaniem Grażyny Szpor – może mieć istotne znaczenie w praktyce stosowania prawa[7]. Druga różnica dotyczy odniesienia samego terminu odporności. Polski ustawodawca odnosi ją do systemów informacyjnych, a ustawodawca unijny do systemów informacyjnych i sieci. Warto również podkreślić, że przedstawiciele doktryny kontestują przyjęte przez polskiego ustawodawcę atrybuty bezpieczeństwa informacji[8].

W procesie konceptualizacji terminu cyberbezpieczeństwo należy również odwołać się do innych regulacji unijnych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.[9] wskazuje, że „cyberbez-

2018; C. Banasiński, M. Rojszczak, J. M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski (red.), *Cyberbezpieczeństwo*, Warszawa 2020.

4 Zob. szerzej: G. Szpor [w:] K. Czaplicki, A. Gryszczyńska (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, art. 2, LEX.

5 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 2016 r., s. 1).

6 G. Szpor [w:] *Ustawa o krajowym systemie…*, art. 1, LEX.

7 Tamże.

8 Zdaniem Krzysztofa Maderaka, Kamila Mroczki i Krzysztofa Zielińskiego przyjęte atrybuty powinny zostać uzupełnione o rozliczalność, niezawodność i niezaprzeczalność zgodnie z brzmieniem rekomendacji D wydanej przez Komisję Nadzoru Finansowego. Zob. szerzej: K. Mroczka, K. Maderak, K. Zieliński, *Nadzór nad cyberbezpieczeństwem rynku finansowego w Polsce*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Informatyzacja, cyfryzacja i danetyzacja*, Warszawa 2021, s. 279.

9 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych

pieczeństwo to nie tylko kwestia związana z technologią, ale kwestia, w przypadku której równie ważne są ludzkie zachowania. Dlatego też należy usilnie propagować «cyberhigienę», czyli proste, rutynowe czynności, których wdrożenie i regularne wykonywanie przez obywateli, organizacje i przedsiębiorstwa minimalizuje ich narażenie na ryzyka związane z cyberzagrożeniami"[10]. W tym kontekście na potrzeby tego aktu prawnego przyjęto, że cyberbezpieczeństwo obejmuje „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami"[11].

Paweł Wajda słusznie podkreśla, że *ratio legis* przepisów prawa unijnego i krajowego jest „ochrona użytkowników usług kluczowych oraz usług cyfrowych przed negatywną ekspozycją tych użytkowników na ryzyka specyficzne związane z brakiem odpowiedniego poziomu cyberbezpieczeństwa". Zdaniem tego autora „prawodawca, określając standard świadczenia usług kluczowych i usług cyfrowych w zakresie cyberbezpieczeństwa, który to standard ma być stosowany przez operatorów usług kluczowych oraz przez dostawców usług cyfrowych, ma za zadanie chronić przede wszystkim końcowych beneficjentów tych usług"[12].

Nie ulega wątpliwości, że cyberbezpieczeństwo „jest szczególnym typem bezpieczeństwa, pojmowanego przez pryzmat porządku i ładu struktur umieszczonych w cyberprzestrzeni"[13]. Jest to obszar, który w ostatnich latach znacząco zyskał na znaczeniu zarówno w wymiarze jednostkowym, jak i systemowym.

Rynek finansowy

Termin rynek finansowy w przeciwieństwie do terminu cyberbezpieczeństwo nie posiada definicji normatywnej, dlatego należy sięgnąć do analizy definicji proponowanych w piśmiennictwie. Przedstawiciele doktryny podejmowali wiele prób zdefiniowania tego terminu. Ich pełny przegląd wykracza jednak poza założenia przyjęte przez autorów niniejszego artykułu.

Najczęściej rynek finansowy jest określany jako miejsce, w którym dokonuje się zawieranie transakcji kupna lub sprzedaży specyficznego towaru, jakim jest

oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 2019 r., s. 15 ze zm.).

10 Tamże, motyw 8.

11 Tamże, art. 2 pkt 1.

12 P. Wajda, *Cyberbezpieczeństwo – sektorowe aspekty regulacyjne*, «internetowy Kwartalnik Antymonopolowy i Regulacyjny» 2020, nr 2(9), s. 12.

13 D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, «Prawo w Działaniu» 2023, nr 53, s. 103.

instrument finansowy[14]. Inni autorzy podkreślają, że rynek finansowy należy postrzegać jako system współzależnych transakcji kupna i sprzedaży dobra[15] albo jako proces, w ramach którego następuje wzajemne oddziaływanie nabywców i sprzedawców danego dobra, w rezultacie czego dochodzi do określenia jego ceny i ilości[16]. Giełda Papierów Wartościowych definiuje rynek finansowy jako miejsce, „na którym są zawierane transakcje kupna i sprzedaży różnych form kapitału pieniężnego, na różne terminy w oparciu o instrumenty finansowe"[17]. Giełda wskazuje również, że uczestnikami rynku finansowego są z jednej strony podmioty potrzebujące kapitału, kreujące popyt, natomiast z drugiej strony – podmioty dysponujące nadwyżkami finansowymi, kreujące podaż kapitału[18].

Wedle innej definicji rynek finansowy to „ogół transakcji związanych z przemieszczaniem kapitałów pieniężnych, od podmiotów dysponujących wolnymi środkami finansowymi do podmiotów zgłaszających zapotrzebowanie na takie środki"[19]. W doktrynie zwraca się również uwagę, że „rynek finansowy tworzą transakcje polegające na zamianie pieniądza na instrument finansowy, zamianie instrumentu finansowego na pieniądz bądź zamianie jednego instrumentu finansowego na inny instrument finansowy"[20].

Rynek finansowy dzielony jest na różne segmenty. Eksperci z GPW dzielą rynek finansowy na (1) rynek pieniężny, (2) rynek kapitałowy, (3) rynek walutowy, (4) rynek terminowy i (5) rynek depozytowo-kredytowy[21]. Przedstawiciele organu nadzoru nad rynkiem finansowym na potrzeby wdrożenia rozporządzenia DORA[22] zaproponowali bardziej szczegółową prezentację podmiotów tworzących rynek finansowy (*vide* grafika 1).

---

14 U. Banaszczak-Soroka, P. Zawadzka, *Struktura systemu finansowego*, [w:] U. Banaszczak-Soroka (red.), *Rynki finansowe. Organizacja, instytucje, uczestnicy*, Warszawa 2019, s. 14; M. Wypych, *Finanse i instrumenty finansowe*, Łódź 2001, s. 15.

15 B. Czarny, R. Rapacki, *Podstawy ekonomii*, Warszawa 2002, s. 81.

16 P. Samuelson, W. Nordhaus, *Ekonomia*, Warszawa 1995, s. 82; P. Wajda, *Rola decyzji administracyjnej w nadzorze nad polskim systemem finansowym*, Warszawa 2009, s. 183.

17 *Rynek finansowy w Polsce*, Giełda Papierów Wartościowych, Rynek finansowy (9.04.2025).

18 Tamże.

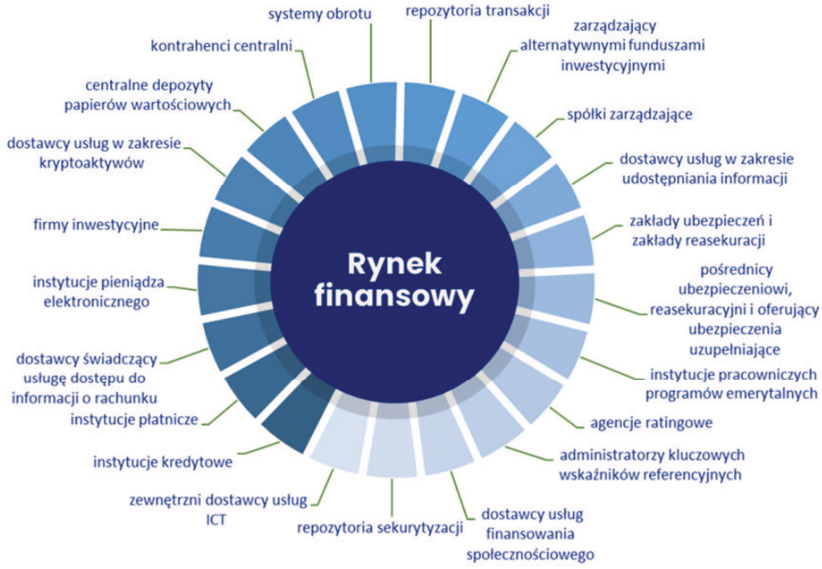
19 W. Bień, *Rynek papierów wartościowych*, Warszawa 2004, s. 183.

20 P. Zawadzka, *Modele nadzoru rynku finansowego. Aspekty prawne*, Warszawa 2017, s. 14.

21 *Rynek finansowy w Polsce*, Giełda Papierów Wartościowych, Rynek finansowy (9.04.2025).

22 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 2022 r., s. 1 ze zm.).

Grafika 1. Rynek finansowy w Polsce



Źródło: *Wymagania Rozporządzenia DORA dla podmiotów stosujących uproszczone ramy zarządzania ryzykiem związanym z ICT*, Urząd Komisji Nadzoru Finansowego, 21 marca 2025 r., Wymagania rozporządzenia DORA dla podmiotów stosujących uproszczone ramy zarządzania ryzykiem związanym z ICT – Komisja Nadzoru Finansowego (9.04.2025).

Konkludując rozważania związane z rynkiem finansowym, należy zgodzić się z przedstawicielami doktryny, którzy podkreślają, że rynek finansowy nie jest kategorią rozumianą w sposób jednolity, ponieważ sposób, w jaki ten rynek jest definiowany oraz kryteria, według jakich dokonywany jest jego podział, zmieniają się wraz z rozwojem rynku finansowego i wzrostem znaczenia poszczególnych jego segmentów[23]. Niezależnie od powyższego, należy zgodzić się z twierdzeniem, że rynek finansowy jest fundamentem gospodarki każdego państwa, ponieważ w dzisiejszych uwarunkowaniach trudno sobie wyobrazić dobrze funkcjonującą i rozwijającą się gospodarkę bez sprawnego i efektywnie działającego rynku finansowego[24].

Edukacja finansowa

Małgorzata Iwanicz-Drozdowska analizując znaczenie edukacji finansowej wskazuje, że pod pojęciem tym należy rozumieć „podejmowanie szeroko zakrojonych działań w celu upowszechniania wiedzy oraz wykształcania wśród

[23] P. Wajda, *Rola decyzji*…, s. 19.
[24] J. Bilski, M. Janicka, T. Miziołek, *Międzynarodowy system finansowy*, Łódź 2016, s. 59.

obywateli pozytywnych nawyków, prowadzących do podejmowania właściwych decyzji w zakresie zarządzania ich osobistymi finansami i efektywnego dysponowania środkami finansowymi, zgodnie z obecnymi i przyszłymi potrzebami (np. zakup własnego mieszkania i/lub sfinansowanie edukacji dzieci)"[25]. Zdaniem tej autorki edukacja finansowa przyczynia się do kształtowania tzw. świadomości finansowej (*financial literacy, financial capability*), która to świadomość umożliwia obywatelom zorientowanie się, jakie „szanse i zagrożenia niosą ze sobą zarówno typowe, jak również coraz nowsze i bardziej skomplikowane produkty finansowe"[26]. Zdaniem innej autorki edukacja finansowa to „kształcenie umiejętności, wiedzy i zachowań, które pozwalają człowiekowi podejmować świadome decyzje dotyczące pieniędzy: płatności, zaciągania kredytów, otwarcia rachunku bankowego, planowania dochodów i zarządzania nimi, inwestowania na rynku i oszczędzania"[27].

W ujęciu eksperckim edukacja finansowa definiowana jest jako „proces, w którym konsumenci i/lub inwestorzy finansowi zwiększają swoje kompetencje w zakresie rozumienia produktów i pojęć z zakresu finansów oraz zagrożeń finansowych, a także, poprzez informacje, wskazówki lub obiektywne porady, rozwijają swoje umiejętności i poczucie pewności siebie, aby stać się bardziej świadomymi zagrożeń i możliwości finansowych, dokonywać odpowiedzialnych wyborów, wiedzieć, gdzie zwrócić się o pomoc, oraz podejmować inne skuteczne działania w celu poprawy swojej sytuacji finansowej"[28].

O znaczeniu edukacji finansowej świadczy fakt, że jest ona przedmiotem działań władz zarówno na poziomie unijnym, jak i krajowym. Już w 2007 r. Komisja Europejska opublikowała komunikat[29], w którym podkreślono, że „edukacja finansowa odgrywa kluczową rolę w tworzeniu jednolitego rynku i z tego powodu pragnie zachęcać obywateli europejskich do zdobywania podstawowej wiedzy dotyczącej finansów osobistych"[30]. W ujęciu krajowym decydenci rządowi we współpracy z OECD opracowali w 2023 r. Krajową Strategię Edukacji Finansowej (KSEF) dla Polski[31]. Dokument ten definiuje dłu-

25 M. Iwanicz-Drozdowska, *Edukacja finansowa*, «infos BAS» 2010, nr 15(85), s. 1.

26 Tamże.

27 M. Rakowska, *Edukacja finansowa dla przyszłości*, obserwatorfinansowy.pl, Obserwator Finansowy: ekonomia, debata, Polska, świat (9.04.2025).

28 *Krajowa Strategia Edukacji Finansowej (KSEF) dla Polski*, OECD – Ministerstwo Finansów, 2023, https://www.oecd.org/content/dam/oecd/pl/publications/reports/2023/04/national-strategy-for-financial-education-for-poland_6fd5288f/8ce6dea5-pl.pdf (9.04.2025), s. 13.

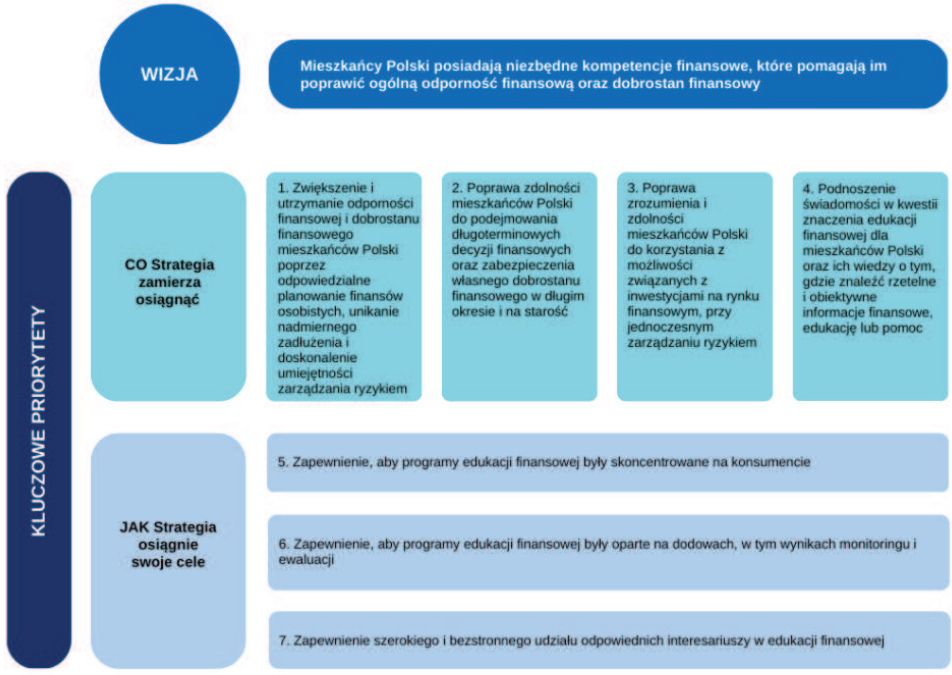
29 Komunikat komisji z dnia 18 grudnia 2007 r. w sprawie edukacji finansowej, COM(2007) 808 wersja ostateczna – nieopublikowany w Dzienniku Urzędowym.

30 Tamże.

31 *Krajowa Strategia Edukacji Finansowej…*

goterminową wizję edukacji finansowej w Polsce, jej priorytety strategiczne, grupy docelowe oraz ramy ewaluacji. Cele strategiczne w zakresie edukacji finansowej, kluczowe priorytety w tym zakresie oraz wizję stanu docelowego prezentuje poniższa grafika.

Grafika 2. Ogólny zarys KSEF i jej kluczowych priorytetów



Źródło: *Krajowa Strategia Edukacji Finansowej (KSEF) dla Polski*, OECD – Ministerstwo Finansów, 2023, https://www.oecd.org/content/dam/oecd/pl/publications/reports/2023/04/national-strategy-for-financial-education-for-poland_6fd5288f/8ce6dea5-pl.pdf (9.04.2025), s. 15.

Strategia jednoznacznie wskazuje, że więcej programów edukacji finansowej powinno skupiać się na zagadnieniach, które wymagają traktowania priorytetowego, takich jak kwestie budżetowania, oszczędzania i inwestowania, cyfryzacji (w tym znajomości zagrożeń związanych z cyberbezpieczeństwem i oszustwami w Internecie), odpowiedzialnego zaciągania kredytów i pożyczek oraz ubezpieczeń. W ujęciu operacyjnym jednym z priorytetów jest opracowanie i wdrożenie działań podnoszących świadomość na temat różnych rodzajów ryzyka związanego z cyberbezpieczeństwem oraz oszustwami i próbami wyłudzenia w Internecie, tak by mieszkańcy Polski wiedzieli, jak bezpiecznie korzystać z narzędzi i usług online[32]. W tym kontekście bez wątpienia należy

[32] Tamże, s. 7 i n.

uznać, że jednym z obszarów szeroko pojętej edukacji finansowej jest edukacja w zakresie cyberbezpieczeństwa. Takie podejście jest prezentowane przez autorów niniejszego artykułu.

Zadania Komisji Nadzoru Finansowego w zakresie cyberbezpieczeństwa

Zadania KNF w zakresie cyberbezpieczeństwa wynikają z jednej strony z przepisów prawa unijnego, a z drugiej z regulacji krajowych. Na poziomie unijnym kluczowym aktem prawnym jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (dalej: rozporządzenie DORA)[33]. W kontekście regulacji krajowych należy przywołać ustawę z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[34] oraz ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[35].

Rozporządzenie DORA

Od 17 stycznia 2025 r. obowiązuje rozporządzenie DORA (ang. *Digital Operational Resilience Act*)[36]. Prace nad rozporządzeniem trwały kilka lat. Rozpoczęto je we wrześniu 2020 r. W grudniu 2022 r. zostało podpisane przez przewodniczących Parlamentu Europejskiego i Rady Unii Europejskiej i opublikowane w Dzienniku Urzędowym UE. Szczegółowe kalendarium prac nad tą regulacją prezentuje poniższa grafika.

Analizowana regulacja ma na celu ujednolicenie i wzmocnienie odporności operacyjnej podmiotów sektora finansowego państw unijnych. Jan Byrski i Justyna Kurek-Sobieraj podkreślają, że unijne rozporządzenie DORA to „instrument, który skupia się na poprawie standardów w sektorze usług finansowych,

[33] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 2022 r., s. 1 ze zm.).

[34] Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz.U. z 2024 r. poz. 135 ze zm.).

[35] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077 ze zm.).

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 2022 r., s. 1 ze zm.).

w szczególności w odniesieniu do zarządzania technologiami informacyjno-technologicznymi oraz zarządzaniem ryzykiem związanym z cyberbezpieczeństwem. Jego celem jest wprowadzenie spójnych regulacji obejmujących wszystkie instytucje finansowe i zabezpieczenie przed poważnymi zakłóceniami operacyjnymi"[37].

Grafika 3. Kalendarium prac nad rozporządzeniem DORA

Źródło: J. Byrski, *Digital Operational Resilience Act (DORA), Szkolenie on-line*, Traple, Konarski, Podrecki & Wspólnicy, 18 marca 2025 r.

Przedmiot analizowanej regulacji został zdefiniowany w art. 1 rozporządzenia. Przepis ten stanowi, że w celu osiągnięcia wysokiego wspólnego poziomu operacyjnej odporności cyfrowej ustanawia się następujące jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych wspierających procesy biznesowe podmiotów finansowych:

1) wymogi mające zastosowanie do podmiotów finansowych w odniesieniu do:
   a) zarządzania ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT);
   b) zgłaszania poważnych incydentów związanych z ICT właściwym organom oraz dobrowolnego informowania ich o znaczących cyberzagrożeniach;
   c) zgłaszania właściwym organom przez podmioty finansowe poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami;

[37] J. Byrski, A. Kurek-Sobieraj, *Od redaktorów*, [w:] J. Byrski, A. Kurek-Sobieraj (red.), *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, Warszawa 2025, s. XIII.

d) testowania operacyjnej odporności cyfrowej;
e) wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze;
f) środków na rzecz należytego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT;

2) wymogi w odniesieniu do ustaleń umownych zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi;
3) zasady dotyczące ustanowienia i funkcjonowania ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT świadczącymi usługi na rzecz podmiotów finansowych;
4) zasady współpracy między właściwymi organami oraz zasady nadzoru i egzekwowania przepisów przez właściwe organy w odniesieniu do wszystkich kwestii objętych niniejszym rozporządzeniem.

W ujęciu podmiotowym rozporządzenie ma zastosowanie do:

1) instytucji kredytowych;
2) instytucji płatniczych;
3) dostawców świadczących usługę dostępu do informacji o rachunku;
4) instytucji pieniądza elektronicznego;
5) firm inwestycyjnych;
6) dostawców usług w zakresie kryptoaktywów i emitentów tokenów powiązanych z aktywami;
7) centralnych depozytów papierów wartościowych;
8) kontrahentów centralnych;
9) systemów obrotu;
10) repozytoriów transakcji;
11) zarządzających alternatywnymi funduszami inwestycyjnymi;
12) spółek zarządzających;
13) dostawców usług w zakresie udostępniania informacji;
14) zakładów ubezpieczeń i zakładów reasekuracji;
15) pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające;
16) instytucji pracowniczych programów emerytalnych;
17) agencji ratingowych;
18) administratorów kluczowych wskaźników referencyjnych;
19) dostawców usług finansowania społecznościowego;
20) repozytoriów sekurytyzacji;
21) zewnętrznych dostawców usług ICT.

Należy podkreślić, że prawodawca unijny wprowadził również katalog wyłączeń od stosowania przepisów rozporządzenia. Dotyczą one m.in. małych

podmiotów[38]. Dodatkowo rozporządzenie nie ma zastosowania do: (1) zarządzających alternatywnymi funduszami inwestycyjnymi, (2) zakładów ubezpieczeń i zakładów reasekuracji, (3) instytucji pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników, (4) osób fizycznych lub prawnych zwolnionych na podstawie przepisów szczególnych, (5) pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające będących mikroprzedsiębiorstwami, małymi lub średnimi przedsiębiorstwami oraz (6) instytucji świadczących żyro pocztowe.

W Polsce nadzór nad wykonaniem obowiązków, które na podmioty zobowiązane nakłada DORA, powierzony został KNF. W piśmiennictwie podkreśla się, że obecnie KNF odgrywa „najważniejszą rolę w zarządzaniu incydentami i zagrożeniami cyberbezpieczeństwa"[39] w zakresie rynku finansowego. Kompetencje organu nadzoru obejmują m.in. przeprowadzanie kontroli i dochodzeń, żądanie od podmiotów finansowych informacji, dokumentów lub wyjaśnień w zakresie niezbędnym do sprawowania nadzoru, wydawanie rekomendacji dotyczących bezpieczeństwa sieci i systemów informatycznych, nakładanie środków naprawczych i kar administracyjnych, wydawanie nakazów zaprzestania naruszeń[40].

Jak wspomniano powyżej, rozporządzenie DORA obowiązuje od 17 stycznia 2025 r. Niestety, krajowy ustawodawca nie uchwalił na czas odpowiednich przepisów wprowadzających rozporządzenie do polskiego systemu normatywnego. Prace (na kwiecień 2025 r.) nadal trwają[41]. Opieszałość decydentów rządowych zmusiła do zabrania głosu Komisję Nadzoru Finansowego. W dniu 31 grudnia 2024 r. na stronie internetowej nadzoru opublikowano *Stanowisko UKNF dotyczące stosowania przez podmioty finansowe Rozporządzenia DORA*[42]. W stanowisku tym UKNF jednoznacznie wskazał, że rozporządzenie jest aktem bezpośrednio stosowanym i nie wymaga odrębnej transpozycji do prawa krajowego. W ocenie nadzoru brak przepisów krajowych stosowanie rozporządzenia DORA nie wstrzymuje obowiązku przestrzegania przez podmioty finansowe wszelkich wymogów wynikających z przepisów

38 E. Borkowska, *DORA już obowiązuje, ale brakuje przepisów krajowych*, 3 lutego 2025 r., Legalis.

39 Tamże.

40 Tamże.

41 Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji, druk nr UC11, Rządowe Centrum Legislacji, https://legislacja.rcl.gov.pl/projekt/12384252 (12.04.2025).

42 *Stanowisko UKNF dotyczące stosowania przez podmioty finansowe Rozporządzenia DORA*, Urząd Komisji Nadzoru Finansowego, Warszawa, 31 grudnia 2024 r.

rozporządzenia DORA[43]. KNF wyraziła również oczekiwanie, że działania dostosowawcze podmiotów finansowych w zakresie wdrożenia wymogów rozporządzenia DORA zostaną zrealizowane najpóźniej do 17 stycznia 2025 r. W przywołanym dokumencie zapowiedziano również planowane uchylenie aktów *soft law* (m.in. rekomendacji D[44] i wytycznych) dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

Syntetyzując tę część rozważań należy podkreślić, że rozporządzenie DORA w państwach unijnych obejmie swoim zakresem około 22 000 podmiotów świadczących różnego rodzaju usługi finansowe dla uczestników rynku finansowego. W tym wymiarze bez wątpienia proces implementacji wymagań rozporządzenia stanowi istotne wyzwanie dla podmiotów rynku finansowego. Trzeba pamiętać, że podmioty rynku finansowego cechuje różny poziom dojrzałości organizacyjnej i procesowej w zakresie ICT. Nie zawsze posiadają odpowiednie zasoby finansowe, organizacyjne czy kadrowe, aby sprostać wymaganiom regulacyjnym. Prawodawca unijny uznał jednak, że bezpieczeństwo uczestników rynku finansowego jest wartością nadrzędną i niezbędne jest wprowadzenie minimalnych standardów w tym zakresie. Takie postrzeganie tej regulacji przyświeca autorom niniejszego tekstu.

Ustawa o nadzorze nad rynkiem finansowym

Zgodnie z brzmieniem art. 2 ustawy o nadzorze nad rynkiem finansowym, celem nadzoru nad tym rynkiem jest zapewnienie prawidłowego jego funkcjonowania, stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku również poprzez rzetelną informację dotyczącą funkcjonowania rynku. W wymiarze instytucjonalnym powyższe cele realizowane są przez Komisję Nadzoru Finansowego oraz Urząd Komisji Nadzoru Finansowego. W ujęciu operacyjnym ustawodawca sformułował zadania KNF. W zakresie prowadzonych rozważań, do zadań Komisji należy podejmowanie działań mających na celu przeciwdziałanie zagrożeniom w zakresie bezpieczeństwa systemów teleinformatycznych, w tym przez wykonywanie zadań organu właściwego do spraw cyberbezpieczeństwa w zakresie określonym w ustawie z lipca 2018 r.

[43] Tamże.

[44] Uchwała Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz. Urz. KNF z 2013 r. poz. 5).

Ustawa o krajowym systemie cyberbezpieczeństwa

Zgodnie z brzmieniem art. 3 ustawy krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. W ujęciu podmiotowym krajowy system cyberbezpieczeństwa tworzy szereg podmiotów, m.in. operatorzy usług kluczowych, dostawcy usług cyfrowych, zespoły CSIRT oraz organy właściwe do spraw cyberbezpieczeństwa. Z perspektywy założonego celu artykułu analiza ograniczona zostanie do scharakteryzowania zadań zespołu sektorowego CSIRT oraz organu właściwego do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych[45].

Zadania organów właściwych zdefiniowano w art. 42 ustawy. Odpowiadają one m.in. za: (1) prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej; (2) wydawanie decyzji uznaniu podmiotu za operatora usługi kluczowej; (3) składanie wniosków o zmianę danych w wykazie operatorów usług kluczowych; (4) przygotowywanie we współpracy z zespołami CSIRT NASK, GOV i MON rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych dotyczących zgłaszania incydentów; (5) monitorowanie stosowania przepisów ustawy operatorów usług kluczowych i dostawców usług cyfrowych; (6) prowadzenie kontroli operatorów usług kluczowych i dostawców usług cyfrowych.

W piśmiennictwie podkreśla się, że rola KNF jako organu właściwego do spraw cyberbezpieczeństwa nie ogranicza się wyłącznie do literalnej realizacji ustawowych obowiązków stypizowanych w art. 42 ustawy. Działalność ta obejmuje również aktywny udział w kształtowaniu i rozwijaniu krajowego systemu cyberbezpieczeństwa m.in. poprzez bezpośrednią współpracę z uczestnikami tego systemu na poziomie krajowym oraz unijnym, podejmowanie działań edukacyjnych i informacyjnych zarówno w wymiarze instytucjonalnym, jak i jednostkowym. Przykładem takich działań mogą być np. spotkania z przedstawicielami Komisji Europejskiej oceniającymi stan wdrażania prawa unijnego, czy współpraca z NASK PIK w zakresie opracowania poradnika dla operatorów usług kluczowych[46]. W wymiarze skierowanym do nieprofesjonalnych uczest-

[45] Art. 41 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa.

[46] B. Biderman, K. Mroczka, *Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce*, «Bezpieczny Bank» 2022, nr 2(87), s. 58.

ników rynku finansowego warto przywołać inicjatywy realizowane w ramach Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (analizy, raporty, encyklopedia cyberbezpieczeństwa etc.)[47].

Zadania sektorowych zespołów cyberbezpieczeństwa (CSIRT) zwarto w art. 44 ustawy. Przepis ten stanowi w ust. 1, że sektorowy zespół cyberbezpieczeństwa jest odpowiedzialny w szczególności za:

1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w ustawie;
3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu;
4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

W lipcu 2020 r. przewodniczący KNF podjął decyzję o powołaniu zespołu CSIRT KNF dedykowanego dla podmiotów rynku finansowego[48]. Był to pierwszy sektorowy zespół powołany w ramach krajowego systemu cyberbezpieczeństwa[49]. W ciągu kilku lat funkcjonowania zespół ten wpisał się na stałe w system cyberbezpieczeństwa. Do najważniejszych zadań zespołu należy również monitorowanie i analiza działań cyberprzestępców wyłudzających środki finansowe, wykrywanie i blokowanie stron o charakterze oszukańczym, analizowanie złośliwego oprogramowania w kontekście bezpieczeństwa środków finansowych, a także zwiększanie poziomu świadomości interesariuszy rynku finansowego odnośnie do zagrożeń w cyberprzestrzeni[50].

---

47 Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego, Urząd Komisji Nadzoru Finansowego, Artykuły CSIRT KNF (8.04.2025).

48 Zob. szerzej: K. Mroczka, P. Piekutowski, *Cyber safe place – ochrona cyberbezpieczeństwa rynku finansowego jako zyskujące na znaczeniu zadanie Komisji Nadzoru Finansowego*, [w:] J. Stelmach (red.), *Bezpieczeństwo terrorystyczne budynków użyteczności publicznej. Tom 4. Bezpieczeństwo w cyberprzestrzeni oraz praktyczny wymiar zabezpieczeń technicznych*, Warszawa 2022.

49 B. Godusławski, *W KNF rusza specjalny zespół, który pomoże instytucjom finansowym przeciwstawić się cyberprzestępcom*, «Dziennik Gazeta Prawna», 9 czerwca 2020; W KNF rusza specjalny zespół, który pomoże instytucjom finansowym przeciwstawić się cyberprzestępcom – GazetaPrawna.pl (10.05.2025).

50 *Raport roczny CSIRT KNF 2024*…, s. 4.

Prognoza cyberzagrożeń w kontekście funkcjonowania rynku finansowego

W marcu 2024 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przedstawiła prognozę cyberzagrożeń na kolejne lata. Eksperci ENISA na podstawie danych empirycznych, obserwacji funkcjonowania cyberprzestrzeni oraz oczekiwań interesariuszy systemu cyberbezpieczeństwa w Unii Europejskiej, a także prognoz co do potencjalnych zagrożeń i ryzyk sformułowała 10 największych cyberzagrożeń, które mogą wystąpić do 2030 r. Są to: (1) naruszenie łańcucha dostaw w zakresie oprogramowania; (2) niedobór umiejętności; (3) błąd ludzki i wykorzystanie starszych systemów w cyberfizycznych ekosystemach; (4) wykorzystanie niezałatanych i nieaktualnych systemów w przeciążonym międzysektorowym ekosystemie technologicznym; (5) autorytaryzm nadzoru cyfrowego/utrata prywatności; (6) transgraniczni dostawcy usług ICT jako pojedynczy punkt awarii; (7) zaawansowane kampanie dezinformacyjne/operacje wywierania wpływu; (8) wzrost zaawansowanych zagrożeń hybrydowych; (9) nadużywanie sztucznej inteligencji; (10) fizyczny wpływ zakłóceń naturalnych/środowiskowych na krytyczną infrastrukturę cyfrową[51].

Dyrektor wykonawczy ENISA, Juhan Lepassaar podczas prezentacji cyberzagrożeń słusznie podkreślił, że „mitygacji przyszłych zagrożeń nie można odkładać ani unikać. Dlatego każdy wgląd w przyszłość jest naszym najlepszym planem ubezpieczeniowym – zgodnie z przysłowiem «lepiej zapobiegać niż leczyć». Naszym obowiązkiem jest podjęcie wszelkich możliwych środków z góry, aby z biegiem lat zwiększyć naszą odporności i przyczynić się do poprawy krajobrazu bezpieczeństwa cybernetycznego w 2030 roku i później"[52].

Przywołane powyżej cyberzagrożenia bez wątpienia wiążą się z koniecznością stosowania wzmożonych środków bezpieczeństwa w cyberprzestrzeni. W tym kontekście eksperci słusznie podkreślają, że wdrażanie rozwiązań z zakresu cyberbezpieczeństwa musi odbywać się w sposób holistyczny, uwzględniający kwestie technologiczne, systemowe i organizacyjne[53]. Bardzo ważne jest również inwestowanie w rozwój wiedzy i kompetencje zarówno ekspertów odpowiedzialnych za cyberbezpieczeństwo, jak i pracowników instytucji finansowych oraz jej klientów. Ten aspekt jest szczególnie ważny w kontekście budowania odporności cyfrowej podmiotów rynku finansowego.

---

51 M. Stachoń, *Foresight Cybersecurity Threats for 2030 – raport ENISA*, «NASK Cyber Policy», 9 kwietnia 2024 r., Foresight Cybersecurity Threats for 2030 – raport ENISA – Cyberpolicy NASK (10.04.2025).

52 *Cyberzagrożenia według ENISA – co nas czeka w 2023 roku i w nadchodzących latach?*, «Resilia», 13 grudnia 2022 r., Prognoza cyberzagrożeń według ENISA na nadchodzące lata (8.04.2025).

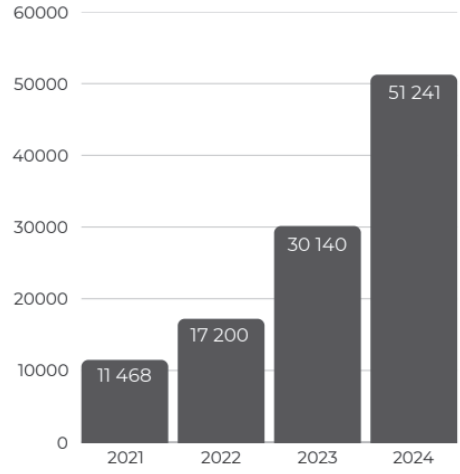
53 Tamże.

Stan cyberbezpieczeństwa rynku finansowego w świetle raportów zespołu CSIRT KNF

Jak wspomniano powyżej, w ramach nadzoru finansowego powołano sektorowy zespół CSIRT, który odpowiada za koordynację obsługi zagrożeń i incydentów poważnych w podmiotach z sektora finansowego. Zespół ten na stałe wpisał się w krajobraz systemu cyberbezpieczeństwa państwa polskiego. Jest jego istotnym elementem. Na potwierdzenie tego twierdzenia w dalszej części artykułu przywołane zostaną informacje i dane prezentujące aktywność zespołu CSIRT KNF.

Z opublikowanego na początku roku *Raportu rocznego CSIRT KNF* wynika, że w 2024 r. dominujące zagrożenie stanowiły oferty fałszywych inwestycji dystrybuowane za pośrednictwem nośników reklamowych w popularnych serwisach społecznościowych, wyszukiwarkach czy serwisach internetowych[54]. Należy również podkreślić, że CSIRT KNF w roku 2024 odnotował rekordową liczbę wykrytych niebezpiecznych domen – 51 241. Za ich pośrednictwem wykradano m.in.: dane do logowania do bankowości elektronicznej, informacje o kartach płatniczych, dane osobowe. Analizując trendy w tym wymiarze należy dostrzec znaczący wzrost liczby niebezpiecznych domen. Na przestrzeni lat 2021–2024 odnotowano ponad czterokrotny wzrost. Szczegóły prezentuje poniższy wykres.

Wykres 1. Liczba zgłoszonych domen *phishingowych* w latach 2021–2024 przez CSIRT KNF



Źródło: *Raport roczny CSIRT KNF 2024*, Urząd Komisji Nadzoru Finansowego, Warszawa 2025, s. 10.

[54] *Raport roczny CSIRT KNF 2024…*, s. 5.

Największa liczba domen *phishingowych* dotyczyła fałszywych inwestycji: 45 985 domen (89,4%), fałszywych ankiet: 4030 domen, usług kurierskich i pocztowych: 521 domen, portali społecznościowych: 166 domen oraz fałszywych bramek płatności: 125 domen. W ujęciu analizy socjotechnik stosowanych przez przestępców uwagę zwraca fakt, że najczęściej wykorzystywano w celach ataków *phishingowych* wizerunek polityków (26%) oraz celebrytów (14%).

Eksperci CSIRT KNF w analizowanym raporcie zwracają uwagę, że przestępcy w atakach wykorzystywali zaawansowane techniki socjotechniczne, budując fałszywe platformy inwestycyjne, które charakteryzowały się: profesjonalnym wyglądem stron internetowych, imitującym oficjalne serwisy inwestycyjne, sfałszowanymi historiami transakcji i wykresami, systemami referencyjnymi zachęcającymi do polecania platformy znajomym, fałszywymi opiniami i rekomendacjami, złożonymi systemami uwierzytelniania imitującymi prawdziwe platformy[55].

Z perspektywy celu niniejszego artykułu warto również przywołać zidentyfikowany przez zespół CSIRT KNF *modus operandi*. Przestępcy w swoich działaniach stosują wieloetapowe schematy działania.

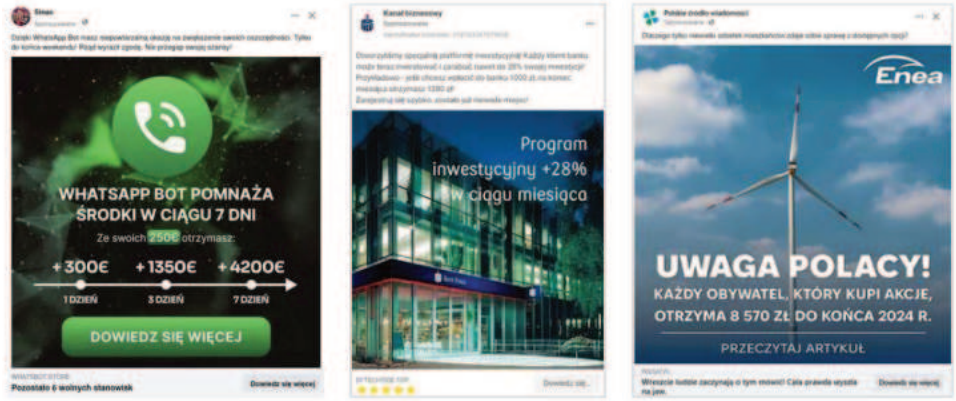
- Etap wstępny obejmujący m.in. targetowanie reklamy w mediach społecznościowych, które wykorzystywały algorytmy do precyzyjnego docierania do potencjalnych ofiar ataku. Przestępcy w przygotowywanych materiałach podszywali się pod bardzo znane osoby, instytucje, spółki Skarbu Państwa czy podmioty z sektora finansowego (grafika 4 i 5).

Grafika 4. Przykłady reklam fałszywych inwestycji, które publikowali cyberprzestępcy

Źródło: *Raport roczny CSIRT KNF 2024*, Urząd Komisji Nadzoru Finansowego, Warszawa 2025, s. 16.

[55] Tamże, s. 15.

Grafika 5. Przykłady reklam fałszywych inwestycji, które publikowali cyberprzestępcy



Źródło: *Raport roczny CSIRT KNF 2024*, Urząd Komisji Nadzoru Finansowego, Warszawa 2025, s. 16.

- Etap przekonywania w ramach którego dochodzi do prezentowania wymyślonych historii sukcesu inwestycyjnego, bardzo często z udziałem rzekomych „ekspertów". W etapie tym dochodzi również do symulowania zysków, które zachęcają potencjalnych klientów do dokonywania większych wpłat. Etap ten charakteryzuje się również stosowaniem presji, np. oferowaniem ograniczonych ofert promocyjnych, tak aby zachęcić ofiarę do natychmiastowego podejmowania decyzji i inwestowania.
- Etap wyłudzenia[56].

Działalność edukacyjna Komisji Nadzoru Finansowego w zakresie cyberbezpieczeństwa

Ustrojowa regulacja dotycząca działalności KNF wśród zadań tego organu wymienia również obszar edukacji. Zgodnie z brzmieniem art. 4 ust. 1 pkt 4 ustawy o nadzorze nad rynkiem finansowym do zadań KNF należy podejmowanie działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego, jego zagrożeń oraz podmiotów na nim funkcjonujących w celu ochrony uzasadnionych interesów uczestników rynku finansowego. Bez wątpienia norma ta odnosi się również do działań edukacyjnych w zakresie bezpieczeństwa w cyberprzestrzeni. Na przestrzeni ostatnich kilku lat KNF zrealizowała szereg aktywności w tym wymiarze, zaznaczając, że działania edukacyjne są istotnym elementem budowania świadomości zagrożeń dla wzmacniania poziomu cyberbezpieczeństwa użytkowników Internetu.

[56] Tamże, s. 15–21.

W strukturze Urzędu Komisji Nadzoru Finansowego powołano Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego. Misją tej jednostki jest „edukować i ostrzegać, a aktywności CEBRF obejmują zarówno sferę wirtualną (webinary i ostrzeżenia), jak i działania terenowe (szkolenia w szkołach, dzielenie się wiedzą na konferencjach i kongresach, organizacja wydarzeń)"[57]. Wśród aktywności zrealizowanych w ramach CEBRF warto wymienić m.in. quizy, encyklopedię cyberbezpieczeństwa, seminaria i webinary dla różnych grup odbiorców, m.in. dla uczniów i nauczycieli oraz rodziców i opiekunów, seniorów i ich opiekunów, a także indywidualnych uczestników rynku finansowego.

W wymiarze edukacyjno-informacyjnym należy również zwrócić uwagę na aktywność KNF w mediach społecznościowych. Zespół CSIRT KNF prowadzi profile w mediach społecznościowych, tj. na portalach X, Facebook i LinkedIn. Zamieszczane są w nich informacje i ostrzeżenia dotyczące najnowszych sposobów działania cyberprzestępców oraz oszustw internetowych. W ciągu 2024 r. przygotowano i opublikowano 254 informacje. Na bazie materiałów przygotowywanych przez CSIRT KNF w 2024 r. powstało ponad dwa tysiące artykułów w portalach branżowych oraz informacyjnych o zasięgu ogólnopolskim[58].

Ostrzeżenia i informacje publikowane przez CSIRT KNF dotyczyły m.in. fałszywych stron bankowości elektronicznej, złośliwego oprogramowania specjalizującego się w kradzieży środków finansowych, fałszywych produktów inwestycyjnych wyłudzających dane od użytkownika, fałszywych stron portali sprzedażowych wyłudzających dane kart płatniczych, fałszywych stron firm kurierskich wyłudzających dane kart płatniczych[59].

Edukacja w zakresie cyberbezpieczeństwa – kluczowe wnioski z badań empirycznych

W tej części artykułu zaprezentowane zostaną zagadnienia związane z kwestią edukacji w zakresie cyberbezpieczeństwa oraz główne wnioski płynące z dostępnych badań empirycznych oraz doświadczeń autorów wynikających z obserwacji uczestniczącej wynikającej z zatrudnienia w podmiotach rynku finansowego.

---

[57] Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego, Urząd Komisji Nadzoru Finansowego, https://cebrf.knf.gov.pl/, Strona Główna CEBRF. Zob. także: B. Godusławski, *Nadzór ma plan na edukacyjną walkę z cyberprzestępcami*, «Dziennik Gazeta Prawna», 14 października 2021 r., źródło: GazetaPrawna.pl, https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8271531,knf-plan-na-edukacyjna-walke-z-cyberprzestepcami.html (8.04.2025).

[58] *Raport roczny CSIRT KNF 2024*…, s. 64.

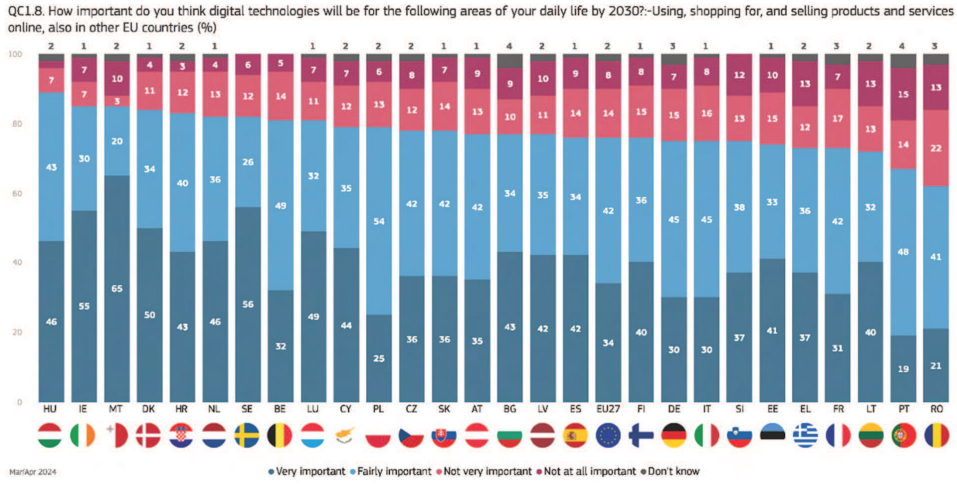
[59] Tamże.

Korzystanie z usług cyfrowych, w tym finansowych jest w Europie coraz bardziej popularne. Okres pandemii przyspieszył trend cyfryzacji wielu obszarów życia, a badania prowadzone wśród obywateli 27 państw UE potwierdzają, że jest to proces wręcz pożądany. W badaniu *„Digital Decade"*, przeprowadzonym na zlecenie Komisji Europejskiej w 2024 r. prawie trzy czwarte (73%) respondentów stwierdza, że cyfryzacja usług publicznych oraz prywatnych czyni ich życie łatwiejszym[60]. W przypadku polskich respondentów było to aż 81%. W tym samym badaniu, na pytanie, jak ważne będą technologie cyfrowe w wielu obszarach ich codziennego życia do 2030 r., około 75% badanych twierdzi, że będą istotne, a ponadto od czasu badania z 2023 r. następuje wzrost postrzegania znaczenia takich obszarów, jak:

- korzystanie z produktów i usług online, dokonywanie zakupów i ich sprzedaż (76%),
- dostęp do usług transportowych i korzystanie z nich (76%),
- dostęp do możliwości kształcenia i szkolenia (75%),
- dostęp do materiałów/treści online, interakcje z nimi lub ich tworzenie (74%),
- angażowanie się w życie demokratyczne (74%),
- pomoc w walce ze zmianą klimatu (74%).

Blisko 70% respondentów oczekuje, że technologie cyfrowe będą istotne dla pracy zdalnej. Polscy respondenci podkreślili znaczenie podwyższenia standardu dostępności usług dostarczania internetu (80%), a na drugim miej-

Wykres 2. Spodziewany wzrost istotności komercyjnych usług cyfrowych w codziennym życiu obywateli 27 państw EU – do roku 2030



Źródło: *Digital Decade*, Eurobarometer, Komisja Europejska, lipiec 2024 r.

60 *Digital Decade*, Eurobarometer, Komisja Europejska, lipiec 2024 r.

scu (77%) umieścili potrzebę podniesienia cyberbezpieczeństwa, bezpieczeństwa danych i technologii cyfrowych.

Konieczność zapewnienia cyberbezpieczeństwa obywatelom UE została wskazana jako jeden z priorytetów unijnej Strategii Cyberbezpieczeństwa. Została ona podkreślona m.in. w komunikacie do Rady i Parlamentu Europejskiego[61]. Stwierdzono w nim, że „cyberbezpieczeństwo jest integralną częścią bezpieczeństwa Europejczyków. Niezależnie od tego, czy są to podłączone urządzenia, sieci elektroenergetyczne, czy banki, samoloty, administracje publiczne lub szpitale, z których korzystają lub które odwiedzają, ludzie zasługują na to, aby robić to z zapewnieniem, że będą chronieni przed cyberzagrożeniami. Gospodarka, demokracja i społeczeństwo UE bardziej niż kiedykolwiek polegają na bezpiecznych i niezawodnych narzędziach cyfrowych i łączności. Cyberbezpieczeństwo jest zatem niezbędne do budowania odpornej, zielonej i cyfrowej Europy"[62].

Państwa członkowskie rozpoczęły działania na rzecz poprawy bezpieczeństwa cyfrowego. Niestety – zdaniem autorów – w Polsce nie nadążamy za tymi wyzwaniami w obszarze edukacji w zakresie cyberbezpieczeństwa, co zostało potwierdzone badaniem Najwyższej Izby Kontroli, przeprowadzonym w trakcie kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości".

Badanie przeprowadzono w okresie 20–28 kwietnia 2022 r. na reprezentatywnej, ogólnopolskiej próbie 1000 pełnoletnich mieszkańców Polski, z wykorzystaniem metody telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI). Na szczególną uwagę w kontekście niniejszych rozważań, zasługuje obszar badania dotyczący działań edukacyjnych zwiększających wiedzę obywateli na temat cyberprzestępczości. Celem badania było m.in. ustalenie deklarowanego przez respondentów stanu wiedzy na temat aktualnych zagrożeń występujących w cyberprzestrzeni oraz zweryfikowanie działań podejmowanych przez obywateli i właściwe organy państwa, w sytuacji faktycznego ataku przestępców komputerowych[63]. Przeprowadzone badanie wykazało, że 77% ankietowanych uważa, że przestępstwa internetowe stanowią dla nich realne zagrożenie, a sześciu na dziesięciu badanych użytkowników Internetu (58%) poszukuje informacji na temat nie-

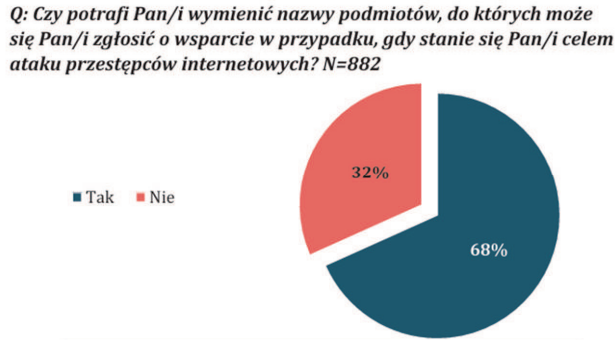
61 *The EU's Cybersecurity Strategy for the Digital Decade*, Joint Communicate to European Parliament and The Council, Brussels, 16.12.2020 r.

62 Tamże.

63 Informacja o wynikach kontroli *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Nr ewid. 125/2022/P/21/042/KPB, Najwyższa Izba Kontroli, Warszawa, 24 listopada 2022 r., s. 41.

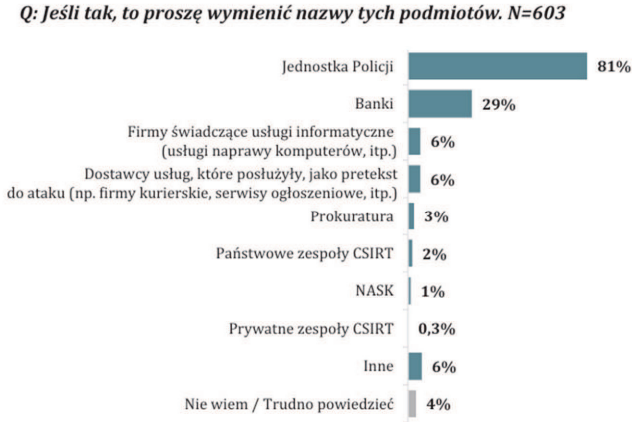
bezpieczeństw związanych z korzystaniem z sieci[64]. Większość respondentów deklarowała, że wie co robić i do jakiej instytucji się zgłosić w przypadku zaistnienia cyberzagrożenia.

Wykres 3. Znajomość instytucji państwa wspierających obywateli w sytuacji cyberzagrożenia



Źródło: Informacja o wynikach kontroli *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Nr ewid. 125/2022/P/21/042/KPB, Najwyższa Izba Kontroli, Warszawa, 24 listopada 2022 r., s. 43.

Wykres 4. Znajomość instytucji państwa wspierających obywateli w sytuacji cyberzagrożenia



Źródło: Informacja o wynikach kontroli *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Nr ewid. 125/2022/P/21/042/KPB, Najwyższa Izba Kontroli, Warszawa, 24 listopada 2022 r., s. 43.

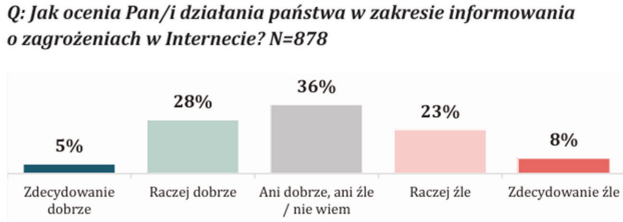
W rzeczywistości większość ankietowanych (81%) wskazywała na jednostki Policji, jako właściwe i kompetentne do udzielenia im pomocy. Warte odnotowania jest również to, że kolejną grupą podmiotów, gdzie respondenci szukaliby pomocy, są banki. Świadczy to o tym, że cyfrowe usługi finansowe

64 Tamże.

są szczególnie ważnym obszarem aktywności społecznej. Banki oraz pozostali operatorzy rynku finansowego nieustannie rozbudowują tzw. ekosystemy usług finansowych oraz niefinansowych, w celu zwiększania satysfakcji klientów, i tym samym maksymalizacji dochodów. W obrębie wspomnianych ekosystemów dochodzi do zetknięcia się świata finansowego ze światem cyberzagrożeń.

To samo badanie wskazuje na relatywnie dobrze wypełnianą funkcję edukacyjną realizowaną przez państwo w zakresie cyberzagrożeń. Jednak pogłębiona analiza szczegółowych odpowiedzi ujawnia inny obraz. Wśród 884 badanych korzystających z Internetu, aż 404 respondentów padło ofiarą różnych form cyberataków, przy czym część z nich (21% ofiar) zostało poszkodowanych co najmniej dwukrotnie. Tylko nieliczni respondenci zgłosili incydent na Policję, czy do właściwego zespołu CSIRT, a niektórzy nie podjęli żadnych działań (np. nie dokonali zmiany hasła do konta bankowego, czy konta w mediach społecznościowych). Powyższe uzasadniali m.in. brakiem wiedzy na temat możliwości zgłaszania tego rodzaju incydentów oraz niskim zaufaniem do skuteczności działań instytucji publicznych[65].

Wykres 5. Ocena działań edukacyjnych państwa przez grupę badawczą



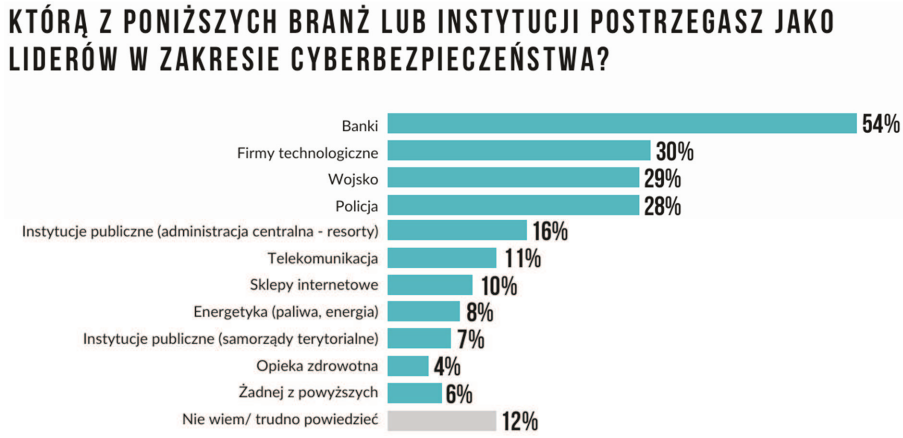
Źródło: Informacja o wynikach kontroli *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, Nr ewid. 125/2022/P/21/042/KPB, Najwyższa Izba Kontroli, Warszawa, 24 listopada 2022 r., s. 43.

Podsumowując, Izba stwierdziła brak skuteczności działań państwa w zakresie edukowania obywateli na temat cyberzagrożeń oraz zasad postępowania w sytuacji ataku cyberprzestępców. Jednocześnie z wyników tego badania dowiadujemy się, że Polacy nieszczególnie pogłębiają swoją wiedzę w zakresie cyberbezpieczeństwa i widzą istotną rolę banków w omawianym wymiarze. Sfera finansów i sfera cyberzagrożeń są coraz bardziej ze sobą powiązane, ponieważ Polacy chętnie i coraz aktywniej korzystają z cyfrowych usług finansowych. Jednocześnie jest widocznym to, że cedują odpowiedzial-

[65] Tamże, s. 44.

ność za swoje cyfrowe bezpieczeństwo na dostarczycieli usług oraz instytucje nadzorujące[66].

Wykres 6. Postrzeganie liderów cyberbezpieczeństwa przez Polaków



Źródło: *Postawy Polaków wobec cyberbezpieczeństwa 2024 – wybrane dane z badania*, Warszawski Instytut Bankowości, Związek Banków Polskich, lipiec 2024 r.

Ze względu na wysoką ocenę znaczenia banków w obszarze cyberbezpieczeństwa warto – choćby sygnalnie – przywołać raport „Cyberbezpieczny Portfel", zawierający wyniki badania „Postawy Polaków wobec cyberbezpieczeństwa 2024". Badanie wykonano w formie ankiety online na reprezentatywnej próbie 1007 osób (Polek i Polaków) w wieku 18–50+. Jest to kontynuacja cyklicznego badania, a raport publikowany jest co 2 lata od 2016 r. Kluczowe wnioski z badania opublikowane w raporcie z 2024 r. są następujące:

- 60% respondentów obawia się, że w cyfrowym świecie zostaną wyłudzone ich dane, a 52%, że pieniądze,
- 49% badanych uważa, że AI jest zarówno szansą jak i zagrożeniem dla człowieka, ale przeciwników AI jest prawie dwukrotnie więcej od zwolenników,
- 51% Polaków obawia się kradzieży tożsamości, a 42% fake newsów i dezinformacji,
- 86% respondentów czuje się bezpiecznie korzystając z bankowości internetowej lub mobilnej, ale tylko 6% zdecydowanie czuje się bezpiecznie korzystając z Internetu,

[66] *Raport Cyberbezpieczny portfel*, Warszawski Instytut Bankowości, edycja V, październik 2024 r., https://www.zbp.pl/aktualnosci/wydarzenia/Cyberbezpieczny-Portfel-2024 (10.04.2025), s. 7.

- 50% Polaków uważa, że odpowiedzialność za bezpieczeństwo finansowych usług cyfrowych spoczywa na bankach, równocześnie 54% wskazuje banki za liderów cyberbezpieczeństwa,
- 57% badanych korzysta z bankowości mobilnej używając smartfona, a 43% respondentów deklaruje chęć weryfikacji płatności odcinkiem palca lub próbką głosu,
- 48% Polaków posiada tylko orientację w temacie cyberbezpieczeństwa, a 15% wie niewiele,
- 92% uważa, że jest potrzeba edukowania społeczeństwa na temat cyberbezpieczeństwa[67].

Wykres 7. Ocena wiedzy o cyberbezpieczeństwa przez Polaków

Źródło: *Postawy Polaków wobec cyberbezpieczeństwa 2024 – wybrane dane z badania*, Warszawski Instytut Bankowości, Związek Banków Polskich, lipiec 2024 r.

Na bazie powyższego raportu można skonstatować, że Polacy chętnie przyswajają nowinki technologiczne i coraz częściej wykorzystują cyfrowe usługi finansowe, przy niewystarczającym poziomie wiedzy na temat cyberzagrożeń. Tym samym mamy do czynienia z istotnie zwiększającym się ryzykiem systemowym, które nie jest wystarczająco mitygowane. Pewnym pocieszeniem jest fakt, że przeważająca większość respondentów (92%) potwierdza, że wiedza o cyberbezpieczeństwie powinna być stale propagowana. Jednocześnie można wnioskować, że wsparcie w tym zakresie jest praktycznie lokowane w bankach, korzystając z wysokiego poziomu zaufania społecznego wobec usług i procesów tego sektora.

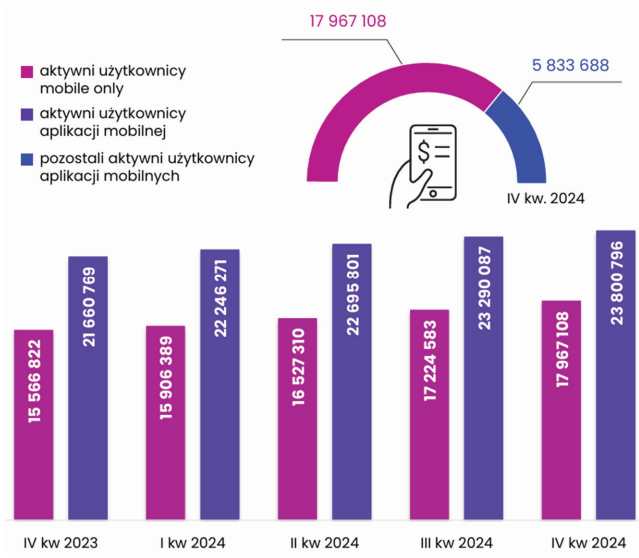
Warto w tym kontekście przyjrzeć się aktywnościom klientów bankowości elektronicznej, a w szczególności mobilnej. Bazując na cyklicznym raporcie „NetBank", publikowanym cyklicznie przez Związek Banków Polskich, można

[67] Tamże, s. 7.

stwierdzić utrzymujący się wzrost liczby klientów korzystających zdalnie z usług bankowych. W czwartym kwartale 2024 r. liczba umów dostępu do bankowości internetowej przekroczyła 44,5 mln, natomiast liczba aktywnych użytkowników aplikacji mobilnej wzrosła do około 24 mln[68].

Dzięki powszechnemu wykorzystaniu telefonów komórkowych, a przede wszystkim smartfonów, wzrasta w szybkim tempie liczba klientów dokonujących operacji lub transakcji finansowych w kanałach mobilnych, gdzie też są szczególnie (i często ze względu na codzienny kontakt z telefonem) narażeni na cyberzagrożenia.

Wykres 8. Liczba klientów bankowości mobilnej



Źródło: *Raport NetBank – bankowość internetowa i mobilna, płatności bezgotówkowe*, Związek Banków Polskich, raport IV kwartał 2024 r.

W czwartym kwartale 2024 r. spośród blisko 24 mln klientów indywidualnych aktywnie korzystających z bankowości mobilnej, aż 18 mln stanowili użytkownicy typu *mobile only*, czyli osoby, które logują się do aplikacji mobilnej co najmniej raz w miesiącu, nie korzystając jednocześnie z bankowości internetowej. Tym samym udział tej grupy wśród wszystkich użytkowników aplikacji mobilnej wzrósł do 76%[69]. Należy się spodziewać dalszego wzrostu liczby użytkowników różnego rodzaju aplikacji mobilnych, ze szczególnym uwzględnieniem aplikacji dedykowanych zarządzaniu finansami oraz inwe-

[68] *Raport NetBank – bankowość internetowa i mobilna, płatności bezgotówkowe*, Związek Banków Polskich, raport IV kwartał 2024 r.

[69] Tamże, s. 11.

stowaniu środków finansowych. Trend ten jest napędzany przez dynamicznie rozwijające się środowisko mocno promowanych, odpowiednio zaprojektowanych pod kątem użytkownika, różnego rodzaju platform inwestycyjnych. Rosnąca popularność instrumentów typu ETF, CFD i kryptowalut jest dodatkowym czynnikiem wzmacniającym przyciąganie nieprofesjonalnych uczestników rynku finansowego do otwierania rachunków na tychże platformach. Sektor bankowy oraz branża maklerska rejestrują odpływ klientów na nowo powstające platformy, i w odpowiedzi na ten trend modyfikują swoją tradycyjną i konserwatywną ofertę produktów inwestycyjnych. Tym samym w systemie finansowym powstaje wzmacniające sprzężenie zwrotne, kierujące uczestników rynku, do eksplorowania w pełni cyfrowej oferty produktów inwestycyjnych.

Zanim dokonana zostanie charakterystyka nieprofesjonalnego uczestnika rynku finansowego w Polsce, warto przywołać podstawowe informacje związane z poziomem wiedzy i kompetencji finansowych tej grupy. Jednym z najważniejszych badań adresujących ten obszar jest raport OECD/INFE: „Znajomość zagadnień finansowych w Polsce". Jest on przygotowany we współpracy z krajową grupą roboczą ds. strategii edukacji finansowej w Polsce i na bazie wkładu DG REFORM Komisji Europejskiej. Projekt 21PL32 „Opracowanie Krajowej Strategii Edukacji Finansowej (KSEF) w Polsce" rozpoczął się w październiku 2021 r.

Główne wnioski tego raportu dotyczące kompetencji finansowych są następujące[70]:

- mieszkańcy Polski, zwłaszcza ci znajdujący się w trudnej sytuacji materialnej, potrzebują wsparcia w zwiększeniu swojej odporności finansowej – mimo że prawie 95% Polaków podejmuje na co dzień decyzje finansowe, mniej niż trzy czwarte ma plan zarządzania swoimi dochodami i wydatkami, a tylko połowa uważnie śledzi swoje osobiste sprawy finansowe;
- mieszkańcy Polski powinni odzyskać pewność i zaufanie do sektora finansowego w celu zwiększenia absorpcji i wykorzystania oferowanych przez instytucje finansowe produktów oszczędnościowych, inwestycyjnych i emerytalnych;
- mieszkańcy Polski powinni mieć świadomość, że długoterminowe oszczędzanie jest ważne dla ich przyszłego dobrostanu finansowego, oraz posiadać umiejętności podejmowania długoterminowych decyzji oszczędnościowych i inwestycyjnych. Mimo że 73% Polaków obawia się ubóstwa w podeszłym wieku, są oni bardziej skłonni skupiać się na krótkotermino-

[70] *Financial Literacy in Poland: Relevance, evidence and provision. Znajomość zagadnień finansowych w Polsce: Znaczenie, dane i oferta edukacyjna*, OECD 2022, https://www.oecd.org/finance/financial-education/Financial-Literacy-Poland-Polish.pdf (22.04.2025).

wych potrzebach finansowych i nie planują przyszłego zabezpieczenia finansowego;
- mieszkańcy Polski powinni posiadać niezbędne umiejętności finansowe, by korzystać z możliwości oferowanych przez rynki kapitałowe, a jednocześnie zarządzać ryzykiem. Obecnie, mimo dobrego zrozumienia pojęć ryzyka i zwrotu, bardzo mały odsetek Polaków inwestuje swoje pieniądze na rynkach kapitałowych (zaledwie 8%), a wielu woli trzymać swoje oszczędności w postaci gotówki lub lokaty bankowej;
- mieszkańcy Polski powinni potrafić mądrze zarządzać kredytem. W porównaniu z innymi krajami UE stosunkowo niewiele Polaków jest nadmiernie zadłużonych (około 20%) lub zagrożonych ryzykiem nadmiernego zadłużenia, ale dla wielu osób z tych grup dług jest obciążeniem;
- mieszkańcy Polski powinni poprawić swoją zdolność do zachowania bezpieczeństwa w Internecie oraz czerpania korzyści z cyfrowych usług finansowych. W porównaniu ze średnią UE podstawowe umiejętności cyfrowe Polaków są na niskim poziomie. Edukacja finansowa, obok umiejętności cyfrowych, może umożliwić konsumentom finansowym czerpanie korzyści z cyfryzacji przy jednoczesnym zachowaniu bezpieczeństwa finansowego w Internecie.

Podsumowaniem tej części diagnozy w raporcie OECD jest rekomendacja adresująca wspomniane potrzeby polskiego społeczeństwa, które powinny być zaadresowane poprzez konkretne projekty będące elementami Krajowej Strategii Edukacji Finansowej. Szczególnie ważnym elementem analizy jest połączenie procesu zwiększania edukacji finansowej z edukacją w zakresie cyberbezpieczeństwa.

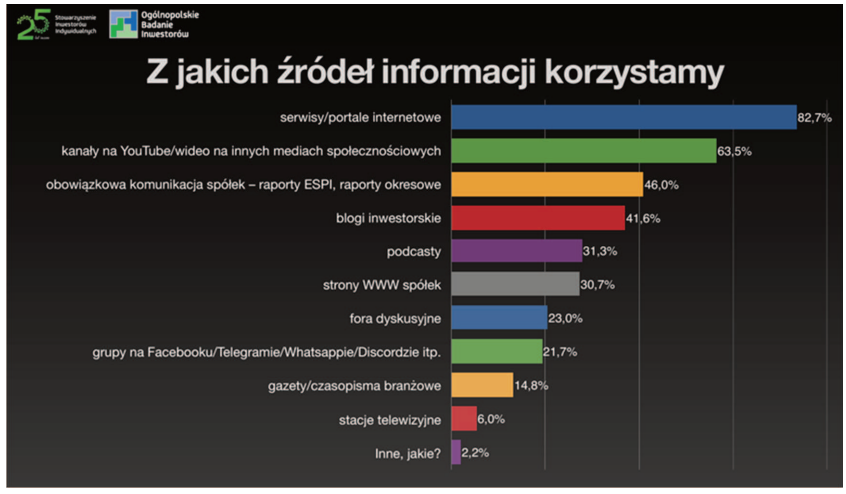
Przywoływana już wielokrotnie branża finansowa ma świadomość relatywnie niskiej wiedzy finansowej zarówno obecnych, jak i potencjalnych klientów. W szczególności dotyczy to wiedzy i kompetencji w zakresie inwestowania. Wynika to częściowo z wypełniania obowiązków regulacyjnych wprowadzonej 3 stycznia 2018 r. dyrektywy MIFID II (*Markets in Financial Instruments Directive*), której przepisy wymagają sprawdzania przez banki stopnia zrozumienia proponowanego produktu przez klienta, a także jego wiedzy ogólnej na temat usług inwestycyjnych i produktów finansowych[71]. Klient przechodząc przez test adekwatności musi wykazać się zrozumieniem ryzyka związanego z daną transakcją, a bank ocenić, czy produkt lub usługa maklerska jest dla niego odpowiednia w kontekście celów inwestycyjnych oraz sytuacji finansowej. Proces zbierania informacji na bazie ankiet daje pewien wstępny obraz poziomu

[71] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (wersja przekształcona) (Dz. Urz. UE L 173 z 2014 r., s. 349 ze zm.).

wiedzy finansowej, jak i doświadczenia przyszłych uczestników rynku finansowego. Obraz ten jest regularnie uzupełniany przez badania prowadzone przez branżę biznesową wspólnie z uczelniami, firmami konsultingowymi oraz stowarzyszeniami takimi, jak np.: Izba Domów Maklerskich (IDM), Izba Zarządzających Funduszami i Aktywami (IZFiA), Stowarzyszenie Inwestorów Indywidualnych (SII).

Jednym z największych i regularnie wykonywanych badań polskich inwestorów jest Ogólnopolskie Badanie Inwestorów przygotowywane przez Stowarzyszenie Inwestorów Indywidualnych. Edycja z 2024 r. objęła 4374 inwestorów. Jeśli chodzi o podejście inwestorów do informacji i edukacji finansowej, widać, że dominują źródła internetowe wraz z mediami społecznościowymi[72].

Wykres 9. Źródła informacji finansowej nieprofesjonalnych uczestników rynku



Źródło: *Długi termin, ETF-y, obligacje i zagranica, czyli w co i jak inwestuje polski inwestor w 2024 r. 22 Ogólnopolskie badanie inwestorów 2024*, Stowarzyszenie Inwestorów Indywidualnych, 29 listopada 2024 r., s. 39.

Zbliżony obraz w zakresie edukacji finansowej wyłania się z innego raportu – na bazie badania przeprowadzonego wspólnie przez Uniwersytet Warszawski oraz firmę Accenture. W raporcie z badania mówi się o „demokratyzacji inwestowania" – trendzie zwiększonej przejrzystości rynku, o lepszym dostępie do edukacji finansowej i o rozwoju intuicyjnych i tanich platform transakcyjnych[73].

[72] *Długi termin, ETF-y, obligacje i zagranica, czyli w co i jak inwestuje polski inwestor w 2024 r. 22 Ogólnopolskie badanie inwestorów 2024,* Stowarzyszenie Inwestorów Indywidualnych, 29 listopada 2024 r., s. 39.

[73] *Inwestor indywidualny w Polsce: autoportret vs. spojrzenie branży*, raport przygotowany przez: Accenture i Uniwersytet Warszawski, marzec 2025 r., s. 6.

Grafika 6. Ocena wiedzy finansowej klientów biur maklerskich

Źródło: *Inwestor indywidualny w Polsce: autoportret vs. spojrzenie branży*, raport przygotowany przez: Accenture i Uniwersytet Warszawski, marzec 2025 r.

Trend ten jest widoczny w Polsce, mimo że w dalszym ciągu ocena i samoocena wiedzy wśród klientów biur maklerskich stoi na niskim poziomie[74].

Kolejnym badaniem potwierdzającym potrzebę zwiększania poziomu edukacji finansowej Polaków jest czwarta edycja projektu badawczego „Polak inwestor". Udział w nim wzięło blisko 1300 osób, z całej Polski, najwięcej z województwa mazowieckiego, w tym 697 inwestujących oraz 575 nieinwestujących. Większość inwestorów (51,8%) uważa swoją wiedzę na temat inwestowania za przeciętną. Do posiadania znacznej wiedzy przyznaje się 27,4% inwestorów, a do bardzo małej 16,8%, 3,4% osób deklaruje dysponowanie profesjonalną wiedzą, a 0,6% określa, że nie ma żadnej wiedzy.

Tabela 1. Samoocena wiedzy inwestycyjnej (%) inwestorów i nieinwestujących

	Cała próba	**Inwestorzy**	**Nieinwestujący**
Nie mam w ogóle takiej wiedzy (1)	13,8	0,6	29,9
Moja wiedza jest mała (2)	26,3	16,8	37,3
Moja wiedza jest przeciętna (3)	41,9	51,8	29,9
Moja wiedza jest znaczna (4)	16,0	27,4	2,2
Moja wiedza jest profesjonalna (5)	2,1	3,4	0,5

Źródło: *Polak inwestor 2024. Raport z badania polskich inwestorów*, iKsync, Warszawa–Kraków 2024, s. 129.

74 Tamże, s. 19.

Z kolei blisko 30% osób nieinwestujących deklaruje nieposiadanie żadnej wiedzy (29,9%), a małą wiedzę 37,3% i następnie przeciętną wiedzę wskazuje 29,9%. W obydwu badanych grupach brak odpowiedniej wiedzy inwestycyjnej jest przeważający[75]. Nie powinno być zaskoczeniem to, jakie powody nieinwestowania wybrali nieinwestujący respondenci. Najczęściej wskazywanym powodem jest brak odpowiednich środków finansowych – deklarowało to aż 69% respondentów. Jednak drugą barierą jest brak wiedzy – tak odpowiedziało aż 51% uczestników badania. Strach przed stratą wskazuje 32%, a niepokój i dyskomfort przy podejmowaniu decyzji – deklaruje 22% respondentów[76].

Wymienione powyżej badanie potwierdzają zgodnie fakt, że wiedza oraz kompetencje finansowe Polaków stoją na stosunkowo niskim poziomie i stwarzają barierę powstrzymującą ich od inwestowania, co sugeruje potrzebę wdrożenia skuteczniejszych niż dotychczasowe, metod promowania edukacji finansowej, jak również z zakresu korzystania z narzędzi internetowych, takich jak platformy i mobilne aplikacje inwestycyjne.

Podsumowanie i wnioski

Rekapitulując rozważania niniejszego artykułu należy stwierdzić, że system cyberbezpieczeństwa rynku finansowego w Polsce jest właściwie ukształtowany w wymiarze prawnym, jak i organizacyjnym. W styczniu 2025 r. weszło w życie rozporządzenie DORA. Jest to kluczowy akt prawny kształtujący system cyberbezpieczeństwa podmiotów rynku finansowego na poziomie unijnym. W wymiarze prawa krajowego od kilku lat obowiązuje ustawa o krajowym systemie cyberbezpieczeństwa. Została ona uchwalona jako implementacja dyrektywy NIS. W ostatnich latach przygotowano kilka projektów nowelizacji tej regulacji, jednak nie została ona finalnie uchwalona przez parlament.

Należy również podkreślić, że prawodawca krajowy planuje uchwalenie ustawy wdrażającej rozporządzenie DORA do polskiego porządku prawnego. W kwietniu 2024 r. na stronie Rządowego Centrum Legislacji zamieszczono projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego wdrażający do prawa krajowego oraz zapewniający stosowanie rozporządzenie DORA oraz towarzyszącą mu dyrektywę 2022/2556. Regulacja ta ma na celu dostosowanie obowiązującego już prawa do zasad ukształtowanych w rozporządzeniu DORA. Projekt zakłada wprowadzenie zmian w tzw. ustawach sektorowych odnoszących się

[75] *Polak inwestor 2024. Raport z badania polskich inwestorów*, iKsync, Warszawa–Kraków 2024, s. 71.

[76] Tamże, s. 111.

do poszczególnych segmentów rynku finansowego, takich jak rynek płatniczy, bankowy czy ubezpieczeniowy[77].

Podwyższenie poziomu wiedzy finansowej powinno iść równolegle ze zwiększaniem kompetencji w zakresie wykorzystania narzędzi ICT do zarządzania finansami i inwestowania. Potwierdzają to zarówno raporty i badania krajowe, jak również raporty OECD. Potrzebę taką dostrzegła również Komisja Europejska, która opublikowała 24 maja 2023 r. pakiet *Retail Investment Strategy* (RIS), którego celem ma być rozwój rynku inwestycji wśród nieprofesjonalnych uczestników rynku. Chodzi o zbudowanie zaufania inwestorów detalicznych do rynków kapitałowych, zapewnienie im wiedzy i informacji niezbędnych do inwestowania. Projekt reguluje również procesy zwiększania świadomości takich zjawisk jak gamifikacja, cyberzagrożenia i pełnych konsekwencji wykorzystania narzędzi cyfrowych podczas inwestowania. Wśród wielu propozycji modyfikujących poprzednią dyrektywę MIFID II, pojawia się propozycja testu adekwatności cyfrowej – *Digital Suitability Test*. Miałby on pełnić rolę wspierającą nieprofesjonalnych uczestników rynku w procesie inwestowania przy wykorzystaniu cyfrowych narzędzi i platform[78]. Jakkolwiek nie znamy jeszcze finalnej wersji dyrektywy oraz przepisów wykonawczych – sam fakt połączenia potrzeby podwyższenia kompetencji finansowych ze zwiększaniem świadomości cyberzagrożeń jest zdecydowanie słusznym kierunkiem unijnego prawodawcy.

Syntetyzując rozważania należy stwierdzić, że cyberbezpieczeństwo ma – zwłaszcza w kontekście obecnej sytuacji geopolitycznej – fenomenalne znaczenie dla bezpieczeństwa państwa, jego instytucji, a także rynku finansowego i jego interesariuszy. Zwiększanie odporności cyfrowej rynku finansowego (ale i szerzej w wymiarze państwa) wymaga działań skoordynowanych i holistycznych. Powinny one obejmować zarówno działania w zakresie tworzenia ram legislacyjnych i organizacyjnych, współpracy, jak i działań o charakterze informacyjnym i edukacyjnym. Zwiększanie poziomu świadomości i wiedzy interesariuszy rynku finansowego na temat zagrożeń w cyberprzestrzeni, cyberhigieny, wykorzystywanych wektorów ataków oraz skutków niestosowania się do zaleceń ekspertów od cyberbezpieczeństwa jest niezbędne. Bez tych działań osiągnięcie celu jakim jest zwiększenie odporności cyfrowej rynku

[77] J. Byrski, P. Rodzynkiewicz, *Prace nad wdrożeniem polskiej ustawy wdrażającej Digitial Operational Resilience Act*, TKP the law, 8 lipca 2024 r., źródło: prace nad wdrożeniem polskiej ustawy wdrażającej Digitial Operational Resilience Act – Kancelaria Traple Konarski Podrecki i Wspólnicy (8.04.2025).

[78] F. Annunziata, *Retail Investment Strategy – How to boost retail investors'participation in financial markets*, Publication for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2023.

finansowego nie będzie możliwe. Należy bowiem pamiętać, że nadal najsłabszym ogniwem w „wirtualnym/cyfrowym krwioobiegu" jest człowiek. Najlepsze regulacje prawne, zaawansowany *hardware* i *software* nie wyeliminują błędów człowieka.

Bibliografia

Annunziata F., *Retail Investment Strategy – How to boost retail investors'participation in financial markets*, Publication for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg 2023.

Banasiński C. (red.), *Cyberbezpieczeństwo*, Warszawa 2018.

Banasiński C., Rojszczak M., Chmielewski J. M., Hydzik W., Łuczak J., Nowak W., Waćkowski K. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.

Banaszczak-Soroka U., Zawadzka P., *Struktura systemu finansowego*, [w:] U. Banaszczak-Soroka (red.), *Rynki finansowe. Organizacja, instytucje, uczestnicy*, Warszawa 2019.

Biderman B., Mroczka K., *Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce*, «Bezpieczny Bank» 2022, nr 2(87).

Bień W., *Rynek papierów wartościowych*, Warszawa 2004.

Bilski J., Janicka M., Miziołek T., *Międzynarodowy system finansowy*, Łódź 2016.

Borkowska E., *DORA już obowiązuje, ale brakuje przepisów krajowych*, 3 lutego 2025 r., Legalis.

Byrski J., Kurek-Sobieraj A., *Od redaktorów*, [w:] J. Byrski, A. Kurek-Sobieraj (red.), *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz*, Warszawa 2025.

Byrski J., Rodzynkiewicz P., *Prace nad wdrożeniem polskiej ustawy wdrażającej Digitial Operational Resilience Act*, TKP the law, 8 lipca 2024 r., źródło: prace nad wdrożeniem polskiej ustawy wdrażającej Digitial Operational Resilience Act – Kancelaria Traple Konarski Podrecki i Wspólnicy (8.04.2025).

Czarny B., Rapacki R., *Podstawy ekonomii*, Warszawa 2002.

Godusławski B., *W KNF rusza specjalny zespół, który pomoże instytucjom finansowym przeciwstawić się cyberprzestępcom*, «Dziennik Gazeta Prawna», 9 czerwca 2020, W KNF rusza specjalny zespół, który pomoże instytucjom finansowym przeciwstawić się cyberprzestępcom, GazetaPrawna.pl (10.05.2025).

Iwanicz-Drozdowska M., *Edukacja finansowa*, «infos BAS» 2010, nr 15(85).

Mroczka K., Maderak K., Zieliński K., *Nadzór nad cyberbezpieczeństwem rynku finansowego w Polsce*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Informatyzacja, cyfryzacja i danetyzacja*, Warszawa 2021.

Mroczka K., Piekutowski P., *Cyber safe place – ochrona cyberbezpieczeństwa rynku finansowego jako zyskujące na znaczeniu zadanie Komisji Nadzoru Finansowego*, [w:] J. Stelmach (red.), *Bezpieczeństwo terrorystyczne budynków użyteczności publicznej. Tom 4. Bezpieczeństwo w cyberprzestrzeni oraz praktyczny wymiar zabezpieczeń technicznych*, Warszawa 2022.

Mroczka K., *Uwarunkowania i kierunki zmian w procesach decydowania publicznego na szczeblu samorządowym w związku z pandemią koronawirusa*, «Polityka i Społeczeństwo» 2020, nr 4(18).

Rakowska M., *Edukacja finansowa dla przyszłości*, obserwatorfinansowy.pl, Obserwator Finansowy: ekonomia, debata, Polska, świat (9.04.2025).

Samuelson P., Nordhaus W., *Ekonomia*, Warszawa 1995.

Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, «Prawo w Działaniu» 2023, nr 53.

Stachoń M., *Foresight Cybersecurity Threats for 2030 – raport ENISA*, «NASK Cyber Policy», 9 kwietnia 2024 r., Foresight Cybersecurity Threats for 2030 – raport ENISA – Cyberpolicy NASK (10.04.2025).

Szkurłat A., *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, «internetowy Kwartalnik Antymonopolowy i Regulacyjny», 2020, nr 2(9).

Wajda P., *Cyberbezpieczeństwo – sektorowe aspekty regulacyjne*, «internetowy Kwartalnik Antymonopolowy i Regulacyjny» 2020, nr 2(9).

Wajda P., *Rola decyzji administracyjnej w nadzorze nad polskim systemem finansowym*, Warszawa 2009.

Zawadzka P., *Modele nadzoru rynku finansowego. Aspekty prawne*, Warszawa 2017.