ARTYKUŁY

„Polityka i Społeczeństwo" 1(23) / 2025
DOI: 10.15584/polispol.2025.1.7

Agnieszka Jankowska[*], Monika Kwiecień-Miland[**]

PODMIOTY KRAJOWEGO SYSTEMU BEZPIECZEŃSTWA

Streszczenie

Przedmiotem niniejszego opracowania jest sformułowanie odpowiedzi na pytanie, czy wyróżnienie określonych podmiotów w ramach krajowego systemu cyberbezpieczeństwa oraz powierzenie im konkretnych zadań w tym obszarze mieści się w realizacji zasady zapewniania bezpieczeństwa. Jest to wartość chroniona, a jej implementacja jest skierowana do władz publicznych. Z tego względu na podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa należy spojrzeć z perspektywy wypełniania tego obowiązku. Problem badawczy jest aktualny nie tylko z uwagi na występujące coraz częściej zjawiska cyberzagrożeń i cyberataków, ale również ze względu na procedowaną obecnie nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, której celem jest m.in. dostosowanie jej do przepisów prawa unijnego.

Słowa kluczowe: Konstytucja RP, bezpieczeństwo, cyberbezpieczeństwo, krajowy system cyberbezpieczeństwa, podmioty krajowego systemu cyberbezpieczeństwa

Wstęp

Ustawa o krajowym systemie cyberbezpieczeństwa[1] (UKSC) została uchwalona 5 lipca 2018 r. Stanowiła bardzo ważną i przełomową regulację, która wprowadziła szereg instytucji prawnych, niefunkcjonujących do tej pory. Zagadnienie ochrony cyberprzestrzeni na stałe zagościło w systemie prawnym, a jednym z ważniejszych uregulowań ustawy było stworzenie systemu określonych podmiotów, które odpowiadają za bezpieczeństwo cyfrowe całego państwa. Pojęcie cyberbezpieczeństwa nie funkcjonuje jednak jako byt odrębny, ale należy przyjąć, że jest ono

[*] E-mail: agnieszka.jankowska1@op.pl, ORCID: 0009-0001-8423-5426.

[**] Europejska Wyższa Szkoła Prawa i Administracji w Warszawie, e-mail: mkwiecien-miland@ewspa.edu.pl, ORCID: 0000-0002-2281-9274.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024, poz. 1077, dalej: UKSC).

elementem szerszego pojęcia bezpieczeństwa. Konstytucja RP[2] w art. 5 wśród wielu chronionych wartości, takich jak niepodległość, nienaruszalność terytorium, wolności i prawa człowieka i obywatela, stanowi, iż obowiązkiem państwa jest również zapewnienie bezpieczeństwa obywateli. Wyszczególnienie tych zadań jest rzeczą bardzo istotną, ponieważ wynikają z nich konkretne kompetencje i zadania organów państwowych[3]. Pomimo nałożenia na organy władzy publicznej obowiązku realizacji celów wskazanych w art. 5, Konstytucja nie wskazuje jednak ani środków, ani sposobów ich realizacji. Ustalenie treści tego obowiązku wymaga zatem odwołania się zarówno do innych przepisów prawnych, jak i do wiedzy o charakterze pozaprawnym[4].

W ujęciu tradycyjnym pojęcie bezpieczeństwa obywateli jest rozumiane jako przeciwdziałanie zagrożeniom porządku publicznego, życia, zdrowia i mienia obywateli oraz związane z nimi powstrzymywanie i odpieranie wszelkich działań godzących w te dobra, zarówno pochodzących z zewnątrz, spoza granic, jak i z wewnątrz kraju. Współcześnie należy je jednak rozumieć znacznie szerzej[5], a mianowicie jako stan dający poczucie pewności i stabilności oraz ochrony[6].

Celem niniejszego opracowania jest zatem udzielenie odpowiedzi na pytanie, czy dobór określonych podmiotów dokonany przez ustawodawcę w UKSC oraz powierzenie im określonych zadań z zakresu cyberbezpieczeństwa mieści się w realizacji obowiązku państwa zapewniania bezpieczeństwa obywatelom. Cel badawczy wymaga dogłębnej analizy przepisów prawnych regulujących KSC, ale z punktu widzenia podmiotów, które go tworzą, ich określonego doboru, przydzielonych zadań i wzajemnych zależności.

Pojęcie bezpieczeństwa i cyberbezpieczeństwa

Pojęcie bezpieczeństwa pochodzi z języka łacińskiego, w którym *securitas* oznacza sytuację *sine cura*, czyli niewymagającą opieki[7]. Należy podkreślić, że konstytucyjne pojęcie bezpieczeństwa odnosi się jedynie

[2] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997, nr 78, poz. 483 z późn. zm.).

[3] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.

[4] P. Tuleja [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Czarny [i in.], Warszawa 2023.

[5] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 52–53.

[6] P. Tuleja, *op.cit.*

[7] I. Niczyporuk-Chudecka, *Konstytucyjna regulacja funkcji ochrony państwa,* Białystok 2021.

do bezpieczeństwa obywateli i nie można tego utożsamiać z bezpieczeństwem państwa, co nie zmienia faktu, że w przypadku zagrożenia bezpieczeństwa państwa zagrożone jest również bezpieczeństwo obywateli[8].

Niewątpliwie realny wpływ na bezpieczeństwo obywateli i państwa mają politycy, ale samo ujęcie bezpieczeństwa, jego interpretacja oraz wszelkie typologie są jednak domeną nauki[9]. W literaturze przedmiotu istnieje wiele typów definicji bezpieczeństwa, ponieważ pojęcie to ma charakter wieloaspektowy. Z tego względu praktycznie każda praca naukowa zawiera jakąś propozycję ujęcia bezpieczeństwa, które zostało zaproponowane na potrzeby przedstawienia konkretnego problemu badawczego. Nie inaczej postąpiono zatem w niniejszym opracowaniu, w którym przyjęto, iż bezpieczeństwo ma zdecydowanie charakter interdyscyplinarny oraz utylitarny, co powoduje, że nie może ono być rozpatrywane jako wartość odrębna od innych[10] i nie funkcjonuje jako byt samodzielny, ale zawsze odnosi się do jakiejś innej wartości, a ściślej jest tylko środkiem do osiągnięcia tej innej wartości, np. zdrowia czy własności[11]. Takie ujęcie tematu pozwala na wyróżnienie bezpieczeństwa energetycznego, ekologicznego oraz bezpieczeństwa cyfrowego, funkcjonującego już pod nazwą cyberbezpieczeństwa.

Natomiast co do definiowania pojęcia cyberbezpieczeństwa, to w przestrzeni regulacyjnej krajów i organizacji międzynarodowych istnieje różnorodne podejście do tego tematu i koncentruje się ono na określonych jego aspektach, np. technicznym, technologicznym, operacyjnym, ludzkim lub ich kombinacji. Najczęściej wskazuje się, iż cyberbezpieczeństwo to pojęcie obejmujące szereg działań, procedur, technologii oraz zasad, które mają na celu zapewnienie ochrony oraz przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni i dotyczącym wszystkich jej użytkowników, zarówno obywateli, jak i jednostek prawnych prywatnych oraz publicznych[12]. Wskazuje na to m.in. definicja stosowana przez Komisję Europejską, zgodnie z którą pojęcie

[8] B. Sosnowski, *Konstytucyjne zadania Państwa wynikające z art. 5 Konstytucji Rzeczypospolitej Polskiej z 1997 roku*, s. 131, Academia, https://www.academia.edu (31.08.2024).

[9] B. Zdrodowski, *Istota bezpieczeństwa państwa,* „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate", 2019, nr 9, s. 47.

[10] H. Zięba-Załucka, *Konstytucyjne aspekty bezpieczeństwa*, „Studia Iuridica Lublinensia", 2014, t. XXII, s. 416.

[11] J. Szmyd, *Bezpieczeństwo jako wartość, refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem: międzynarodowa konferencja naukowa, Kraków 11–13 maja 2000*, red. P. Tyrała, Kraków 2000, s. 48.

[12] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law", 2019, nr 2.

cyberbezpieczeństwa oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami[13].

W Polsce ustawodawca zdefiniował cyberbezpieczeństwo jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[14]. Relacja pomiędzy pojęciami cyberbezpieczeństwo oraz cyberprzestrzeń jest ścisła i komplementarna, gdyż cyberprzestrzeń jest przestrzenią, w której działają wszystkie systemy cyfrowe i sieci oraz użytkownicy, a cyberbezpieczeństwo ma za zadanie ich ochronę. Definicję legalną cyberprzestrzeni w polskim ujęciu prawnym znajdujemy w ustawie o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, ustawie o stanie wyjątkowym oraz ustawie o stanie klęski żywiołowej[15]. W ustawach tych pojęcie cyberprzestrzeni ujednolicono i zdefiniowano jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Taką samą definicją cyberprzestrzeni posługuje się *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, dokument określający strategiczne cele i środki polityczne oraz regulacyjne, których realizacja ma zapewnić odporność systemów informacyjnych, operatorów usług kluczowych oraz infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej[16].

---

[13] 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) 526/2013 (Dz. Urz. UE L 151 z 7.06.2019, s. 15).

[14] UKSC w zakresie swojej regulacji wdraża 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 (Dz. Urz. UE L 194 z 19.07.2016, s. 1).

[15] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2022, poz. 2091 z późn. zm.); Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. 2017, poz. 1897); Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. 2017, poz. 1928).

[16] *Strategia Cyberbezpieczeństwa RP na lata 2019–2024, zaakceptowana przez Radę Ministrów w dniu 22 października 2019 r., obowiązująca od 31 października 2019 roku*, Gov.pl, https://www.gov.pl (31.08.2024).

W dzisiejszym świecie dynamicznego postępu technologicznego cyberbezpieczeństwo oraz cyberprzestrzeń stają się nowym wymiarem aktywności państwa w zakresie realizacji zadań związanych z ochroną obywateli, osób prawnych, w tym przedsiębiorstw oraz instytucji publicznych. Cyberprzestrzeń staje się nowym wymiarem bezpieczeństwa, zaś cyberbezpieczeństwo jest „procesem zapewnienia bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni”[17].

Klasyfikacja podmiotów Krajowego Systemu Bezpieczeństwa

Art. 3 UKSC określa cel Krajowego Systemu Cyberbezpieczeństwa (KSC), którym jest 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. Cyberbezpieczeństwo zostało zatem uznane za dobro podlegające ochronie.

Dla realizacji powyższego celu w art. 4 UKSC ustanowiono sieć podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, które mają swoje określone zadania i ściśle ze sobą współpracują. Pod względem funkcjonalnym podmioty te można podzielić na administrację systemu (organy i inne podmioty administrujące w ramach uprawnień określonych w przepisach UKSC), uczestników systemu (operatorów usług kluczowych, dostawców usług cyfrowych oraz podmioty publiczne jako adresatów obowiązków, o których mowa w rozdziale 5 UKSC) oraz podmioty wspierające uczestników systemu (podmioty świadczące usługi z zakresu cyberbezpieczeństwa i akredytowane jednostki oceniające)[18].

[17] S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego”, 2022, nr 14, s. 200; C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2023, s. 27.

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

Operatorzy kluczowi i dostawcy usług cyfrowych

Krajowy system cyberbezpieczeństwa na poziomie krajowym ma na celu m.in. zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, o których mowa w art. 3 UKSC, zaś jednym z kluczowych aspektów ustawy jest regulacja działalności operatorów usług kluczowych oraz dostawców usług cyfrowych. Obie te grupy podmiotów pełnią istotną rolę w zapewnieniu bezpieczeństwa cybernetycznego kraju, jednak ich funkcjonowanie i zadania różnią się w zależności od charakteru świadczonych usług oraz stopnia ich krytyczności dla społeczeństwa i gospodarki. Podmioty te są uczestnikami KSC i na nich spoczywają obowiązki wymienione w rozdziale 5 UKSC.

Operatorzy usług kluczowych to podmioty, które posiadają jednostki organizacyjne na terytorium Rzeczypospolitej, wobec których organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. W załączniku nr 1 do UKSC określono sektory (m.in. energia, transport), podsektory (m.in. energia elektryczna, transport lotniczy) oraz rodzaje podmiotów (m.in. zarządzający lotniskiem), zaś decyzja o uznaniu podmiotu za operatora usługi kluczowej należy do organu właściwego ds. cyberbezpieczeństwa, który wydaje ją na podstawie kryteriów wymienionych w art. 5 UKSC. Zgodnie z ustawą usługi kluczowe muszą spełniać trzy podstawowe warunki: są niezbędne dla utrzymania kluczowych funkcji społecznych lub działalności gospodarczej; świadczenie tych usług zależy od systemów informatycznych; incydent, który dotknie tych usług, może spowodować zakłócenia w świadczeniu usługi kluczowej. A zatem funkcjonowanie operatorów usług kluczowych ma fundamentalne znaczenie dla bezpieczeństwa państwa i jego obywateli. Współcześnie społeczeństwo jest silnie związane z systemami cyfrowymi, a zakłócenia świadczenia takich usług kluczowych, jak energia, transport czy finanse, może mieć katastrofalne skutki. Dostawcy usług kluczowych mają szereg obowiązków do wypełnienia w celu zagwarantowania ciągłości działania ich systemów oraz minimalizacji ryzyka cyberataków. Obowiązki te wymieniono w rozdziale 3 UKSC, a najważniejsze z nich obejmują:

- zarządzanie ryzykiem, a więc wdrożenie odpowiednich środków technicznych i organizacyjnych, które pozwolą na identyfikację, analizę i ocenę ryzyka związanego z bezpieczeństwem systemów informacyjnych;
- zgłaszanie do właściwego zespołu CSIRT (będzie o nich mowa w dalszej części artykułu) istotnych dla usług kluczowych incydentów, ich obsługa oraz współpraca z CSIRT w celu minimalizacji skutków incydentów;

– prowadzenie dokumentacji dotyczącej stosowanych środków bezpieczeństwa oraz incydentów bezpieczeństwa;
– regularne poddawanie swoich systemów audytom i weryfikacji w celu sprawdzenia zgodności z obowiązującymi przepisami oraz oceny, czy wdrożone środki bezpieczeństwa są wystarczające.

Dostawcy usług cyfrowych to osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, mające siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej, albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadczące usługi cyfrowe, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o który mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców. Rodzaje usług cyfrowych określone są w załączniku nr 2 do UKSC i obejmują internetową platformę handlową, usługę przetwarzania w chmurze oraz wyszukiwarkę internetową. Dostawcy usług cyfrowych, podobnie jak operatorzy usług kluczowych, mają obowiązki dotyczące zapewnienia cyberbezpieczeństwa, ale ich zakres jest nieco inny, mniej rygorystyczny z uwagi na globalny charakter usług cyfrowych i mniejszy stopień bezpośredniego wpływu na krytyczne funkcje społeczne. Obowiązki dostawców usług cyfrowych zostały określone w rozdziale 4 UKSC i obejmują m.in.:
– wdrożenie odpowiednich środków bezpieczeństwa, które zapewniają ochronę przed zagrożeniami w cyberprzestrzeni;
– zgłaszanie właściwemu zespołowi CSIRT incydentów bezpieczeństwa, które mogą wpłynąć na świadczenie przez nich usług;
– w przypadku wystąpienia incydentu, który może mieć wpływ na bezpieczeństwo narodowe lub gospodarkę, współpraca z organami państwowymi;
– ochrona danych użytkowników przed nieuprawnionym dostępem.

Obecnie większość sektorów gospodarki korzysta masowo z usług cyfrowych, w wielu przypadkach usługi te są wręcz niezbędne dla funkcjonowania wielu przedsiębiorstw, zatem zakłócenie takich usług, jak platformy *e-commerce* czy usługi chmurowe może spowodować znaczące straty gospodarcze. Z tego względu dostawcy usług cyfrowych stanowią równie ważny element KSC, jak operatorzy usług kluczowych, pomimo że obowiązki nałożone na nich przez ustawę i zadania z niej wynikające są mniej rygorystyczne.

Podmioty świadczące usługi z zakresu cyberbezpieczeństwa pełnią funkcję wspierającą innych uczestników KSC, a więc operatorów usług kluczowych oraz dostawców usług cyfrowych. Są to firmy oraz organizacje, które oferują usługi związane z ochroną systemów informatycznych, reagowaniem na incydenty oraz zabezpieczaniem infrastruktury teleinfor-

matycznej. Usługi te obejmują m.in. monitorowanie bezpieczeństwa systemów, zarządzanie incydentami, doradztwo w zakresie wdrażania środków ochrony, przeprowadzanie audytów i testów penetracyjnych.

Mimo że UKSC nie nakłada na te podmioty bezpośrednich obowiązków w zakresie zgłaszania incydentów, to ich działania są istotne z punktu widzenia wsparcia innych podmiotów, które są objęte regulacjami ustawy, na przykład operatora usługi kluczowej w celu realizacji nałożonych na niego zadań z zakresu zarządzania incydentami. Ponadto, podmioty świadczące usługi z zakresu cyberbezpieczeństwa są o tyle istotne dla krajowego systemu cyberbezpieczeństwa, że również współpracują z innymi jednostkami KSC – organami oraz podmiotami administrującymi, w tym z zespołami CSIRT. Trzy wymienione wielopodmiotowe kategorie jednostek KSC podejmują działania mające na celu minimalizację ryzyka związanego z cyberzagrożeniami i cyberatakami. Cały system cyberbezpieczeństwa w Polsce opiera się na współpracy tych kategorii podmiotów z organami państwowymi, a także na ścisłej koordynacji działań w ramach zespołów CSIRT.

Operatorzy usług kluczowych odpowiadają za systemy o znaczeniu strategicznym dla państwa i obywateli, natomiast dostawcy usług cyfrowych zapewniają kluczowe funkcje gospodarki cyfrowej, z kolei podmioty świadczące usługi z zakresu cyberbezpieczeństwa wspierają zarówno operatorów usług kluczowych, jak i dostawców usług cyfrowych w ochronie ich infrastruktury oraz reagowaniu na incydenty. Współpraca między tymi grupami podmiotów a organami państwowymi, w tym zespołami CSIRT, ma zatem zasadnicze znaczenie dla bezpieczeństwa cyberprzestrzeni w Polsce.

Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)

Kolejnym, istotnym elementem KSC są Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (*Computer Security Incident Response Team* – CSIRT) oraz sektorowe zespoły cyberbezpieczeństwa. Jest to grupa podmiotów, którym przypisano funkcję administrowania krajowym systemem cyberbezpieczeństwa i które podlegają podmiotom wymienionym w art. 4 pkt 17–20 UKSC[19]. Działalność tych podmiotów koncentruje się na podnoszeniu poziomu bezpieczeństwa innych uczestników KSC, a ich szczegółowe zadania określone zostały w rozdziale 6 UKSC.

[19] G. Szpor, *op.cit.*

Ustawa określa trzy krajowe zespoły CSIRT: CSIRT MON, CSIRT NASK i CSIRT GOV, a także sektorowe zespoły cyberbezpieczeństwa, które wspólnie tworzą infrastrukturę reagowania na incydenty oraz zapobiegania im. CSIRT MON to zespół reagowania na incydenty bezpieczeństwa komputerowego w sektorze obronnym. Zespół ten funkcjonuje pod nadzorem Ministra Obrony Narodowej i skupia się na ochronie kluczowych systemów informatycznych oraz sieci, które mają strategiczne znaczenie dla bezpieczeństwa narodowego, szczególnie w kontekście obronności i działalności Sił Zbrojnych Rzeczypospolitej Polskiej. Główne zadania CSIRT MON obejmują monitorowanie systemów informatycznych i infrastruktury krytycznej sektora obronnego oraz reagowanie na incydenty, zapewnianie wsparcia technicznego podmiotom odpowiedzialnym za bezpieczeństwo w sektorze obronnym, a także analizowanie zagrożeń i podatności. Zgodnie z art. 26 ust. 5 UKSC, CSIRT MON koordynuje obsługę incydentów zgłaszanych przed podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, jak również te, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są sporządzanym przez Dyrektora Rządowego Centrum Bezpieczeństwa jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

Ponadto, CSIRT MON prowadzi działania z zakresu współpracy międzynarodowej w kontekście obronności, współpracując m.in. z jednostkami NATO oraz sojusznikami militarnymi w celu wymiany informacji o zagrożeniach oraz skutecznych środkach zaradczych. Tym samym CSIRT MON pełni kluczową rolę w ochronie narodowej cyberprzestrzeni, dbając o bezpieczeństwo informatycznych systemów wojskowych i infrastruktury krytycznej, których utrata lub naruszenie mogłoby prowadzić do zagrożenia suwerenności państwa. A zatem, istotę funkcji ochrony państwa tworzy właśnie m.in. konstytucyjna wartość bezpieczeństwa, wskazana w art. 5 Konstytucji, zaś jej trzonem jest m.in. ważna rola Sił Zbrojnych, które gwarantują bezpieczeństwo jednostki i państwa, w tym cyberbezpieczeństwo[20].

CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy[21]) odpowiada za obsługę incydentów naru-

[20] K. Prokop, *Konstytucyjne podstawy bezpieczeństwa narodowego – kilka uwag krytycznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E. M. Guzik-Makaruk, E.W. Pływaczewski, Białystok 2015, s. 279.

[21] Naukowa i Akademicka Sieć Komputerowa powstała w 1993 r. jako państwowy instytut badawczy. W 1996 r. w ramach NASK powstał CERT Polska, dziś CSIRT NASK, który określany jest jako tzw. CERT ostatniej szansy, gdyż każdy, bez względu na osobowość prawną czy obywatelstwo, może zgłosić do niego incydent, który nie jest obsługiwany przez pozostałe CSIRT-y. K. Chałubińska-Jentkiewicz, M. Nowikowska, *Podmioty zaangażowane*

szających bezpieczeństwo sieci informatycznych w sektorze prywatnym oraz w zakresie infrastruktury krytycznej. NASK podlega ministrowi właściwemu ds. informatyzacji, pełni funkcję koordynatora działań w zakresie ochrony sieci i systemów informatycznych przedsiębiorstw oraz operatorów usług kluczowych. Najważniejsze zadania CSIRT NASK obejmują monitorowanie i analizę incydentów w sektorze prywatnym oraz w zakresie infrastruktury krytycznej, a także udzielanie wsparcia technicznego, przede wszystkim przedsiębiorstwom zarządzającym infrastrukturą krytyczną, w zakresie szybkiego reagowania na incydenty oraz wdrożenia odpowiednich środków ochronnych. CSIRT NASK prowadzi również szerokie działania edukacyjne, współpracuje z innymi zespołami CSIRT oraz instytucjami i zespołami międzynarodowymi.

CSIRT GOV z kolei jest rządowym zespołem odpowiedzialnym za reagowanie na incydenty bezpieczeństwa komputerowego w sektorze publicznym. Zespół ten funkcjonuje w ramach Agencji Bezpieczeństwa Wewnętrznego od stycznia 2008 r. i zajmuje się ochroną systemów informatycznych administracji państwowej, jednostek samorządu terytorialnego oraz innych instytucji państwowych, których działalność jest kluczowa z punktu widzenia funkcjonowania państwa.

Najważniejsze zadania CSIRT GOV obejmują monitorowanie, wykrywanie i zapobieganie zagrożeniom bezpieczeństwa w systemach informatycznych organów administracji publicznej lub systemach i sieciach teleinformatycznych, stanowiących infrastrukturę krytyczną. CSIRT GOV odpowiada za koordynowanie obsługi incydentów zgłaszanych przez podmioty wymienione w art. 26 ust. 7 UKSC, tj. administrację rządową, jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane, Narodowy Bank Polski oraz Bank Gospodarstwa Krajowego. Ponadto, CSIRT GOV jest właściwym zespołem reagowania w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym. Zespół ten, jak pozostałe CSIRT-y krajowe, zobowiązany jest współpracować z innymi zespołami CSIRT krajowymi oraz międzynarodowymi.

Obok wyżej wymienionych trzech krajowych CSIRT, UKSC w art. 44 przewiduje tworzenie sektorowych zespołów cyberbezpieczeństwa dla sektora lub podsektora wymienionego w załączniku nr 1 do ustawy. Sektorowy zespół cyberbezpieczeństwa, który ma na celu wsparcie dla operatorów usług kluczowych, tworzony jest zgodnie z odrębnymi przepisami regulującymi funkcjonowanie podmiotów w danym sektorze[22].

---

w politykę zapewniania bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2), „Cybersecurity and Law", 2024, nr 2, s. 15–16.

[22] K. Prusak-Górniak, K. Silicki [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz…*

Przykładowo dla utworzonego w Polsce sektorowego zespołu dedykowanego dla sektora bankowego CSIRT KNF, który funkcjonuje od 1 lipca 2020 r., były to przepisy prawa bankowego[23]. W przypadku utworzenia takiego zespołu sektorowego art. 44 UKSC wyszczególnia obszary jego odpowiedzialności, które koncentrują się przede wszystkim na obowiązkach w zakresie przyjmowania zgłoszeń o incydentach poważnych, wspierania obsługi tych incydentów, wspierania operatorów usług kluczowych w zakresie ich obowiązków, analizowania incydentów poważnych. Katalog głównych zadań wskazanych w UKSC nie jest zamknięty, zatem podmiot tworzący zespół sektorowy ma dowolność w jego rozszerzeniu. Ponadto, największą zaletą takich zespołów jest to, że posiadają one specyficzne dla danego sektora lub podsektora wiedzę oraz doświadczenie, a także zrozumienie dla jego potrzeb i wyzwań. Zespół sektorowy obowiązany jest do koordynacji i współpracy z krajowymi zespołami CSIRT, zwłaszcza w zakresie incydentów o znaczeniu krajowym, a także z organami regulacyjnymi oraz nadzorczymi, które odpowiadają za dany sektor. Jednak należy pamiętać, że zespół sektorowy jest podmiotem pośrednim pomiędzy właściwym krajowym CSIRT a operatorami usług kluczowych, a w przypadku wystąpienia incydentu poważnego, operator usługi kluczowej zgłasza informację zarówno do właściwego krajowego CSIRT, jak i do CSIRT sektorowego. Sektorowy zespół CSIRT stanowi wsparcie dla dostawców usług kluczowych w danym sektorze i jednocześnie jest podmiotem pośrednim pomiędzy dostawcą usług kluczowych a właściwym krajowym zespołem CSIRT. Pomimo funkcjonowania zespołów sektorowych wypełnienie obowiązków ustawowych spoczywa na dostawcach usług kluczowych, krajowych zespołach CSIRT, a także na właściwych organach państwowych administrujących w ramach KSC[24].

Podmioty publiczne

UKSC określa podmioty wymienione w art. 4 pkt 7–15 jako publiczne. Wśród nich część jest określona z nazwy (Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji oraz Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej i wojewódzkie fundusze ochrony środowiska i gospodarki wodnej), a część wskazana

[23] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. 2023, poz. 2488 z późn. zm.). Zadania CSIRT KNF na stronie internetowej Komisji Nadzoru Finansowego: https://www.knf.gov.pl (31.08.2024).

[24] K. Chałubińska-Jentkiewicz, M. Nowikowska, *op.cit.,* s. 15–16.

jedynie nazwą generalną (podmioty sektora jednostek finansów publicznych, instytuty badawcze oraz spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy o gospodarce komunalnej). Dokładne ustalenie katalogu tych podmiotów wymaga zatem sięgnięcia do innych ustaw, do których odsyła UKSC.

Ustalenie podmiotów tworzących sektor finansów publicznych, które zostały zaliczone do KSC, wymaga zapoznania się z art. 9 ustawy o finansach publicznych[25], który pozwala wyróżnić następujące jednostki: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; uczelnie publiczne oraz Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne. Grupa ta jest najliczniejsza, ponieważ z wyjątkiem pięciu kategorii podmiotów wyłączonych przez UKSC z art. 9 ustawy o finansach publicznych, do KSC wchodzą prawie wszystkie jednostki sektora finansów publicznych. Daje to wręcz ogromną liczbę różnych podmiotów, które z punktu widzenia funkcjonowania administracji państwowej mają odmienne kompetencje, a co za tym idzie, różny status prawny.

Jeśli chodzi o instytuty badawcze, to zgodnie z art. 1 ust. 1 ustawy o instytutach badawczych[26] są to państwowe jednostki organizacyjne, wyodrębnione pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, które prowadzą badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce. Dane dotyczące nazw i liczby poszczególnych instytutów badawczych są na bieżąco udostępniane na stronie Rady Głównej Instytutów Badawczych[27].

Nieco trudniejsze jest określenie liczby podmiotów będących spółkami prawa handlowego wykonującymi zadania o charakterze użyteczności publicznej. W tym przypadku UKSC odwołuje się do definicji zawartej w art. 1 ust. 2 ustawy o gospodarce komunalnej[28], zgodnie z którą gospodarka komunalna obejmuje w szczególności zadania reali-

[25] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2024, poz. 1270).

[26] Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz.U. 2024, poz. 534).

[27] Baza instytutów badawczych, https://www.rgib.org.pl/ (31.08.2024).

[28] Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. 2021, poz. 679 z późn. zm.).

zowane przez jednostki samorządu terytorialnego o charakterze użyteczności publicznej, których celem jest bieżące i nieprzerwane zaspokajanie zbiorowych potrzeb ludności w drodze świadczenia usług powszechnie dostępnych. Art. 2 tej ustawy doprecyzowuje, że gospodarka komunalna może być prowadzona przez gminy w formie spółek prawa handlowego, których enumeratywne wyliczenie zawiera art. 1 § 2 Kodeksu spółek handlowych[29]. Spółki takie mogą być tworzone przez jednostki samorządu terytorialnego w celu realizowania usług publicznych, takich jak np. ochrona zdrowia, oświata, opieka społeczna, transport czy gospodarka odpadami.

Biorąc pod uwagę wymienioną powyżej grupę podmiotów, należy przede wszystkim zauważyć, że ustalanie ich dokładnej liczby mija się z celem i niczego nie wniesie poza suchą informacją. O wiele ważniejsze jest zwrócenie uwagi na bardzo istotny fakt, iż katalog podmiotów publicznych, które zostały włączone do KSC, jest niezwykle szeroki. Znajdują się w nim bowiem podmioty o różnym statusie prawnym, posiadające kompetencje praktycznie w każdym obszarze działalności państwowej, a co za tym idzie, mające niezwykle istotny wpływ na funkcjonowanie obywatela w różnych jego rolach i podejmowanych działalnościach. W przypadku realizowania zadań publicznych z użyciem systemu teleinformatycznego, w którym przetwarzane są dane w postaci elektronicznej, podmioty publiczne mają konkretne obowiązki. Przede wszystkim są odpowiedzialne za zarządzanie, zgłaszanie i obsługę tzw. incydentu, czyli zdarzenia niekorzystnie wpływającego na cyberbezpieczeństwo, które powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego. W tym celu powinny wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami KSC.

Zadania podmiotów publicznych dotyczące reagowania na incydenty stanowią ważną część ich działalności, a ich właściwa realizacja przyczynia się do osiągnięcia pożądanego stopnia bezpieczeństwa w obszarze cyfrowym na poziomie całego kraju. Natomiast szeroki dobór kręgu podmiotów publicznych dowodzi wysokiej świadomości ustawodawcy w dostrzeganiu potencjalnych cyberzagrożeń praktycznie w każdym aspekcie działalności państwa. Wydaje się zatem, że podejście ustawodawcy do kwestii sporządzenia katalogu podmiotów publicznych włączonych do KSC należy oceniać bardzo pozytywnie, co pozwala na wyciągnięcie wniosku, że ustawodawca niezwykle poważnie potraktował zagadnienie zapewnienie bezpieczeństwa.

[29] Ustawa z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz.U. 2024, poz. 18).

Organy właściwe ds. cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Wśród podmiotów wymienionych w tym zestawieniu najliczniejszą grupę tworzą tzw. organy właściwe do spraw cyberbepieczeństwa. W ich przypadku, na potrzeby UKSC, ustawodawca wyróżnił jedenaście obszarów, które w działalności państwa uznał za najbardziej strategiczne. W zakresie każdego z tych obszarów ustanowił właściwość sześciu ministrów oraz Komisji Nadzoru Finansowego (KNF). Ministrowie odpowiadają za przydzielony obszar lub obszary, które należą do określonego działu administracji pozostającego w kompetencji danego ministra. Przemawia za tym fakt, iż organy te (z wyjątkiem KNF) dysponują odpowiednimi możliwościami prawnymi oraz zasobami niezbędnymi do skutecznej realizacji powierzonych zadań[30]. Natomiast KNF przydzielono sektor bankowy i infrastrukturę rynków finansowych ze względu na fakt, iż zgodnie z art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, do zadań Komisji należy nadzór nad rynkiem finansowym[31]. Szczegółowy podział na obszary i odpowiadające im organy został przedstawiony w tabeli 1.

Tabela 1. Przypisanie sektorów organom właściwym

Obszar działalności państwa	**Organ właściwy do spraw cyberbezpieczeństwa**
1	*2*
sektor energii	minister właściwy do spraw energii
sektor transportu z wyłączeniem podsektora transportu wodnego	minister właściwy do spraw transportu
podsektor transportu wodnego	minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej
sektor bankowy i infrastruktury rynków finansowych	Komisja Nadzoru Finansowego
sektor ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 UKSC	minister właściwy do spraw zdrowia
sektor ochrony zdrowia obejmujący podmioty, o których mowa w art. 26 ust. 5 UKSC	Minister Obrony Narodowej

[30] K. Prusak-Górniak, K. Silicki, *op.cit.*

[31] Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz.U. 2024, poz. 135).

1	*2*
sektor zaopatrzenia w wodę pitną i jej dystrybucji	minister właściwy do spraw gospodarki wodnej
sektor infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 UKSC	minister właściwy do spraw informatyzacji
sektor infrastruktury cyfrowej obejmujący podmioty, o których mowa w art. 26 ust. 5 UKSC	Minister Obrony Narodowej
dostawcy usług cyfrowych z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 UKSC	minister właściwy do spraw informatyzacji
dostawcy usług cyfrowych obejmujących podmioty, o których mowa w art. 26 ust. 5 UKSC	Minister Obrony Narodowej

Źródło: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024, poz. 1077).

Analiza powyższej tabeli pozwala zauważyć, że minister do spraw informatyzacji i Minister Obrony Narodowej[32] są właściwi w więcej niż jednym sektorze. Dodatkowo, w sektorach ochrony zdrowia, infrastruktury cyfrowej oraz dostawców usług cyfrowych pozostawiono właściwość Ministra Obrony Narodowej nad podmiotami, które mu podlegają lub są przez niego nadzorowane[33]. Co więcej, w przypadku ministra do spraw informatyzacji i Ministra Obrony Narodowej, UKSC oprócz zadań wspólnych dla wszystkich organów właściwych odrębnie określiła ich dodatkowe zadania. Ustawodawca zatem uznał, że znaczenie tych dwóch organów w realizacji konstytucyjnej zasady zapewniania bezpieczeństwa jest kluczowe i wyraźnie zaakcentował ich rolę w KSC.

Zadania powierzone organom właściwym koncentrują się wokół nadawania i wygaszania statusu operatora usługi kluczowej oraz ustanawiania, zgodnie z odrębnymi przepisami, sektorowego zespołu cyberbezpieczeństwa. W zakresie każdego wyróżnionego sektora lub podsektora dany organ właściwy jest zobowiązany do bieżącego monitorowania podmiotów pod kątem weryfikacji warunków, które kwalifikują dany podmiot jako operatora usługi kluczowej. Z punktu widzenia reali-

[32] W miejsce określenia „minister właściwy do spraw obrony" używa się „Minister Obrony Narodowej", ponieważ ustawodawca wyjątkowo określił jego status prawny w ustawie z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz.U. 2022, poz. 1438 z późn. zm.), która w art. 1 przesądza, że Minister Obrony Narodowej kieruje działem administracji rządowej „obrona narodowa".

[33] Przykładem podmiotu nadzorowanego przez Ministra Obrony Narodowej w sektorze ochrony zdrowia jest Wojskowy Instytut Medyczny Państwowy Instytut Badawczy w Warszawie.

zacji konstytucyjnej zasady zapewniania bezpieczeństwa jest to bardzo istotna kompetencja, którą każdy organ realizuje wobec podmiotów działających w ramach przydzielonego mu sektora lub podsektora. Decyzja administracyjna uznająca dany podmiot za operatora usługi kluczowej nie zawsze spotyka się z jego akceptacją, o czym świadczą spory sądowe pomiędzy organami i podmiotami[34].

Jeśli chodzi o Pojedynczy Punkt Kontaktowy (PPK), to jego prowadzenie jest jednym z zadań ministra właściwego do spraw informatyzacji. Głównym celem PPK jest koordynacja współpracy organów właściwych do spraw cyberbezpieczeństwa z odpowiednimi organami w państwach członkowskich Unii Europejskiej, współpraca z Komisją Europejską w obszarze cyberbezpieczeństwa oraz reprezentowanie i wymiana informacji w tzw. Grupie Współpracy na poziomie Unii Europejskiej. W praktyce PPK jest łącznikiem pomiędzy PPK w innych państwach członkowskich Unii Europejskiej a zespołami CSIRT lub sektorowymi zespołami bezpieczeństwa, którego celem jest przekazywanie im wzajemnie informacji o incydentach poważnych lub istotnych dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. Ponadto w ramach wymiany informacji PPK jest zobowiązany do bieżącego przekazywania Grupie Współpracy i Komisji Europejskiej informacji m.in. o realizowanej strategii i dobrych praktykach w obszarze cyberbezpieczeństwa.

Ostatnie dwa podmioty objęte KSC to Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa. Pełnomocnik w randze ministra, sekretarza lub podsekretarza stanu jest powoływany przez Prezesa Rady Ministrów, której podlega i składa roczne sprawozdanie, gdzie oprócz informacji może zawrzeć wnioski i rekomendacje. Głównym zadaniem Pełnomocnika jest koordynacja działań i realizacja polityki rządu w zakresie zapewnienia cyberbezpieczeństwa, na które składają się czynności mające na celu analizę funkcjonowania KSC, nadzorowanie procesu zarządzania ryzykiem, opiniowanie dokumentów rządowych i aktów prawnych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa oraz wydawanie rekomendacji dotyczących upowszechniania i zapewnienia cyberbezpieczeństwa na poziomie krajowym.

[34] Zob. m.in. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 grudnia 2019 r., VI SA/Wa 1436/19, LEX nr 2976744; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 sierpnia 2020 r., VI SA/Wa 2667/19, LEX nr 3068097; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 września 2020 r., VI SA/Wa 2151/19, LEX nr 3084055; wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 14 stycznia 2021 r., VI SA/Wa 2293/20, LEX nr 3161783 oraz Wyrok Naczelnego Sądu Administracyjnego z dnia 21 maja 2024 r., II GSK 557/21, LEX nr 3728727.

Kolegium do Spraw Cyberbezpieczeństwa działa przy Radzie Ministrów jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa, a także organów właściwych do spraw cyberbezpieczeństwa. W skład Kolegium wchodzi Prezes Rady Ministrów jako przewodniczący, Pełnomocnik, sekretarz Kolegium oraz członkowie Kolegium, którymi są minister właściwy do spraw wewnętrznych, informatyzacji, spraw zagranicznych, Minister Obrony Narodowej, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej, oraz minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub Szef Agencji Bezpieczeństwa Wewnętrznego.

Zadania Kolegium koncentrują się na wyrażaniu opinii głównie w zakresie kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa oraz w obrębie współdziałania w tym obszarze innych podmiotów i organów. Z uwagi na tak szeroki zakres zadań w posiedzeniach Kolegium uczestniczy Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca, Szef Służby Kontrwywiadu Wojskowego albo jego zastępca oraz Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego. Na podstawie rekomendacji Kolegium, Prezes Rady Ministrów w celu koordynacji działań administracji rządowej może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa oraz obsługi incydentów krytycznych.

Patrząc na umiejscowienie Pojedynczego Punktu Kontaktowego, Pełnomocnika oraz Kolegium do Spraw Cyberbezpieczeństwa w obrębie organów KSC, należy zauważyć, że w przeciwieństwie do organów właściwych, ich zadania polegają na zapewnieniu koordynacji działań systemu, wyznaczaniu celów i wymiany informacji. Podmioty te pełnią więc istotną funkcję w KSC, ponieważ są w stanie efektywnie formułować postulaty zmian w poszczególnych ogniwach tego systemu.

Zakończenie

Bezpieczeństwo jest wartością należącą do grupy najważniejszych, jeżeli chodzi o egzystencję każdego człowieka, a zarazem jest to jedna z jego ważniejszych potrzeb. Podstawowym zadaniem państwa powinno być zatem kompleksowe stworzenie, organizacja i doskonalenie systemu bezpieczeństwa, w taki sposób, aby je zapewnić

obywatelom[35]. Art. 5 Konstytucji RP nie rozstrzyga wprawdzie o całej materii zadań i obowiązków państwa polskiego wobec jednostki, ale sprawą bezsporną jest to, że prezentuje on główny katalog tych wartości, będących jednocześnie normami programowymi, które narzucają pewien kierunek działania państwa[36].

Analiza roli, struktur oraz funkcjonowania podmiotów wchodzących w skład KSC w Polsce pozwala na wyciągnięcie wniosku, iż dobór tych podmiotów oraz powierzone im kompetencje mieszczą się w realizacji zasady zapewnienia bezpieczeństwa obywateli. Natomiast cyberbezpieczeństwo, jako integralna część bezpieczeństwa państwa stanowiąca nowy wymiar funkcjonowania państwa i gospodarki, wymaga ochrony na równi z innymi obszarami bezpieczeństwa publicznego. Realizacją powyższego jest uchwalenie ustawy o krajowym systemie cyberbezpieczeństwa, która ustanawia krąg podmiotów objętych KSC oraz przypisuje im określony katalog obowiązków i zadań, który nie jest katalogiem zamkniętym.

Operatorzy usług kluczowych i dostawcy usług cyfrowych stanowią fundament KSC, są jego uczestnikami i adresatami obowiązków wymienionych w rozdziale 5 UKSC. Ich rola w ochronie krytycznych sektorów gospodarki ma bezpośredni wpływ na bezpieczeństwo obywateli, ponieważ ich działania są niezbędne dla ochrony kluczowych interesów społecznych i gospodarczych. Wsparciem dla operatorów usług kluczowych oraz dostawców usług cyfrowych są podmioty świadczące usługi z zakresu cyberbezpieczeństwa (podmioty wspierające). Te trzy wielopodmiotowe kategorie podmiotów krajowego systemu cyberbezpieczeństwa wspólnie realizują zadania z zakresu minimalizacji ryzyk związanych z cyberzagrożeniami i cyberatakami oraz współpracują z organami państwowymi i innymi podmiotami administrującymi w ramach KSC (m.in. krajowe zespoły CSIRT, podmioty wymienione w art. 4 pkt 7–15 i 17–20 UKSC). Współpraca i koordynacja oraz jasne określenie obowiązków i zadań ma kluczowe znaczenie dla zapewnienia bezpiecznej polskiej cyberprzestrzeni, a tym samym dla bezpieczeństwa państwa i obywateli.

Tak szeroki krąg podmiotów publicznych włączonych do KSC wskazuje na wysoką świadomość ustawodawcy w zakresie cyberzagrożeń i ich potencjalnych skutków dla bezpieczeństwa narodowego. Rozciągnięcie realizacji zasady zapewniania bezpieczeństwa na różne obsza-

[35] M. Huczek, *Problematyka zarządzania bezpieczeństwem w organizacji samorządu terytorialnego i szkołach wyższych*, Humanitas, https://www.humanitas.edu.pl (31.08.2024).

[36] B. Sosnowski, *op.cit.*, s.131.

ry administracji publicznej i sektora prywatnego świadczy o całościowym podejściu do ochrony obywateli. Rola podmiotów KSC w ochronie kluczowych funkcji państwa oraz przeciwdziałaniu cyberzagrożeniom ma fundamentalne znaczenie w kontekście współczesnych wyzwań bezpieczeństwa.

Jedocześnie, pomimo tak szerokiego zakresu zadań i kompetencji przypisanych podmiotom krajowego systemu cyberbezpieczeństwa, wobec masowo rosnącej liczby incydentów cyberbezpieczeństwa, należy zwrócić uwagę na wyzwania wiążące się z koniecznością ciągłego doskonalenia koordynacji między podmiotami KSC, bieżącej walidacji skuteczności stosowanych procedur i procesów oraz regularnej analizy zakresów przypisanych obowiązków i zadań.

Należy stwierdzić, że analiza doboru konkretnych podmiotów tworzących krajowy system cyberbezpieczeństwa zdecydowanie pozwala na sformułowanie wniosku, iż ustawodawca, kierując się wytycznymi płynącymi z zasady zapewniania bezpieczeństwa, uchwalając przepisy UKSC, dokonał doboru i podziału tych podmiotów w sposób właściwy i przemyślany. Należy natomiast odnotować, że obecnie procedowana jest nowelizacja UKSC, mająca na celu m.in. dostosowanie do tzw. Dyrektywy NIS[37], którą należy postrzegać jako odpowiedź na dynamicznie zmieniające się warunki funkcjonowania Unii Europejskiej w obszarze cyberbezpieczeństwa. Analiza porównawcza znowelizowanych przepisów UKSC będzie przedmiotem odrębnego opracowania.

Bibliografia

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2023.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law", 2019, nr 2.

Chałubińska-Jentkiewicz K., Nowikowska M., *Podmioty zaangażowane w politykę zapewniania bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2)*, „Cybersecurity and Law", 2024, nr 2.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) 910/2014 i dyrektywę (UE)

[37] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz. Urz. UE L 333 z 27.12.2022, s. 80).

2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz. Urz. UE L 333 z 27.12.2022).

Huczek M., *Problematyka zarządzania bezpieczeństwem w organizacji samorządu terytorialnego i szkołach wyższych*, Humanitas, https://www.humanitas.edu.pl (31.08.2024).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., (Dz.U. 1997, nr 78, poz. 483 z późn. zm.).

Prokop K., *Konstytucyjne podstawy bezpieczeństwa narodowego – kilka uwag krytycznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E. M. Guzik-Makaruk, E.W. Pływaczewski, Białystok 2015, s. 279.

Prusak-Górniak K., Silicki K. [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

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

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) 526/2013 (Dz. Urz. UE L 151 z 7.06.2019).

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.

Sosnowski B., *Konstytucyjne zadania Państwa wynikające z art. 5 Konstytucji Rzeczypospolitej Polskiej z 1997 roku*, s. 131, Academia, https://www.academia.edu (31.08.2024).

Strategia Cyberbezpieczeństwa RP na lata 2019–2024, zaakceptowana przez Radę Ministrów w dniu 22 października 2019 r., obowiązująca od 31 października 2019 roku, Gov.pl, https://www.gov.pl (31.08.2024).

Szmyd J., *Bezpieczeństwo jako wartość, refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem: międzynarodowa konferencja naukowa, Kraków 11–13 maja 2000*, red. P. Tyrała, Kraków 2000.

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

Tuleja P. [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Czarny [i in.], Warszawa 2023.

Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego", 2022, 14.

Ustawa z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz.U. 2021, poz. 679 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. 2023, poz. 2488 z późn. zm.).

Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz.U. 2024, poz. 18).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2022, poz. 2091 z późn. zm.).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. 2017, poz. 1897).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. 2017, poz. 1928).

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2024, poz. 1270).

Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz.U. 2024, poz. 534).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024, poz. 1077).

Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U. 2024, poz. 1221).
Wyrok Naczelnego Sądu Administracyjnego z dnia 21 maja 2024 r., II GSK 557/21, LEX nr 3728727.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 grudnia 2019 r., VI SA/Wa 1436/19, LEX nr 2976744.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 sierpnia 2020 r., VI SA/Wa 2667/19, LEX nr 3068097.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 września 2020 r., VI SA/Wa 2151/19, LEX nr 3084055.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 14 stycznia 2021 r., VI SA/Wa 2293/20, LEX nr 3161783.
Zdrodowski B., *Istota bezpieczeństwa państwa,* „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate", 2019, nr 3.
Zięba-Załucka H., *Konstytucyjne aspekty bezpieczeństwa*, „Studia Iuridica Lublinensia", 2014, t. XXII.

Entities of the national cybersecurity system

Abstract

The subject of this study is to formulate an answer to the question of whether distinguishing specific entities within the national cybersecurity system and entrusting them with specific tasks in this area is within the implementation of the principle of ensuring security. This is a protected value, and its implementation is addressed to public authorities. For this reason, entities included in the national cybersecurity system should be viewed from the perspective of fulfilling this obligation. The research problem is current not only due to the increasingly frequent phenomena of cyber threats and cyberattacks, but also due to the currently processed amendment to the Act on the National Cybersecurity System, the purpose of which is, among others, to adapt it to the provisions of EU law.

Keywords: Constitution, security, cybersecurity, national cybersecurity system, entities of the national cybersecurity system