DOI: 10.26354/bb.3.2.87.2022

Bartosz Biderman*
ORCID: 0000-0002-8503-5207
bartosz.biderman@knf.gov.pl

Kamil Mroczka**
ORCID: 0000-0003-3809-3479
ks.mroczka@uw.edu.pl

Uwarunkowania prawne nadzoru nad cyberbezpieczeństwem rynku finansowego w Polsce

Streszczenie

Zasadniczym celem artykułu jest analiza uwarunkowań prawnych kształtujących system cyberbezpieczeństwa rynku finansowego w Polsce. Autorzy dokonują dogmatyczno-prawnej analizy przepisów prawa krajowego oraz – częściowo – unijnego, a następnie omawiają implementację tych przepisów w sektorze finansowym. Analizie poddano rolę i pozycję KNF jako organu właściwego do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych. Zaprezentowano katalog zadań tej instytucji oraz działania jakie zostały podjęte w celu ich właściwej realizacji. Pogłębionej analizie poddano również rekomendacje i wytyczne przyjęte przez Komisję w zakresie cyberbezpieczeństwa oraz zwrócono uwagę na ich specyficzny charakter prawny. Przeanalizowano również proces tworzenia zespołu CSIRT KNF oraz omówiono jego szczególną rolę w budowaniu cyberodporności polskiego systemu cyberbezpieczeństwa. Zwrócono uwagę zwłaszcza na istotę edukacji finansowej, podkreślając konieczność prowadzenia kampanii informacyjno-edukacyjnych w zakresie cyberbezpieczeństwa. We wnioskach zawarto uwagi autorów w zakresie dalszego rozwoju cyberzagrożeń oraz zaprezentowano koncepcje przeciwdziałania im.

Słowa kluczowe: Komisja Nadzoru Finansowego, cyberbezpieczeństwo, rynek finansowy, krajowy system cyberbezpieczeństwa

JEL: G32, L88, M15, F52

* Bartosz Biderman – doktorant Wojskowej Akademii Technicznej.
** Kamil Mroczka – dr, MBA, Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, dyrektor generalny Urząd Komisji Nadzoru Finansowego.

Legal status of supervision over cybersecurity of the financial market in Poland

Abstract

The essential purpose of the paper is to analyse the legal conditions determining the system of cybersecurity of the financial market in Poland. The authors have performed a dogmatical legal analysis of provisions of the Polish and, partly, EU legislation and then discussed the implementation of the provisions in the financial sector. The analysis covers the role and position of the KNF Board as an authority competent for cybersecurity for the banking sector and the infrastructure of financial markets. The paper also presents a catalogue of the institution's tasks and activities that have been undertaken to perform the tasks properly. The paper includes an in-depth analysis of recommendations and guidelines adopted by the KNF Board in the area of cybersecurity, and points their specific legal nature. The paper also explores the process of establishing the CSIRT KNF team and discusses its special role in building cyber resilience of the Polish cybersecurity system. Special emphasis is placed on the important role of financial education, in particular the need to run awareness-raising and educational campaigns regarding cybersecurity. The conclusions include the authors' free thoughts on the further development of cyber threats and a presentation of ideas on how to prevent them.

Key words: KNF Board, cyber security, financial market, national cyber security system

Wstęp

Cyberbezpieczeństwo w ostatnich kilkudziesięciu miesiącach stało się kluczowym zagadnieniem agendy zarówno instytucji państwowych, jak i innych organizacji, a także osób indywidualnych. Zagadnieniem tym w coraz większym stopniu interesują się również podmioty rynku finansowego. Działania związane z cyberbezpieczeństwem były przedmiotem intensywnych działań legislacyjnych, zarówno na szczeblu krajowym, jak i unijnym. Można zaryzykować twierdzenie, że cyberbezpieczeństwo stało się niezwykle istotnym punktem zainteresowania władz, biznesu oraz społeczeństwa. Wynika to z kilku powodów, ale ich szczegółowa analiza wykracza poza ramy niniejszego tekstu. Autorzy ograniczają się bowiem wyłącznie do stwierdzenia, że bardzo istotnym powodem wzrostu zainteresowania cyberbezpieczeństwem była pandemia koronawirusa i wynikająca z tego faktu migracja setek tysięcy procesów do przestrzeni cyfrowej. Ograniczenia w przemieszczaniu się oraz tradycyjnej formie kontaktów zmusiły wiele organizacji do zmiany paradygmatów świadczenia usług oraz zmian w organizacji wewnętrznej. Niezbędne było również praktycznie natychmiastowe przeniesienie procesów wewnętrznych realizowanych w poszczególnych organizacjach, w tym organizacjach szeroko pojętego rynku finansowego, do przestrzeni cyfrowej.

Zasadniczym celem niniejszego artykułu jest analiza uwarunkowań prawnych kształtujących system cyberbezpieczeństwa rynku finansowego w Polsce. W tym celu przeprowadzono dogmatyczno-prawną analizę przepisów prawa krajowego oraz – częściowo – unijnego. Organem właściwym do spraw cyberbezpieczeństwa

dla sektora bankowego i infrastruktury rynków finansowych jest Komisja Nadzoru Finansowego, więc przede wszystkim temu podmiotowi poświęcone jest niniejsze opracowanie. Pełna analiza kompetencji, zadań i roli innych podmiotów tworzących krajowy system cyberbezpieczeństwa wykracza poza założenia badawcze określone przez autorów.

Hipoteza badawcza przyjęta na potrzeby prowadzonych rozważań jest następująca: przepisy prawa krajowego i unijnego kształtującego system cyberbezpieczeństwa rynku finansowego w Polsce będą podlegać ciągłej ewolucji, ponieważ uwarunkowania cyberbezpieczeństwa rynku finansowego, a tym samym wyzwania z nim związane, ulegają dynamicznym zmianom W tym kontekście szczególnego znaczenia nabiorą akty prawa miękkiego określanego mianem *soft law*, a więc rekomendacje, wytyczne i tzw. listy pasterskie kierowane do podmiotów rynku finansowego. Ich niewątpliwą zaletą – przy zasadniczej wadzie związanej z brakiem mocy wiążącej – jest stosunkowo krótki czas ich przygotowywania i wdrażania. Hipotezą pomocniczą jest twierdzenie, że ukształtowany w ostatnich miesiącach instytucjonalny system cyberbezpieczeństwa będzie względnie stały, a zmiany będą miały charakter dostosowujący i doskonalący. Działania doskonalące skupiać się będą na zagadnieniach związanych z edukacją społeczeństwa, dzięki czemu wzrośnie poziom cyfrowej odporności operacyjnej państwa i jego instytucji, a także podmiotów prowadzących działalność gospodarczą oraz obywateli.

Przyjęte hipotezy będą weryfikowane w procesie badawczym z wykorzystaniem odpowiedzi na następujące pytania: czym jest cyberbezpieczeństwo? Czy termin ten ma legalną definicję w polskim porządku prawnym? Jakie akty prawne regulują kwestie cyberbezpieczeństwa w Polsce? Jak kształtują one instytucjonalny wymiar cyberbezpieczeństwa? Jaką funkcję pełni w systemie cyberbezpieczeństwa Komisja Nadzoru Finansowego? Jakie są kluczowe wyzwania związane z cyberbezpieczeństwem rynku finansowego w Polsce? Jaki wpływ na poziom cyberbezpieczeństwa rynku finansowego mają czynniki geopolityczne, m.in. wojna w Ukrainie? W jaki sposób można zwiększać cyfrową odporność operacyjną rynku finansowego?

1. Cyberbezpieczeństwo – definicja legalna

Mając na uwadze zasadnicze cele badawcze niniejszego artykułu, pominięty zostanie szczegółowy proces konceptualizacji terminu „cyberbezpieczeństwo". Proces ten był przedmiotem analizy doktryny. Na potrzeby prowadzonych rozważań zostaną przywołane jedynie definicje legalne tego terminu. Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: u.k.s.c.) cyberbezpieczeństwo to: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". W piśmiennictwie podkreśla się, że terminowi „cyberbezpieczeństwo" u.k.s.c. nadaje znaczenie zbliżone do zdefiniowanego w dyrektywie 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 (dalej: dyrektywa NIS) określenia „bezpieczeństwo sieci i systemów informacyjnych" (Szpor 2019, LEX). Zgodnie z brzmieniem art. 4 pkt 2 dyrektywy NIS 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 poprzez te sieci i systemy informatyczne. Pobieżna analiza przytoczonych definicji prowadzi do wniosku, że polski ustawodawca pominął występujący w dyrektywie zwrot „przy danym poziomie zaufania", nadający charakter względny „odporności", co – zdaniem Grażyny Szpor – może mieć znaczenie w stosowaniu prawa. Druga różnica dotyczy odniesienia samego terminu odporności. Polski ustawodawca odnosi ją do systemów informacyjnych, a ustawodawca unijny do takich systemów i sieci. W piśmiennictwie podkreśla się również, że sporne pozostają kwestie związane z wymienionymi w u.k.s.c. atrybutami bezpieczeństwa informacji, które powinny zostać uzupełnione o rozliczalność, niezawodność i niezaprzeczalność (Mroczka, Maderak, Zieliński 2021, s. 279). Zostały one wskazane w wydanej przez KNF w styczniu 2013 r. Rekomendacji D[1], Rekomendacji D-SKOK oraz wytycznych[2] dla sektora kapitałowego i ubezpieczeniowego. Stały się one powszechnie używanymi przez rynek finansowy w Polsce.

Analizując termin cyberbezpieczeństwo, należy zwrócić uwagę na treść przepisów prawa unijnego. W myśl rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 cyberbezpieczeństwo 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" (Rozporządzenie Parlamentu Europejskiego i Rady 2019). W tym kontekście na potrzeby przywołanego rozporządzenia przyjęto, że cyberbezpieczeństwo oznacza „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami".

W doktrynie słusznie podkreśla się, że *ratio legis* regulacji unijnych, jak i tych z u.k.s.c. jest: „ochrona użytkowników usług kluczowych oraz usług cyfrowych przed negatywną ekspozycją tych użytkowników na ryzyka specyficzne związane

[1] *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach* przyjęta przez KNF w styczniu 2013 r. (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).

[2] Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego odpowiednio dla towarzystw funduszy inwestycyjnych, firm inwestycyjnych, podmiotów infrastruktury runku kapitałowego, zakładów ubezpieczeń i zakładów reasekuracji oraz powszechnych towarzystw emerytalnych.

z brakiem odpowiedniego poziomu cyberbezpieczeństwa". Jak stwierdza Paweł Wajda: „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" (Wajda 2020, s. 12).

Bez wątpienia cyberbezpieczeństwo ma – zwłaszcza w kontekście sytuacji geopolitycznej na świecie – kluczowe znaczenie dla funkcjonowania państwa, jego instytucji, a także rynku finansowego i jego interesariuszy.

2. Ramy prawne krajowego systemu cyberbezpieczeństwa

Termin „krajowy system cyberbezpieczeństwa" (dalej: k.s.c.) został wprowadzony do polskiego porządku prawnego na podstawie przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[3] (dalej: u.k.s.c.). Regulacja ta wdraża do krajowego porządku prawnego dyrektywę 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 (dyrektywa NIS)[4]. W rządowym uzasadnieniu do projektu u.k.s.c. złożonym w Sejmie w kwietniu 2018 r.[5] podkreślono, że: „podjęcie prac związanych z kompleksowym uregulowaniem krajowego systemu cyberbezpieczeństwa wynika z jednej strony z potrzeby zapewnienia systemowego podejścia do krajowego systemu cyberbezpieczeństwa w obliczu stale rosnących i dynamicznie zmieniających się zagrożeń cyberbezpieczeństwa dla funkcjonowania państwa, gospodarki i społeczeństwa, a z drugiej strony konieczności wdrożenia do polskiego porządku prawnego dyrektywy 2016/1148"[6].

Zakres podmiotowy ustawy zdefiniowano w art. 1 u.k.s.c. Zgodnie z wolą ustawodawcy regulacja ta określa: 1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu; 2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy; 3) zakres Strategii Cyberbezpieczeństwa RP. Przepisy powołanej ustawy nie mają zastosowania do: przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[7], w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów; dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług

[3] T.j. Dz.U. z 2020 r. poz. 1369 z późn. zm.
[4] Dz. Urz. UE L 194 z 19.07.2016.
[5] Sejm VIII Kadencji, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, Druk nr 2505.
[6] *Ibidem*.
[7] T.j. Dz.U. z 2021 r. poz. 576 z późn. zm.

zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[8] oraz podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

Wyłączenie z zakresu ustawy przedsiębiorców telekomunikacyjnych może budzić pewne obawy co do kompletności systemu cyberbezpieczeństwa. Nie ulega bowiem wątpliwości, że przedsiębiorcy telekomunikacyjni i ich działalność mają istotny wpływ na stan bezpieczeństwa w cyberprzestrzeni (Piątek 2020, s. 28–29). Podmiotom tym poświęcono jednak odrębną regulację, która definiuje obowiązki i zadania w zakresie cyberbezpieczeństwa. Należy bowiem pamiętać, że odrębność prawnych rozwiązań dotyczących cyberbezpieczeństwa tego sektora ma dłuższą historię w systemie prawa unijnego (Rojszczak 2018, LEX). Analiza tego wątku wykracza jednak poza przyjęte założenia badawcze.

W art. 2 u.k.s.c. zdefiniowano najważniejsze – zdaniem ustawodawcy – terminy związane z krajowym systemem cyberbezpieczeństwa. Przepis ten ma charakter słownika ustawowego.

Drugi z istotnych – obok cyberbezpieczeństwa – terminów definiowanych w ustawie to „incydent". Jest to w świetle u.k.s.c. zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Ustawa wprowadza kilka kategorii incydentów, co jest logiczną konsekwencją wdrażania mechanizmów odpowiedniego reagowania.

Po pierwsze w u.k.s.c. jest mowa o incydencie krytycznym, który skutkuje: „znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi". Incydent tego typu jest klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV. Drugi typ incydentu to tzw. incydent poważny, który w myśl u.k.s.c.: „powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej". Ostatni typ incydentu to incydent istotny, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ[9].

Przywołany art. 4 rozporządzenia wykonawczego określa, że dany incydent uznaje się za mający istotny wpływ, jeżeli zaistniała co najmniej jedna z następujących sytuacji: 1) usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin, przy czym pojęcie „użytkownikogodziny"

[8] Dz. Urz. UE L 257 z 28.08.2014.
[9] Dz. Urz. UE L 26 z 31.01.2018.

odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut; 2) incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych, bądź przetwarzanych danych lub powiązanych usług, oferowanych, bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w Unii; 3) incydent spowodował ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych; lub 4) incydent wyrządził co najmniej jednemu użytkownikowi w Unii stratę materialną, której wysokość przekracza 1 000 000 EUR.

Krajowy ustawodawca w u.k.s.c. wprowadził również do porządku prawnego pojęcie incydentu w podmiocie publicznym. Jest to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Podmioty, których dotyczy ten obowiązek, to m.in. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (u.f.p.)[10], instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, a także spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej[11].

Zdaniem Grażyny Szpor definicje dotyczące incydentów przyjęte w art. 2 pkt 6–9 u.k.s.c. obarczone są błędem formalnym (*idem per idem*), polegającym na powtórzeniu słowa definiowanego w jego objaśnieniu (*definiens* i *definiendum* zawierają to samo słowo odpowiednio: poważny/e, istotny, podmiot publiczny) (Szpor 2019).

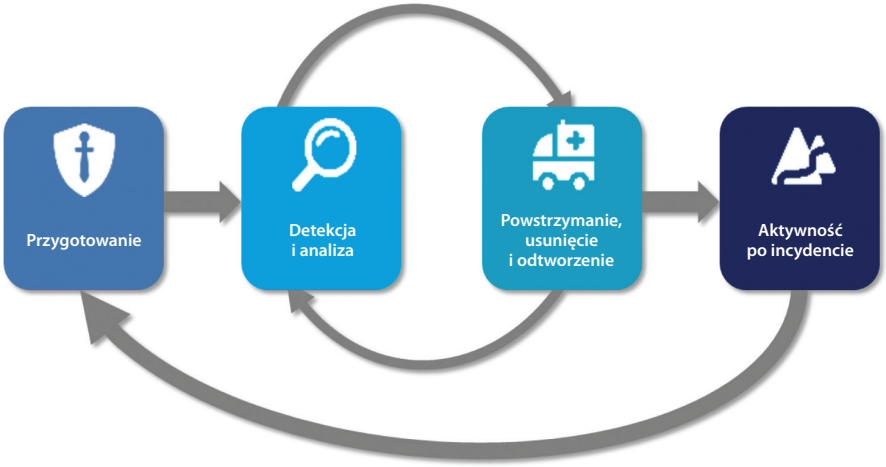
W celu zapewnienia przejrzystości i spójności działania u.k.s.c. objaśnia również pojęcie obsługi incydentu. Są to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu. W *Podręczniku postępowania z incydentami naruszenia bezpieczeństwa komputerowego*, wydanym w 2021 r. przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa, podkreślono, że obsługa incydentu stanowi proces reakcji na incydent składający się z kilku faz. Fazy te przedstawia rysunek 1.

Ustawodawca definiuje również w u.k.s.c. termin „podatność". Jest to właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa. W doktrynie słusznie podkreśla się, że podatność oznacza *de facto* jego słabość, tj. brak odporności na incydent (Radoniewicz 2019). Krzysztof Liderman twierdzi natomiast, że podatność to: „luka lub wada, która może być wykorzystana przez zagrożenia do spowodowania szkód w systemie informacyjnym organizacji lub w jej działalności" (Liderman 2018, s. 67–82). Warto przypomnieć, że podatności: „w wielu przypadkach wynikają z braku odpowiedniej higieny bezpieczeństwa

[10] Dz.U. z 2019 r. poz. 869, z późn. zm.
[11] Dz.U. z 2019 r. poz. 712 i 2020.

infrastruktury sieciowej, ale nie tylko. Mogą być również wynikiem niedostatecznej znajomości obsługi danego rozwiązania lub powstać w trakcie jego eksploatacji, np. w wyniku odejścia z pracy jedynego pracownika przeszkolonego w obsłudze danego rozwiązania" (Banasiński i in. 2020).

Rysunek 1. Cykl życia reakcji na incydent



Źródło: *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego*, wer. 1.0, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Warszawa 2021, s. 39.

W kontekście incydentów niezbędne jest również zwrócenie uwagi na pojęcie „zarządzanie incydentem". Wedle przepisów u.k.s.c. jest to obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków płynących z obsługi incydentu.

Pod pojęciem „system informacyjny" przepisy u.k.s.c. definiują w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej[12]. Ustawa niniejsza definiuje system teleinformatyczny jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[13].

Analizowana regulacja definiuje również kwestie związane z procesem zarządzania ryzykiem. Mianem ryzyka zgodnie z regulacjami u.k.s.c. definiuje się kombinację

[12] Dz.U. z 2020 r. poz. 346, 568 i 695.
[13] Dz.U. z 2021 r. poz. 576.

prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji. Z kolei szacowanie ryzyka to – zgodnie z intencją ustawodawcy – całościowy proces identyfikacji, analizy i oceny ryzyka. Należy również podkreślić, że ustawa objaśnia pojęcie zarządzania ryzykiem, przez które rozumie skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Niezbędne jest również podkreślenie, że analizowana regulacja definiuje usługę cyfrową. W myśl u.k.s.c. jest to usługa świadczona drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[14]. W załączniku nr 2 do u.k.sc. zdefiniowano trzy usługi. Są to: internetowa platforma handlowa[15], usługa przetwarzania w chmurze[16] oraz wyszukiwarka internetowa[17]. Ustawodawca wyszczególnił również pojęcie usługi kluczowej. Jest to usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych.

Ustawa definiuje również trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). Są to: 1) CSIRT GOV działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego; 2) CSIRT MON działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej; 3) CSIRT NASK działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. W piśmiennictwie podkreśla się, że w art. 9 dyrektywy NIS mowa jest o „Computer security incident response teams" (CSIRTs), ale w polskiej wersji językowej zastosowano liczbę pojedynczą, co: „skutkuje błędami gramatycznymi (składni) w całym tekście polskiej wersji tego przepisu" (Szpor 2019).

Ustawodawca zdecydował się również na sformułowanie w formie przepisu prawnego celu funkcjonowania krajowego systemu cyberbezpieczeństwa. Zgodnie z brzmieniem art. 3 u.k.s.c. system ma zapewnić cyberbezpieczeństwo na poziomie krajowym, w tym niezakłócone świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług, oraz zapewnić obsługę incydentów. Nie ulega wątpliwości, że przywołane powyżej cele szczegółowe nie wyczerpują wszystkich funkcji przypisanych systemowi cyberbezpieczeństwa RP. Świadczy o tym użyte przez ustawodawcę wyrażenie „w szczególności". Można zatem przyjąć, że spośród wielu, dwa cele szczegółowe były kluczowe dla ustawodawcy.

[14] Dz.U. z 2020 r. poz. 344.

[15] Jest to usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami za pośrednictwem strony internetowej platformy handlowej albo strony internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową.

[16] Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników.

[17] Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą pytania poprzez wpisanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku przedmiotowego wyszukiwania odnośniki, związane z tematem pytania lub wpisanego hasła.

Krajowy system cyberbezpieczeństwa w ujęciu podmiotowym obejmuje bardzo dużą liczbę podmiotów. W u.k.s.c. wymieniono z nazwy wyłącznie wybrane podmioty, m.in. Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej oraz Polskie Centrum Akredytacji. W pozostałym zakresie ustawa tworzy nowe kategorie – np. operatorów i dostawców usług kluczowych, organy właściwe do spraw cyberbezpieczeństwa oraz odsyła do innych aktów prawnych, m.in. u.f.p. W kontekście u.f.p. ustawodawca objął systemem jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 tej ustawy.

3. Pozycja, rola i zadania Komisji Nadzoru Finansowego w systemie cyberbezpieczeństwa rynku finansowego

Jak stwierdzono powyżej, KNF jest organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych. Wynika to z brzmienia art. 41 pkt 4 u.k.s.c.

Zadania organów właściwych do spraw cyberbezpieczeństwa zdefiniowano w art. 42 u.k.s.c. Przepis ten definiuje jedenaście zadań, które realizuje każdy z organów, niezależnie od innych uregulowań zawartych w przepisach szczególnych. Organy właściwe odpowiadają 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 o uznaniu podmiotu za operatora usługi kluczowej albo decyzji stwierdzających wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej; 3) niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazanie do ministra właściwego do spraw informatyzacji wniosku o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu; 4) składanie wniosków o zmianę danych w wykazie operatorów usług kluczowych; 5) przygotowywanie we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych dotyczących zgłaszania incydentów; 6) monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych; 7) wzywanie na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego; 8) prowadzenie kontroli operatorów usług kluczowych i dostawców usług cyfrowych; 9) prowadzenie współpracy z właściwymi organami państw członkowskich Unii Europejskiej; 10) przetwarzanie informacji dotyczących świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;

11) uczestniczenie w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej.

Przywołany przepis ma charakter normy ustrojowej w zakresie krajowego systemu cyberbezpieczeństwa. Celem ustawodawcy było zdefiniowanie katalogu zadań i obowiązków, które muszą realizować podmioty systemu cyberbezpieczeństwa, określane jako organy właściwe do spraw cyberbezpieczeństwa. Co istotne, katalog ten obejmuje nie tylko obowiązki, ale również uprawnienia tych organów.

W ust. 3 art. 42 ustawodawca w u.k.s.c. ustanowił mechanizm delegowania realizacji zadań. Przepis ten przewiduje, że organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację, w jego imieniu, niektórych zadań jednostkom podległym lub nadzorowanym przez ten organ. W regulacji tej dookreślona została również forma prawna owego powierzenia. Powierzenie następuje na podstawie porozumienia zawartego pomiędzy organem a podmiotem, któremu powierzono zadania. Obowiązkiem prawnym jest zawarcie w przedmiotowym porozumieniu zasad sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań. Warunek ten jest obligatoryjny, wobec czego nie może zostać pominięty. Brak mechanizmów kontroli sposobu wykonywania powierzonych zadań może być podstawą nieważności porozumienia oraz powodować odpowiedzialność po stronie organu właściwego do spraw cyberbezpieczeństwa. Można bowiem przyjąć, że celem przyjęcia tego przepisu była konieczność ustanowienia mechanizmów walidacji prawidłowości realizacji istotnych zadań państwa.

Ustawa przewiduje również obowiązki informacyjne związane z zawarciem porozumienia. Na organie właściwym ciąży obowiązek ogłoszenia komunikatu o zawarciu porozumienia w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. W komunikacie wskazuje się informacje o: 1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami; 2) terminie, od którego porozumienie będzie obowiązywało.

Po wejściu w życie w 2018 r. Ustawy o krajowym systemie cyberbezpieczeństwa Komisja Nadzoru Finansowego za operatorów usługi kluczowej (OUK) uznała 15 podmiotów z sektora bankowego i SKOK oraz 4 inne podmioty należące do infrastruktury rynku finansowego. Rok później – w 2019 roku – KNF przyznała status OUK dwóm innym podmiotom oraz zdecydowała o wygaśnięciu tej decyzji dla jednego podmiotu. Obecnie – w połowie 2022 roku – KNF za OUK uznaje 20 podmiotów.

KNF w swojej misji przygotowuje we współpracy z zespołami CSIRT poziomu krajowego, jak i z sektorowymi zespołami, rekomendacje działań mających na celu wzmocnienie cyberbezpieczeństwa, zwłaszcza w obszarze sektora finansowego. KNF monitoruje stosowanie u.k.s.c. przez OUK-i w swoim sektorze. Art. 42 ust. 1 pkt 7 u.k.s.c. mówi, że na wniosek CSIRT-ów krajowych KNF może również wezwać OUK-i lub dostawców usług kluczowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego,

istotnego lub krytycznego. KNF ma również kompetencję do kontrolowania operatorów usług kluczowych i dostawców usług cyfrowych.

Weryfikacja spełnienia przez OUK wymagań ustawowych jest realizowana zarówno poprzez kontrole, jak i w formie działań analitycznych prowadzonych w osobnym (od strumienia nadzorczego) strumieniu wymiany informacji. Katalog obowiązków podmiotu kontrolowanego ustawodawca określił w art. od 56 do 59 u.k.s.c. ustawy, zawierając w nich również wiele praw przysługujących kontrolującym.

W kolejnych ustępach art. 42 u.k.s.c., została przewidziana możliwość powołania Pojedynczego Punktu Kontaktowego przy KNF do prowadzenia współpracy z właściwymi organami państw członkowskich Unii Europejskiej. KNF ma uprawnienia do przetwarzania informacji, w tym danych osobowych, dotyczących świadczonych usług kluczowych oraz OUK-ów w zakresie niezbędnym do realizacji zadań wynikających z ustawy. KNF na mocy ustawy uczestniczy również w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w RP lub UE. Jednym z przykładów tego rodzaju uprawnień może być udział KNF w ćwiczeniach KSC EXE 2020.

Rola KNF jako organu właściwego do spraw cyberbezpieczeństwa nie kończy się jedynie na wypełnianiu obowiązków ustawowych uregulowanych w 42 art. u.k.s.c., ale obejmuje również aktywny udział w kształtowaniu krajowego systemu cyberbezpieczeństwa poprzez bezpośrednią współpracę z uczestnikami tego systemu oraz organami europejskimi. Przykładem takich działań mogą być np. spotkania z przedstawicielami Komisji Europejskiej oceniającymi stan wdrożenia Dyrektywy NIS w prawodawstwie polskim, określenie zasad komunikacji pomiędzy UKNF a CSIRT NASK dotyczących współpracy w ramach ustawy o krajowym systemie cyberbezpieczeństwa, współpraca z NASK PIB w zakresie opracowania poradnika dla operatorów usług kluczowych oraz organów właściwych.

4. Sektorowy zespół cyberbezpieczeństwa rynku finansowego – CSIRT KNF

Ustawodawca krajowy, dążąc do zwiększenia skuteczności i efektywności systemu cyberbezpieczeństwa, wprowadził możliwość powoływania tzw. sektorowych zespołów do spraw cyberbezpieczeństwa. Możliwość taką daje art. 44 u.k.s.c., zgodnie z którym organ właściwy do spraw cyberbezpieczeństwa może ustanowić, na podstawie odrębnych przepisów, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku nr 1 do ustawy. Zespół taki odpowiada 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 u.k.s.c.[18]; 3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz

[18] Mowa tu o obowiązkach w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 u.k.s.c.

opracowywanie wniosków z obsługi incydentu; oraz 4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

Ustawa dopuszcza możliwość powołania zespołu cyberbezpieczeństwa dla sektora bankowość i infrastruktura rynków finansowych. Zgodnie z brzmieniem załącznika nr 1 do u.k.s.c. obejmuje on następujące podmioty: instytucje kredytowe[19], banki krajowe[20], oddziały banków zagranicznych[21], oddziały instytucji kredytowych[22], spółdzielcze kasy oszczędnościowo-kredytowe[23], podmiot prowadzący rynek regulowany[24] oraz podmioty, o których mowa w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[25].

Powstanie zespołu CSIRT dla sektora finansowego wynikło więc z ewolucji modelu nadzoru oraz analizy zagrożeń i wyzwań związanych z cyberbezpieczeństwem. Utworzenie CSIRT KNF było również odpowiedzią na postulaty podmiotów nadzorowanych, chcących wzmocnienia działań i polepszenia ich koordynacji w walce z cyberzagrożeniami. Analiza dotychczasowego modelu funkcjonowania wykazała, że poszczególne przedsięwzięcia pojedynczych podmiotów w walce z cyberzagrożeniami są nieefektywne i niemiarodajne. Konieczne było między innymi zapewnienie wymiany informacji pomiędzy podmiotami z różnych obszarów polskiego rynku finansowego. Obserwacja trendów cyberprzestępczości wykazała, że niezbędne jest powołanie zespołu mającego na celu całościowe podejście do walki z cyberzagrożeniami, działającego globalnie i reagującego jednocześnie w wielu obszarach.

Powołanie takiego zespołu wymagało zmiany postrzegania nadzoru przez podmioty rynku finansowego. Konieczne było wytworzenie relacji zaufania pomiędzy zespołem a podmiotami nadzorowanymi. Wyzwaniem było zarówno utworzenie zasad i procedur pozwalających podmiotom nadzorowanym na zgłaszanie incydentów bez np. ryzyka wykorzystania tej wiedzy w późniejszych czynnościach przez zespół (np. w inspekcjach), jak i nakłonienie ich do dzielenia się tą wiedzą. Co istotne, żadne informacje uzyskane w trakcie pracy operacyjnej CSIRT KNF nie są przekazywane do organu nadzoru, pozostając tylko i wyłącznie w relacji CSIRT KNF – podmiot zgłaszający incydent.

[19] Instytucje kredytowe, o których mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, Dz.U. z 2017 r. poz. 1876, z późn. zm.

[20] Banki krajowe, o których mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

[21] Oddziały banków zagranicznych, o których mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

[22] Oddziały instytucji kredytowych, o których mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

[23] Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, Dz.U. z 2017 r. poz. 2065, z późn. zm.

[24] Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, Dz.U. z 2017 r. poz. 1768, z późn. zm.

[25] Mowa tu o podmiotach, o których mowa w art. 3 pkt 49 oraz art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

Budowa zespołu CSIRT KNF przebiegała etapowo; najpierw skupiała się na realizacji zadań przewidzianych w art. 44 u.k.s.c. dotyczącym sektorowego zespołu cyberbezpieczeństwa, a następnie zostały dodane kolejne zadania mające na celu wzmocnienie podmiotów rynku finansowego w walce z cyberzagrożeniami.

Jednym z pierwszych, pozaustawowych działań zespołu jest wyszukiwanie i analiza fałszywych stron phishingowych. Powstawanie CSIRT KNF zbiegło się z wybuchem pandemii koronawirusa, na skutek czego większość działań konsumentów przeniosła się do internetu. W związku z tym wprost proporcjonalnie wzrosła liczba stron fałszywych, mających na celu oszukanie klientów i kradzież ich środków finansowych. Zespół na bieżąco wyszukuje pojedyncze złośliwe domeny, identyfikuje bieżące kampanie oszustów, i im przeciwdziała.

Kolejnym działaniem CSIRT KNF jest *Threat Intelligence* – gromadzenie i analizowanie informacji o aktualnych i potencjalnych atakach, zagrażających bezpieczeństwu podmiotów sektora finansowego i ich zasobom. Wyniki działań analitycznych przekazywane są nie tylko podmiotom z sektora, lecz również pozostałym zespołom CSIRT poziomu krajowego, a w niektórych przypadkach również innym zespołom cyberbezpieczeństwa.

CSIRT KNF w ramach swoich działań analizuje również pozyskane przez siebie próbki złośliwego oprogramowania. Analiza wsteczna pozwala zbadać charakterystykę oraz sposób działania oprogramowania. Raporty opisujące analizę udostępniane są podmiotom nadzorowanym, a następnie publikowane na stronie CSIRT KNF w formie artykułów.

Członkowie zespołu na bieżąco monitorują fora i czaty grup przestępczych, zarówno te umieszczone w zasobach Open Web, jak i Dark Netu. Celem tego działania jest jak najwcześniejsze wykrycie potencjalnych ataków oraz zdobycie wiedzy o formie działania przestępców. Pozyskane informacje są poddawane wnikliwej analizie, a następnie przekazywane podmiotom nadzorowanym.

CSIRT KNF opracowuje również rekomendacje w zakresie przeciwdziałania cyberzagrożeniom. W przypadku wykrycia nowego zagrożenia Zespół przygotowuje dokument mający na celu mitygacje skutków zagrożenia. Rekomendacja, w zależności od potrzeby, przekazywana jest szerszej lub węższej grupie odbiorców (podmiotów). Część z rekomendacji podawana jest do publicznej wiadomości (Dobre praktyki 2022).

Ostatnim, niezmiernie istotnym działaniem Zespołu jest misja edukacyjna. Członkowie CSIRT KNF prowadzą w zakresie obszaru cyberbezpieczeństwa szkolenia, wykłady, pogadanki z zainteresowanymi podmiotami, szkołami i uczelniami. Dodatkowo w mediach społecznościowych CSIRT KNF regularnie publikowane są ostrzeżenia o najświeższych kampaniach cyberoszustów. Artykuły ostrzegające przed bieżącymi zagrożeniami publikowane są zarówno na stronie Zespołu, jak i w tradycyjnej prasie. Dla ułatwienia działań zostało powołane Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego KNF, w ramach którego planowane jest rozszerzenie grupy docelowej i wzmocnienie filaru edukacji.

5. Rekomendacje i wytyczne KNF (*soft law*) jako narzędzie wzmacniające odporność cyfrową rynku finansowego

Nie ulega wątpliwości, że dynamiczne otoczenie społeczno-polityczne i gospodarcze wymusza na organach prawotwórczych pragmatyczne podejście do prawa. Ma ono wzmacniać działania związane z aktualnymi problemami i wyzwania w obszarze cyberbezpieczeństwa. Aleksandra Nadolska zauważa, że: „ostatni globalny kryzys finansowy zrewolucjonizował podejście do tworzenia, rozumienia i stosowania prawa rynku finansowego w UE i poszczególnych państwach członkowskich, skutkując przyjęciem nowego paradygmatu regulacyjnego opartego na wzajemnej zależności prawa 'twardego' i 'miękkiego'". Jej zdaniem: „*ius cogens, ius dispositovum* i *soft law* wzajemnie oplatają się, raz się krzyżując, a innym razem oddalając, współtworząc stałą tkankę prawa rynku finansowego, niezdolną już do podziałów i całkowitego rozróżnienia. W takim ujęciu *soft law* stanowi źródło tego prawa. Określa ono hierarchiczne relacje pomiędzy różnymi aktami prawnymi i zasady obowiązujące w przypadku rozbieżności w stosowaniu tych aktów" (Nadolska 2021, s. 9).

W doktrynie podkreśla się również, że *soft law* można postrzegać jako odpowiedź na problemy społeczne i ekonomiczne, których nie udaje się rozwiązać w sposób satysfakcjonujący na poziomie prawa unijnego i krajowego przy wykorzystaniu aktów prawnie wiążących (Dąbrowska 2005). Marcin Pietrzyk trafnie podkreśla, że *soft law* zapewnia elastyczność, podążając za wyzwaniami, którym sprostać musi system prawny. Dodaje również, że *soft law* może być stanowione i zmieniane bez zbędnej zwłoki i długotrwałych procedur legislacyjnych, co pozwala na ciągłe eksperymentowanie i dostosowywanie do zmieniających się potrzeb (Pietrzyk 2015).

Jak wspomniano powyżej, celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do niego, a także zapewnienie ochrony interesów wszystkich jego uczestników. W tym kontekście zadaniem KNF jest również ochrona prawna rynku finansowego. W nowszej doktrynie podkreśla się, że KNF pełni m.in.: „funkcję regulacyjną, dzięki której wydaje akty nadzorcze *sensu largo* obejmujące specyficzne (nienormatywne) dla rynku finansowego instrumenty prawne o charakterze miękkim – w szczególności rekomendacje, wytyczne i listę ostrzeżeń publicznych" (Nadolska 2021, s. 12).

Należy również zauważyć, że w ostatnich latach rysuje się tendencja odchodzenia od wiążących (twardych) norm prawa rynku finansowego w kierunku zasad i tzw. prawa miękkiego (*soft law*). Zdaniem cytowanej już Nadolskiej: „*soft law*, chociaż nie mają charakteru prawnie obowiązującego, często mogą torować drogę standardom prawnie wiążącym" (Nadolska 2021, s. 15). Zagadnienia związane z charakterem *soft law* budzą żywe zainteresowanie doktryny, jednak szczegółowa analiza tego zagadnienia wykracza poza ramy niniejszego artykułu. Warto jednak zaznaczyć, że zdaniem uznanego przedstawiciela doktryny i praktyki Aleksandra Chłopeckiego: „'miękkie prawo' stanowi element systemu prawnego zarówno w rozumieniu prawa europejskiego, jak i prawa polskiego. Ta konstatacja zdaje się umykać regulatorom i części środowiska

prawniczego" (Chłopecki 2013, s. 34). Rację ma również Paweł Wajda pisząc, że KNF w drodze rekomendacji dokonuje dookreślenia treści pojęć ustawowych, które często są nieostre. Jego zdaniem rekomendacje pozwalają nadzorowanym podmiotom uzyskać dostęp do wiedzy określającej lub będącej podstawą dla podejścia organu nadzoru w zakresie rozumienia pojęć niedookreślonych wykorzystywanych w treści przepisów prawa powszechnie obowiązującego, stanowiących podstawę prawną dla regulacji rynku finansowego (Wajda 2016, s. 125).

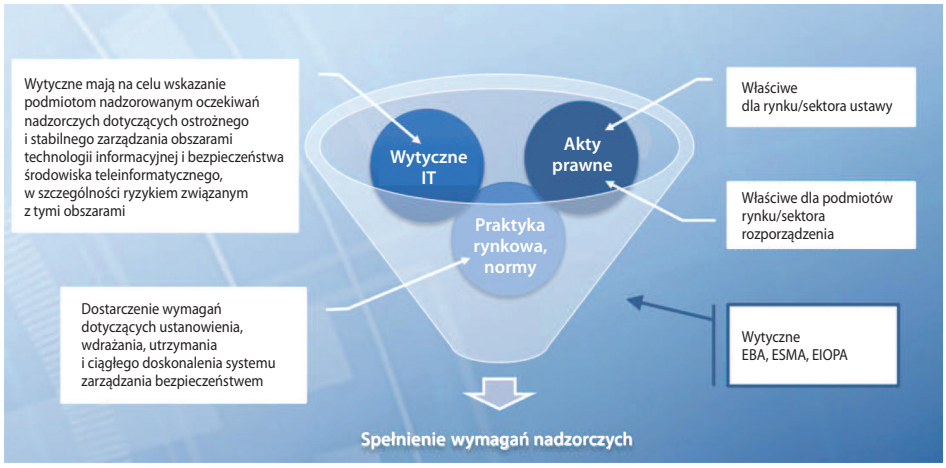
Rodzima nauka prawa uznaje KNF za organ regulacyjny (Hoff 2005, s. 37–54). Ma to istotne konsekwencje związane z kompetencjami prawotwórczymi tego organu. W doktrynie podkreśla się, że KNF realizując tę funkcję samodzielnie wprowadza akty, z których wynikają normy abstrakcyjno-generalne w stosunku do podmiotów nadzorowanych (Głuchowski 2010, s. 141 i nast.). Podstawy prawne do wydawania rekomendacji sformułowano w kilku aktach prawnych. Warto tu przywołać m.in. art. 137 ustawy Prawo bankowe (Ustawa *Prawo bankowe* 1997). Mówi on, że KNF może wydawać rekomendacje dotyczące dobrych praktyk ostrożnego i stabilnego zarządzania bankami. W ust. 2 tego przepisu ograniczono częściowo to prawo wskazując, że w przypadku gdy rekomendacje odnoszą się do spraw mogących dotyczyć nadzoru makroostrożnościowego, o którym mowa w ustawie o nadzorze makroostrożnościowym, KNF wydaje takie rekomendacje po zasięgnięciu opinii Komitetu Stabilności Finansowej (Ustawa *o nadzorze makroostrożnościowym* 2015). W nowszej doktrynie podkreśla się jednak, że rekomendacje nie mają charakteru wiążącego dla banków i stanowią jedynie „kodeksy" dobrych praktyk w zakresie funkcjonowania banków (Lewandowski 1997; Krzyżewski 2000; Czech 2009; Olszak 2010; Ochnio 2013; Ofiarski 2017). W podobnym tonie wypowiada się judykatura. W wyroku Sądu Okręgowego w Łodzi (Wyrok Sądu Okręgowego w Łodzi 2019) stwierdzono, że: „rekomendacje Komisji Nadzoru Finansowego nie mają w polskim systemie prawnym charakteru źródeł prawa, jednakże są wyznacznikiem dobrych obyczajów w relacjach banku z konsumentem"(Wyrok Sądu Okręgowego w Łodzi 2019).

Zbliżoną kompetencję KNF zdefiniowano w art. 62 ust. 2 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Ustawa *o spółdzielczych kasach oszczędnościowo-kredytowych* 2009). Przepis ten stanowi, że KNF może wydawać, po zasięgnięciu opinii Kasy Krajowej, rekomendacje dotyczące dobrych praktyk ostrożnego i stabilnego zarządzania kasami. Nie jest jasne, czy opinia Kasy Krajowej SKOK ma charakter wiążący, jednak należy podkreślić, że ograniczanie kompetencji organu nadzoru i regulatora jest niewłaściwe, i powinno zostać wyeliminowane. Interesy organu nadzoru i podmiotów nadzorowanych mogą być częściowo rozbieżne.

Podstawy prawne do wydawania rekomendacji zawiera również ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Ustawa *o usługach płatniczych* 2011). W art. 102 ust. 2 precyzuje, że KNF może wydawać rekomendacje dotyczące dobrych praktyk ostrożnego i stabilnego zarządzania krajowymi instytucjami płatniczymi, mając na uwadze ochronę interesów użytkowników lub posiadaczy pieniądza elektronicznego.

Obok rekomendacji KNF należy również wyszczególnić wytyczne, które mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami. Należy również zwrócić uwagę na praktykę rynkową oraz normy i standardy, które są istotne dla zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Kompleksowe podejście do wymagań nadzorczych obejmuje wobec tego zarówno „twarde prawo", jak i *soft law* (krajowe i unijne). Szczegóły prezentuje rysunek 2.

Rysunek 2. Kompleksowe podejście do wymagań nadzorczych w zakresie cyberbezpieczeństwa



Źródło: opracowanie własne.

Mając na uwadze tematykę artykułu, poniżej scharakteryzowane zostaną rekomendacje i wytyczne, które zostały sformułowane przez KNF. Poza głównym nurtem rozważań pozostaną wytyczne europejskich organów nadzoru.

Kluczową z perspektywy omawianych tu zagadnień jest *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa* środowiska *teleinformatycznego w bankach* przyjęta przez KNF w styczniu 2013 r. Ma ona na celu wskazanie bankom oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami. Jak podkreślono w treści tego dokumentu, rekomendacja D powinna być traktowana jako dopełnienie *Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach* w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego), ale również m.in. z ryzykiem utraty reputacji i ryzykiem strategicznym.

W rekomendacji D sformułowano 22 rekomendacje. Zostały one uporządkowane w ramach czterech obszarów: 1. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego; 2. Rozwój środowiska teleinformatycznego; 3. Utrzymanie i eksploatacja środowiska teleinformatycznego; oraz 4. Zarządzanie bezpieczeństwem środowiska teleinformatycznego.

W obszarze „Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego" sformułowano 5 rekomendacji. Pierwsza mówi, że rada nadzorcza banku powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd banku powinien sprawić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny. W rekomendacji drugiej podkreślono, że w banku powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach. Kolejna trzecia rekomendacja stanowi, że bank powinien opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania banku. W czwartej rekomendacji przyjęto, że bank powinien określić zasady współpracy oraz zakresy odpowiedzialności obszaru biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności banku. Ostatnia, piąta rekomendacja precyzuje, że rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach.

Drugi obszar „Rozwój środowiska teleinformatycznego" zawiera dwie rekomendacje. Pierwsza z nich wskazuje, że bank powinien mieć sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów. Druga zakłada, że systemy informatyczne banku powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego.

Najbardziej rozbudowana sekcja „Utrzymanie i eksploatacja środowiska teleinformatycznego" definiuje 10 rekomendacji[26]. Zawierają one wiele oczekiwań związa-

[26] (1) Bank powinien mieć sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności banku. (2) Bank powinien mieć sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych. (3) Bank powinien mieć sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej banku. (4) Bank powinien mieć sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infra-

nych m.in. z zasadami zarządzania danymi, zasadami zarządzania infrastrukturą teleinformatyczną, zasadami współpracy z zewnętrznymi podmiotami, będącymi jednocześnie dostawcami usług informatycznych oraz mechanizmami ochrony środowiska teleinformatycznego.

Ostatni obszar zawarty w rekomendacji D – „Zarządzanie bezpieczeństwem środowiska teleinformatycznego" sformułował pięć oczekiwań wobec podmiotów nadzorowanych. Rekomendacje w tym obszarze są następujące:

- W banku powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w banku;
- Bank powinien klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa;
- Bank powinien mieć sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn;
- Bank powinien zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami;
- Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być przedmiotem systematycznych, niezależnych audytów.

Nie ulega wątpliwości, że rekomendacja D miała na celu zwiększenie odporności cyfrowej podmiotów nadzorowanych oraz zwrócenie uwagi na aspekty związane z zarządzaniem ryzykiem IT. Stanowi ona pewnego rodzaju drogowskaz dla podmiotów nadzorowanych w zakresie bezpieczeństwa środowiska teleinformatycznego.

struktury teleinformatycznej. (5) Bank powinien zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem. (6) Bank powinien zapewniać wewnętrznym użytkownikom systemów informatycznych wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie. (7) Bank powinien podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku. (8) System zarządzania ciągłością działania banku powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi. (9) Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien mieć skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów. (10) Bank powinien mieć sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego, skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.

Podsumowując tę część, należy zgodzić się z poglądem Zbigniewa Ofiarskiego, który trafnie podkreśla, że: „rekomendacje są wydawane z reguły po zaobserwowaniu przez KNF określonych zjawisk, zdarzeń lub zachowań w danym sektorze rynku finansowego. Wydanie rekomendacji jest szczególnego rodzaju sygnałem (zwróceniem uwagi) dla podmiotów instytucjonalnych, że takie zdarzenia mogą wywierać istotny wpływ na ich działalność" (Ofiarski 2017, s. 5). W podobnym tonie wypowiada się Anna Zalcewicz, która uważa, że zalecenia są: „wytycznymi, dyrektywami, których przestrzeganie nie może zostać nakazane, a jest jedynie doradzane" (Zalcewicz 2021).

Niezależnie od powyższych wątpliwości co do charakteru prawnego *soft law*, należy podkreślić, że praktyka nadzorcza i doświadczenia autorów wynikające z faktu zatrudnienia w UKNF pozwalają na sformułowanie wniosku, że podmioty nadzorowane – co do zasady – stosują się do rekomendacji i wytycznych, w szczególności w zakresie cyberbezpieczeństwa. Z perspektywy osób zarządzających podmiotami nadzorowanymi ryzykowne byłoby lekceważenie rekomendacji i wytycznych, których celem jest zwiększenie bezpieczeństwa klientów tych podmiotów oraz systemu finansowego w ujęciu instytucjonalnym. Niepodjęcie odpowiednich działań, co mogłoby spowodować powstanie istotnych problemów, byłoby niewątpliwie podstawą do wszczęcia innych procedur nadzorczych związanych m.in. z badaniem rękojmi członków organów podmiotów nadzorowanych w związku z prowadzeniem działalności banku z naruszeniem przepisów prawa, w sposób niegwarantujący stabilnego, ostrożnego i bezpiecznego zarządzania bankiem, w tym poprzez np. niestosowanie rekomendacji KNF i stwarzanie zagrożenia dla klientów banków.

Podsumowanie

Syntetyzując rozważania zawarte w niniejszym artykule, należy podkreślić, że pozycja i rola KNF w systemie cyberbezpieczeństwa Rzeczypospolitej Polskiej, w szczególności w zakresie funkcjonowania rynku finansowego, jest istotna. Wynika to z jednej strony z przyjętych rozwiązań prawnych kształtujących krajowy system cyberbezpieczeństwa, a z drugiej – z trendów obecnych w legislacji na poziomie unijnym oraz aktywności UKNF w tym zakresie. Bez wątpienia dobrowolne powołanie CSIRT KNF w lipcu 2021 r. zasygnalizowało, że tematyka ta pozostaje w ścisłym polu zainteresowania organu nadzoru i Urzędu Komisji, który na bieżąco wspiera KNF w realizacji ustawowych obowiązków. Sytuacja geopolityczna, a wcześniej pandemiczna, przyczyniły się do zwiększenia zainteresowania kwestiami cyberbezpieczeństwa. Wynika to z jednej strony z nieuchronnych procesów informatyzacji kolejnych obszarów funkcjonowania państwa oraz podmiotów gospodarczych, a z drugiej strony wiąże się ze wzrostem aktywności przestępczości w cyberprzestrzeni.

Sformułowana we wstępie hipoteza badawcza została częściowo potwierdzona. Ostatnie kilkanaście miesięcy obfitowało w kolejne zmiany prawne związane z sys-

temem cyberbezpieczeństwa. W grudniu 2021 r. uchwalono ustawę regulującą kwestie wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Ustawa *o szczególnych zasadach wynagradzania* 2021). Ustawa ta powołała do życia Fundusz Cyberbezpieczeństwa. Jego celem jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych i ochrony ich przed cyberzagrożeniami.

Omawiając ewolucję krajowego systemu cyberbezpieczeństwa, nie sposób również pominąć ustawy, która dała podstawę do powołania w strukturach Policji Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) (Ustawa *o zmianie niektórych ustaw w związku z powołaniem* 2021). CBZC jest jednostką organizacyjną Policji służącą zwalczaniu cyberprzestępczości, odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie: (1) rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw; (2) wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw, o których mowa w pkt 1, a także wykrywaniu i ściganiu sprawców tych przestępstw.

Również w zakresie cyberbezpieczeństwa rynku finansowego sformułowano kilka propozycji, które – zdaniem autorów – są niezbędne do wdrożenia. W naszej ocenie należałoby przyznać KNF kompetencje do podejmowania działań mających na celu przeciwdziałanie zagrożeniom w zakresie bezpieczeństwa systemów teleinformatycznych, które są wykorzystywane przez podmioty podlegające nadzorowi, w szczególności chodzi o uprawnienie do przekazywania tym podmiotom informacji niezbędnych do identyfikacji zagrożeń dla ich systemów teleinformatycznych oraz ochrony interesów ich klientów. Propozycja ta nabiera szczególnego znaczenia dla bezpieczeństwa rynku finansowego z punktu widzenia cyberbezpieczeństwa, szczególnie w okresie wojny w Ukrainie i agresywnych działań ze strony Rosji. Aby zwiększyć skuteczność i efektywność działań w cyberprzestrzeni niezbędne jest wdrożenie podstaw prawnych dających możliwość wymiany informacji służących przeciwdziałaniu zagrożeniom w zakresie bezpieczeństwa systemów teleinformatycznych. Mechanizm ten powinien obejmować również wymianę informacji między KNF a podmiotami przez nią nadzorowanymi. Obecne rozwiązania u.k.s.c. dają nieskrępowaną możliwość wymiany informacji z operatorami usług kluczowych, a takiej podstawy prawnej i formalnej nie mają wszystkie podmioty nadzorowane. W tym kontekście postulowane są zatem zmiany regulacyjne w u.n.r.f., w u.k.s.c. oraz prawie bankowym. Trzeba podkreślić, że powyższe propozycje zmian zostały przez Przewodniczącego KNF sformułowane i przekazane do odpowiednich instytucji, posiadających inicjatywę legislacyjną.

O tym, jak ważna jest sprawna i efektywna wymiana informacji, świadczą doświadczenia płynące z funkcjonowania zespołu CSIRT KNF od 2020 r. Dzięki szybkiej wymianie informacji między KNF a podmiotami nadzorowanymi udało się zminimalizować ryzyka operacyjne i systemowe związane z bezpieczeństwem systemów

informatycznych. W konsekwencji – zdaniem autorów – pozwoliło to na utrzymanie ciągłości działania państwa i jego instytucji, w tym podmiotów rynku finansowego.

Rosnący zakres zadań związanych z cyberbezpieczeństwem rynku finansowego powoduje istotny wzrost obciążenia po stronie UKNF. W efekcie w ostatnich kilkunastu miesiącach znacząco zwiększono poziom zatrudnienia w obszarze cyberbezpieczeństwa. Trend ten będzie aktualny również w kolejnych latach. Można wręcz zaryzykować twierdzenie, że nadzór nad cyberbezpieczeństwem rynku finansowego staje się „niezwykle istotnym – obok nadzoru bankowego, ubezpieczeniowego i nadzoru nad rynkiem kapitałowym – filarem aktywności KNF. Można również założyć, że wzrost znaczenia tego obszaru doprowadzi do poszerzenia składu zawodowej części Komisji o nadzorcę do spraw cyberbezpieczeństwa. Być może ustawodawca krajowy zdecyduje się również na poszerzenie składu niezawodowej części KNF o przedstawiciela ministra do spraw informatyzacji. Działanie to może w konsekwencji zwiększyć odporność państwa na zagrożenia płynące z cyberprzestrzeni.

Bibliografia

Banasiński C., Rojszczak M., Chmielewski J.M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., *Zarządzanie podatnościami oprogramowania i systemów IT*, [w:] C. Banasiński, M. Rojszczak, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski, *Cyberbezpieczeństwo*, LEX, Warszawa 2020.

Chłopecki A., *Zakres, sposób i skutki stosowania „miękkiego prawa" jako alternatywy dla regulacji ustawowych – na przykładzie rynku finansowego,* „Wiadomości Ubezpieczeniowe" 2013, nr 3 (wydanie specjalne).

Czech T., *Charakter prawny rekomendacji Komisji Nadzoru Finansowego*, „Przegląd Prawa Publicznego" 2009, nr 11.

Dąbrowska P., *Koncepcja „nowego rządzenia" w prawie Unii Europejskiej a Konstytucja dla Europy*, [w:] *Konstytucja dla Europy. Przyszły fundament Unii Europejskiej*, red. S. Dudzik, Kraków 2005.

Dobre praktyki w zakresie przeciwdziałania atakom DDoS, Rekomendacja CSIRT KNF, luty 2022; https://www.knf.gov.pl/knf/pl/komponenty/img/Dobre%20praktyki%20w%20zakresie%20przeciwdzia%C5%82ania%20atakom%20DDoS_77247.pdf (dostęp: 08.05.2022).

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.

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 19.07.2016.

Głuchowski J. [w:] J. Głuchowski (red.), *System prawa finansowego*, t. IV, Warszawa 2010.

Hoff W., *Recepcja pojęcia regulacji i organu regulacyjnego na przykładzie polskiego prawa,* „Państwo i Prawo" 2005, nr 8.

Krzyżewski J.A., *Rekomendacje nadzorcze – charakter prawny i zakres mocy obowiązującej*, „Prawo Bankowe" 2000, nr 7–8.

Lewandowski D., *Regulacyjna funkcja nadzoru bankowego. Nadzorcze rekomendacje ostrożnościowe A, B, C z dnia 3 marca 1997 r.*, „Prawo Bankowe" 1997, nr 3.

Liderman K., *Dziesięć definicji*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2017*, Szczytno 2018.

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.

Nadolska A., *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

Nieborak T., *Uwagi do rozdziału 1. Przepisy ogólne*, [w:] T. Nieborak, T. Sójka (red.), *Ustawa o nadzorze nad rynkiem kapitałowym. Komentarz*, Warszawa 2011.

Ochnio M., *Rekomendacje organu nadzoru bankowego w świetle polskiego systemu źródeł prawa,* [w:] M. Zubik, R. Puchta (red.), *Źródła prawa z perspektywy piętnastu lat obowiązywania Konstytucji*, Warszawa 2013.

Ofiarski Z., *Status prawny i funkcje rekomendacji wydawanych przez Komisję Nadzoru Finansowego oraz Komitet Stabilności Finansowej*, „Przegląd Ustawodawstwa Gospodarczego" 2017, nr 9.

Olszak M., *Rekomendacje organu nadzoru bankowego – geneza, przedmiot regulacji, charakter prawny*, „Przegląd Ustawodawstwa Gospodarczego" 2010, z. 11.

Piątek S., *Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, nr 2(9).

Pietrzyk M., *Soft law i hard law w europejskim prawie administracyjnym: relacja alternatywy, uzupełnienia, wykluczenia oraz przejścia*, [w:] M. Giełda, R. Raszewska-Sałecka (red.), *Administracja publiczna wobec wyzwań i oczekiwań społecznych*, Wrocław 2015.

Prawo spółdzielcze. System Prawa Prywatnego, tom 21, K. Pietrzykowski (red.), Warszawa 2020.

Radoniewicz F. [w:] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach przyjęta przez KNF w styczniu 2013 r. (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).

Rojszczak M., *Cyberbezpieczeństwo w łączności elektronicznej*, [w:] C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, Dz.U. UE. L. z 2019 r. Nr 151.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WEDz., Urz. UE L 257 z 28.08.2014.

Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ, Dz.U. UE. L. z 2018 r. Nr 26.

Sejm Rzeczypospolitej Polskiej, *Rządowy projekt ustawy o nadzorze nad rynkiem finansowym*, druk nr 654, http://orka.sejm.gov.pl/Druki5ka.nsf/wgdruku/654 (dostęp: 14.10.2020).

Sejm VIII Kadencji, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, Druk nr 2505.

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

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 z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t.j. Dz.U. z 2021 r. poz. 576 z późn. zm.

Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości, Dz.U. poz. 2447.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej, Dz.U. z 2020 r. poz. 346, 568 i 695.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2020 r. poz. 344.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, t.j. Dz.U. z 2021 r. poz. 1907 z późn. zm.

Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, Dz.U. poz. 2333.

Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej, Dz.U. z 2019 r. poz. 712 i 2020.

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. z 2019 r. poz. 869, z późn. zm.

Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, t.j. Dz.U. z 2021 r. poz. 2439 z późn. zm.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. z 2020 r. poz. 1369 z późn. zm.

Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, t.j. Dz.U. z 2021 r. poz. 1844 z późn. zm.

Ustawa z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym, t.j. Dz.U. z 2021 r. poz. 140 z późn. zm.

Wajda P., *Rekomendacje Komisji Nadzoru Finansowego dla zakładów ubezpieczeń i zakładów reasekuracji*, „Wiadomości Ubezpieczeniowe" 2016, nr 3.

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

Wyrok Sądu Okręgowego w Łodzi z dnia 16 maja 2019 r., sygn. III Ca 2139/18.

Wyrok Trybunału Konstytucyjnego z dnia 15 czerwca 2011 r., sygn. akt K 2/09, Dz. U z 2011 r., nr 134, poz. 788.

Zalcewicz A. [w:] J. Byrski (red.), *Ustawa o usługach płatniczych. Komentarz*, wyd. II, Warszawa 2021.