Przegląd Prawa Konstytucyjnego
-----ISSN 2082-1212-----
DOI 10.15804/ppk.2021.02.20
-----Nr 2 (60)/2021-----

Marzena Toumi[1]

Zmiany w strukturze centralnej administracji publicznej w świetle ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo, prawo
Keywords: cybersecurity, security, law

Streszczenie

Na bezpieczeństwo narodowe Polski w XXI w. duży wpływ wywierają procesy zachodzące we współczesnym, globalnym środowisku bezpieczeństwa. Cechują się one dużą dynamiką i złożonością zmian oraz występowaniem zagrożeń asymetrycznych, wśród których do najgroźniejszych należy zaliczyć zagrożenia w cyberprzestrzeni. Funkcjonowanie państwa i realizacja przez nie obowiązków konstytucyjnych w coraz większym stopniu uzależnione jest od rozwoju nowoczesnych technologii, społeczeństwa informacyjnego oraz niezakłóconego funkcjonowania cyberprzestrzeni. Szybki postęp w dziedzinie technologii cyfrowych powoduje konieczność efektywnego wykorzystania najnowszych technologii, stwarzając jednocześnie państwu polskiemu możliwość wyjścia z roli wyłącznie użytkownika i dołączenie do grona krajów o efektywnie funkcjonującej gospodarce cyfrowej, dostarczających rozwiązania i współtworzących międzynarodowe standardy. Wyjściem naprzeciw tym oczekiwaniom było podpisanie przez Prezydenta RP w dniu 1 sierpnia 2018 r. ustawy o krajowym systemie cyberbezpieczeństwa, implementującą do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[1] ORCID ID: 0000-0003-3838-1315, doktor habilitowany, Katedra Historii i Teorii Prawa, Instytut Prawa, Akademia Sztuki Wojennej w Warszawie. E-mail: m.toumi@akademia.mil.pl.

Abstract

Changes in the Structure of the Central Public Administration in the Light of the Act on the National Cybersecurity System of 2018

The national security of Poland in the 21st century is strongly influenced by the processes taking place in the contemporary global security environment. They are characterized by high dynamics and complexity of changes as well as the occurrence of asymmetrical threats, among which the most dangerous are threats in cyberspace. The functioning of the state and the implementation of their constitutional obligations are increasingly dependent on the development of modern technologies, the information society and the smooth functioning of cyberspace, which is largely dependent on the security of the ICT infrastructure enabling the use of cyberspace, information resources and services accumulated therein. thanks to it they function. Rapid progress in the field of digital technologies necessitates the effective use of the latest technologies while creating the opportunity for the Polish state to leave the role of only the user and join the group of countries with an effectively functioning digital economy, providing solutions and co-creating international standards. To meet these expectations, the President of the Republic of Poland signed the Act on the national cybersecurity system on 1 August 2018, implementing the Directive of the European Parliament and the Council (EU) into the Polish legal order regarding measures for a high common level of security of network and information systems in the territory of Union (Directive 2016/1148) – (the so-called NIS Directive).

*

Władza państwowa jest typem władzy uniwersalnej, ogólnospołecznej, obejmującej ludzi zamieszkujących określone terytorium. Jest sprawowana przez specjalny aparat, wyodrębniony od ogółu ludności. Powinna spełniać cztery podstawowe funkcje: integracyjną, dystrybucyjną, zapewnienia bezpieczeństwa oraz strukturotwórczą. W niniejszym artykule w sferze zainteresowań pozostaje przede wszystkim trzecia z ww. funkcji.

System bezpieczeństwa narodowego tworzą wszystkie odpowiedzialne za bezpieczeństwo w świetle Konstytucji RP i właściwych ustaw organy oraz instytucje należące do władzy ustawodawczej, wykonawczej i sądowniczej, w tym Parlament, Prezydent RP, Prezes Rady Ministrów, Rada

Ministrów, centralne organy administracji rządowej oraz inne państwowe urzędy centralne i instytucje państwowe. Strategia Bezpieczeństwa określa kompleksową wizję kształtowania bezpieczeństwa narodowego we wszystkich jego wymiarach[2].

Funkcjonowanie państwa i realizacja przez nie obowiązków konstytucyjnych w coraz większym stopniu uzależnione jest od rozwoju nowoczesnych technologii[3], społeczeństwa informacyjnego oraz niezakłóconego funkcjonowania cyberprzestrzeni, rozumianej jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Cyberprzestrzeń RP stanowi cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)[5].

Zgodnie z postanowieniami zawartymi w strategicznym dokumencie rządowym Strategia na rzecz odpowiedzialnego rozwoju, przyjętym przez Radę Ministrów w 2017 r., e-administracja została wskazana jako jeden z warunków sprawnego państwa[6]. Jednym z kluczowych czynników zapewnienia transparentności i skuteczności działań realizowanych przez administrację publiczną jest wykorzystanie technologii cyfrowych[7].

Mimo wszystkich swoich zalet, cyfryzacja niesie ze sobą również ryzyko znacznie większej podatności na ataki cyberprzestępców, a każde znaczące

---

[2] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, s. 5.

[3] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 318–338. Patrz również: M. Borkowski, *Cyberprzestrzeń a bezpieczeństwo jednostki*, Warszawa 2013, s. 112–134.

[4] Dz.U. 2005, Nr 64, poz. 565, ze zm.

[5] Przestrzeń wirtualna zaczyna być również traktowana jak terytorium danego państwa. *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, dokument przyjęty przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego, Warszawa 2013, s. 5.

[6] *Strategia na rzecz odpowiedzialnego rozwoju*, Rada Ministrów, Warszawa 2017, s. 226.

[7] Patrz: K. Śledziewska, A. Levai, D. Zięba, *Use of e-government in Poland in comparison to other European Union member states*, „Information Systems in Management" 2016, nr 5 (1), s. 119–130.

zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, ma wpływ na ogólnie pojmowane bezpieczeństwo narodowe[8] – kwestie bezpieczeństwa informacyjnego stały się są elementem prawa bezpieczeństwa narodowego[9].

W Rzeczpospolitej Polskiej zadania z zakresu bezpieczeństwa cyberprzestrzeni realizowane są przez władzę publiczną (ustawodawczą, wykonawczą i sądowniczą) oraz podległe jej organy administracyjne. Istotną rolą władzy ustawodawczej (Sejmu i Senatu) w zakresie cyberbezpieczeństwa jest prawodawstwo i określanie zasadniczych kierunków działalności państwa[10]. Do władzy sądowniczej należy sprawowanie wymiaru sprawiedliwości w sprawach karnych, dotyczących często ogólnie pojętego bezpieczeństwa narodowego, a także jego transsektorowego obszaru, czyli bezpieczeństwa cyberbprzestrzeni, obwarowanego normami wyznaczającymi reguły postępowania[11]. Jednak kluczowa rola w tej materii przypada władzy wykonawczej. Rada Ministrów, stojąca na czele administracji rządowej, przez wykonywanie zadań na rzecz ochrony cyberprzestrzeni realizuje swoje konstytucyjne obowiązki i to ona głównie ponosi odpowiedzialność za zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli[12].

Dnia 1 sierpnia 2018 r. Prezydent RP podpisał ustawę o krajowym systemie cyberbezpieczeństwa[13], implementującą do polskiego porządku prawnego tzw. Dyrektywę NIS[14]. Pełne jej wdrożenie wymagało przyjęcia

---

[8] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, s. 4.

[9] Por. M.A. Kamiński, *Prawo bezpieczeństwa narodowego*, „Wiedza Obronna" 2019, nr 3, t. 268, s. 57–76; M.A. Kamiński, *Military Law in the Republic of Poland*, „Safety& Defense" 2019, nr 2, t. 5, s. 28–34.

[10] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011, s. 76–77.

[11] K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, s. 360–361. Zob. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

[12] K. Chałubińska-Jentkiewicz, op.cit., s. 353.

[13] Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560).

[14] Dyrektywa 2016/1148 Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz.UE L 194/1 z 19 lipca 2016 r.).

dwóch rozporządzeń Rady Ministrów: w sprawie uznania incydentu za poważny[15], jak i w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[16]. Stworzony w ten sposób krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w szczególności niezakłóconego świadczenia usług kluczowych i usług cyfrowych przez osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[17].

System ten obejmuje operatorów usług kluczowych[18], dostawców usług cyfrowych, zespoły CSIRT (Zespół ds. Bezpieczeństwa i Reagowania na Incydenty Komputerowe)[19] poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa oraz pojedynczy punkt kon-

---

[15] Rozporządzenie Rady Ministrów z 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz.U. poz. 2180).

[16] Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. poz. 1806).

[17] Art. 3. Ustawy o krajowym systemie cyberbezpieczeństwa. Przy czym cebrbezpieczeństwo zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, rozumiane jest jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. *Wprowadzenie,* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* red. K. Czaplicki, A. Gryszczyńska, G. Szpor, P. Dronek, K. Prusak-Górniak, K. Silicki, K. Świtała, B. Szafrański, M. Wilbrandt-Gotowicz, Warszawa 2019.

[18] Operatorzy usług kluczowych to firmy i instytucje świadczące usługi w jednym z sześciu obszarów krytycznych z punktu widzenia gospodarki państwa: energii, transporcie, bankowości, ochronie zdrowia, zaopatrzenia w wodę pitną (wraz z jej dystrybucją) oraz infrastruktury cyfrowej. Wykaz operatorów usług kluczowych prowadzi minister właściwy do spraw informatyzacji. Wpisanie i wykreślenie operatora z listy odbywa się na wniosek organu właściwego do spraw cyberbezpieczeństwa, patrz szerzej: F. Radoniewicz, *Art. 4 (Zakres podmiotowy),* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* red. W. Kitler, J. Taczkowska-Olszewska i F. Radoniewicz, Warszawa 2019, s. 55, P. Dawidziak, B. Łęcki, M.P. Stolarski, *Sieć Internet – znaczenie dla nowoczesnego państwaoraz problemy bezpieczeństwa,* [w:] *Bezpieczeństwo teleinformatyczne państwa,* red. M. Madej, M. Terlikowski, Warszawa 2009, s. 55–56.

[19] Z ang.: *Computer Security Incident Response Team*.

taktowy do komunikacji w ramach współpracy w Unii Europejskiej w dziedzinie spraw cyberbezpieczeństwa.

Ustawa wyznaczyła trzy CSIRT poziomu krajowego: CSIRT NASK (prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie), CSIRT GOV (w strukturach Agencji Bezpieczeństwa Wewnętrznego) oraz CSIRT MON (w strukturach resortu obrony narodowej). Każdy CSIRT poziomu krajowego ma jasno określone constituency – zakres podmiotów, które zobowiązane są raportować i którym świadczy on wsparcie.

CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz przedsiębiorstwa o szczególnym znaczeniu gospodarczo–obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej[20].

CSIRT GOV[21] koordynuje incydenty zgłaszane przez administrację rządową, jednostki sektora finansów publicznych, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej[22].

CSIRT NASK koordynuje incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych (niebędących operatorami in-

[20] Zob. CSIRT Ministerstwa Obrony Narodowej, https://csirt-mon.wp.mil.pl/pl/pages/zadania-2017-01-16-4 (20.04.2020).

[21] Działający od stycznia 2008 r. w ramach Agencji Bezpieczeństwa Wewnętrznego jako CERT.GOV.PL.

[22] Zgodnie z ustawami: z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. Nr 89 poz. 590, ze zm.) oraz z 27 sierpnia 2009 r. o finansach publicznych (Dz.U. Nr 157 poz. 1240 ze zm.). Do CSIRT GOV należy przede wszystkim rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, patrz: Cyfryzacja KPRM, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt (20.04.2020).

frastruktury krytycznej), dostawców usług cyfrowych, samorząd terytorialny. Można powiedzieć, że CSIRT NASK stanowi również tzw. cert ostatniej szansy (CERT of last resort)[23], bowiem mogą zgłaszać do niego incydenty także osoby fizyczne (bez względu na obywatelstwo lub jego brak) i jednostki organizacyjne (bez względu na siedzibę), dla których nie są właściwe pozostałe CSIRT-y.

Ponadto w przypadku incydentów o charakterze terrorystycznym właściwe są CSIRT MIL i CSIRT GOV (zgodnie z przepisami ustawy o działaniach antyterrorystycznych i ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego)[24]. W przypadku incydentów związanych z obronnością kraju zawsze właściwy jest CSIRT MON.

Podstawowym założeniem ustawy jest ścisła współpraca CSIRT poziomu krajowego, zarówno ze sobą jak i z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym ds. informatyzacji oraz Pełnomocnikiem ds. Cyberbezpieczeństwa, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów (art. 26, pkt 1).

Kolejnym ważnym elementem, który wprowadza ustawa w zakresie cyberbezpieczeństwa jest możliwość wykonywania przez zespoły CSIRT badań urządzeń lub oprogramowania w celu identyfikacji podatności na zagrożenia oraz składanie rekomendacji w celu ich usunięcia[25].

Również operatorzy usług kluczowych są zobowiązani do wdrożenia skutecznych zabezpieczeń, szacowania ryzyka związanego z cyberbezpieczeństwem oraz przekazywania informacji o poważnych incydentach oraz ich obsługi we współpracy z CSIRT poziomu krajowego. Wymienione podmioty są również zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbez-

[23] Deployment of Baseline Capabilities of National/Governmental CERTs, ENISA – http://www.enisa.europa.eu; także: C. Banasiński, W. Nowak, *Europejski i krajowy system cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, s. 149–160.

[24] Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. poz. 904); ustawa z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. Nr 104 poz. 709).

[25] Cyfryzacja KPRM…, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt (20.04.2020).

pieczeństwo świadczonych usług, obsługi i zgłaszania incydentów oraz udostępniania wiedzy na temat cyberbezpieczeństwa.

Do krajowego systemu cyberbezpieczeństwa zostały również włączone organy administracji publicznej, a także przedsiębiorcy telekomunikacyjni. Wymaganiami z zakresu cyberbezpieczeństwa zostali objęci dostawcy usług cyfrowych (internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe). Z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych są objęte zharmonizowanym na poziomie UE reżimem regulacyjnym (a ustawa odwołuje się tutaj do decyzji wykonawczej Komisji Europejskiej).

Ponadto w skład krajowego systemu cyberbezpieczeństwa wchodzą podmioty publiczne tj.: Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, a także instytuty badawcze i spółki prawa handlowego, wykonujące zadania o charakterze użyteczności publicznej.

Zgodnie z art. 21 ustawy o krajowym systemie cyberbezpieczeństwa każdy z powyższych podmiotów ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych[26].

Dodatkowo na każdym z podmiotów publicznych spoczywa obowiązek zarządzania incydentem w podmiocie publicznym, w tym zapewnienia jego obsługi. Czas na zgłoszenie poważnego incydentu do właściwego CSIRT nie może przekroczyć 24 godzin od momentu wykrycia (art. 11, pkt 4). Taka decyzja musi być wcześniej skonsultowana z operatorem usługi kluczowej lub dostawcą usługi cyfrowej, który zgłosił incydent.

CSIRT MON, CSIRT NASK lub CSIRT GOV za pośrednictwem Pojedynczego Punktu Kontaktowego informuje inne państwa członkowskie Unii Eu-

[26] „Włączenie tak dużej liczby podmiotów publicznych pod reżim ustawy wynika z chęci zbudowania kompleksowego i systemowego podejścia do krajowego systemu cyberbezpieczeństwa, a nie samej implementacji dyrektywy NIS", za: *Art. 21 Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami* krajowego systemu cyberbezpieczeństwa, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa…*

ropejskiej w przypadku, gdy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej (art. 29).

Ustawa wprowadza również formułę Zespołu ds. Incydentów Krytycznych, będącego organem pomocniczym w sprawach obsługi incydentów krytycznych, w skład którego wchodzą CSIRT poziomu krajowego oraz Rządowe Centrum Bezpieczeństwa jako sekretariat, co zapewnia współpracę z Rządowym Zespołem Zarządzania Kryzysowego. Do udziału w pracach zespołu mogą być również zaproszeni przedstawiciele organów właściwych[27].

Zgodnie z ustawą informacje o podatnościach, incydentach i ryzyku ich wystąpienia oraz zagrożeniach cyberbezpieczeństwa nie podlegają ustawie o dostępie do informacji publicznej[28], nie mniej jednak właściwy CSIRT MON, CSIRT NASK i CSIRT GOV mogą publikować takie informacje (w niezbędnym zakresie), na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów. Publikowane informacje nie mogą jednak naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych (art. 35, pkt 5).

Nadzór nad każdym z kluczowych sektorów gospodarki sprawuje organ właściwy ds. cyberbezpieczeństwa. Organami właściwymi do spraw cyberbezpieczeństwa są ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym, co w praktyce oznacza, że regulatorzy sektorowi (jeśli istnieją) mogą realizować te funkcje zamiast ministra właściwego.

Zadaniem organu właściwego ds. cyberbezpieczeństwa jest analiza podmiotów funkcjonujących w danym sektorze i wydawanie decyzji o uznaniu za operatora usługi kluczowej. Poza tym organ właściwy przygotowuje

---

[27] Ustawa o krajowym systemie cyberbezpieczeństwa, https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa (10.01.2020).

[28] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112 poz. 1198, ze zm.).

także rekomendacje działań, które wzmocnią cyberbezpieczeństwo sektora. Do obowiązków organu należy również wzywanie podmiotu do usunięcia podatności, które mogą lub mogły doprowadzić do poważnego incydentu, prowadzenie kontroli operatorów usług kluczowych, współpraca z innymi państwami UE za pośrednictwem Pojedynczego Punktu Kontaktowego, udział w ćwiczeniach oraz przetwarzanie danych osobowych niezbędnych do realizacji zadań[29].

Organy właściwe do spraw cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych (art. 42, p. 7).

Cywilne aspekty cyberbezpieczeństwa RP pozostały w gestii Ministra właściwego ds. informatyzacji. Do jego zadań, we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa oraz innymi ministrami, należy m.in. opracowanie Strategii Cyberbezpieczeństwa[30], prowadzenie polityki informacyjnej na temat krajowego systemu cyberbezpieczeństwa, realizacja obowiązków sprawozdawczych wobec instytucji unijnych oraz uruchomienie z dniem 1 stycznia 2021 r. systemu teleinformatycznego, umożliwiającego zautomatyzowane zgłaszanie i obsługę incydentów, szacowanie ryzyka teleinformatycznego, ostrzeganie o zagrożeniach cyberbezpieczeństwa, rekomendowanie obszarów współpracy z sektorem prywatnym, prowadzenie działań informacyjnych na temat dobrych praktyk, programów edukacyjnych, kampanii i szkoleń z poszerzania wiedzy oraz budowania świadomości w zakresie cyberbezpieczeństwa. Minister prowadzi także Pojedynczy Punkt Kontaktowy. PPK od-

[29] *Ustawa o krajowym systemie cyberbezpieczeństwa*, https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa (10.01.2020).

[30] Strategia Bezpieczeństwa określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, które pozwolą osiągnąć i utrzymać wysoki poziom cyberbezpieczeństwa. Strategia uwzględnia również priorytety, podmioty zaangażowane w jej wdrażanie oraz działania odnoszące się do programów edukacyjnych, informacyjnych oraz planów badawczo-rozwojowych. Przyjmowana jest uchwałą Rady Ministrów. Dnia 22 października 2019 r. Rada Ministrów przyjęła uchwałę w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. 2019, poz. 1037). Dokument obowiązuje od 31 października 2019 r. i zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Za wypełnienie postanowień dokumentu odpowiada minister właściwy ds. informatyzacji, we współpracy z pozostałymi Członkami Rady Ministrów, który do 30 marca każdego roku przedstawia informację o realizacji Strategii Cyberbezpieczeństwa.

powiada za współpracę z Komisją Europejską i przekazywanie corocznych raportów, współpracuje z innymi państwami członkowskimi w zakresie cyberbezpieczeństwa oraz koordynuje współpracę pomiędzy organami właściwymi w kraju (art. 45–50).

Do głównych zadań Ministra Obrony Narodowej należy prowadzenie międzynarodowej współpracy Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami NATO, UE i innych organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa. Minister Obrony Narodowej jest także odpowiedzialny za zapewnienie zdolności Siłom Zbrojnym RP w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych; rozwijanie umiejętności Sił Zbrojnych RP w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych, pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP; ocenę wpływu incydentów na system obrony państwa a także kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego (art. 51–52).

Ponieważ tematyka cyberbezpieczeństwa jest horyzontalna – dotyczy wielu ministerstw i agencji rządowych, ustawa wprowadza Kolegium ds. Cyberbezpieczeństwa i Pełnomocnika ds. Cyberbezpieczeństwa w celu koordynacji polityki w skali państwa. Pełnomocnik prowadzi współpracę międzynarodową, wspiera badania naukowe i rozwój technologii z zakresu cyberbezpieczeństwa, a także działa na rzecz podnoszenia świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu. Do niego należy również analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa; nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa oraz wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

Pełnomocnik jest powoływany i dowoływany przez Prezesa Rady Ministrów w randze sekretarza lub podsekretarza stanu i podlega Radzie Ministrów (art. 60–63).

Kolegium ds. Cyberbezpieczeństwa jest organem opiniodawczo-doradczym Rady Ministrów w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa (art. 64). Przewodniczy mu Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa Narodowego oraz minister odpowiedzialny za koordynację działalności służb specjalnych. W posiedzeniach kolegium uczestniczą dodatkowo 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 (art. 66). Zakres kompetencji Kolegium do spraw cyberbezpieczeństwa został wskazany w art. 65 ustawy.

Wdrożenie ustawy o krajowym systemie cyberbezpieczeństwa to wyzwanie zarówno dla administracji, jak i sektora prywatnego. Ogromnym wyzwaniem organizacyjnym jakie nakłada ustawa jest również zbudowanie sprawnie funkcjonującego systemu w poszczególnych sektorach (co jest związane z ustanowieniem sektorowych zespołów cyberbezpieczeństwa oraz zmianami prawnymi w prawie sektorowym). Organy właściwe muszą przede wszystkim zbudować kompetencje w zakresie nadzoru nad cyberbezpieczeństwem. Dużą zmianą dla sektora prywatnego jest obowiązek raportowania incydentów[31], która jednocześnie staje się wyzwaniem dla administracji w zakresie opracowania konkretnych narzędzi – systemu teleinformatycznego, który w założeniu będzie wspierać krajowy system cyberbezpieczeństwa. Kluczowa dla bezpieczeństwa funkcjonowania struktur władzy państwowej będzie realizacja tych zadań w praktyce.

*

[31] W polskim porządku prawnym jest to nowość, ponieważ dotychczas – poza sektorem telekomunikacyjnym – nie było obowiązku zgłaszania incydentów.

Błyskawiczny rozwój Internetu oraz ekspansja technologii informacyjno-komunikacyjnych spowodowały m.in. globalizację zjawisk gospodarczych, społecznych i politycznych.

Funkcjonowanie państwa i realizacja przez nie obowiązków konstytucyjnych w coraz większym stopniu uzależnione jest od rozwoju nowoczesnych technologii, społeczeństwa informacyjnego oraz niezakłóconego funkcjonowania cyberprzestrzeni, które w dużej mierze zależne jest od bezpieczeństwa infrastruktury teleinformatycznej umożliwiającej korzystanie z cyberprzestrzeni, zgromadzonych w niej zasobów informacyjnych i usług, które dzięki niej funkcjonują. Ważnym zadaniem dla państwa powinno być stałe kształcenie i podnoszenie świadomości urzędników administracji publicznej z kwestii związanych z bezpieczeństwem cyberprzestrzeni, zwłaszcza w zakresie odpowiedniej i skutecznej ochrony. Szczególną uwagę powinno zwrócić się na edukację w tej kwestii osób odpowiedzialnych za zamówienia publiczne w urzędach i instytucjach publicznych. Docelowo zamawiający urządzenia i usługi, które narażone są na potencjalne cyberataki, powinni dokonywać wyborów takich rozwiązań, które gwarantują bezpieczeństwo cyfrowe.

Wyniki kontroli w zakresie zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego przeprowadzonej przez NIK w 2018 r. wykazały brak dostatecznej świadomości wśród osób pełniących funkcję organu w Krajowym Systemie Cyberbezpieczeństwa, jak istotna jest tematyka bezpieczeństwa informacji. Wykazano także brak środków finansowych, aby realizować niezbędne przedsięwzięcia oraz niedostateczną liczbę fachowców z zakresu bezpieczeństwa informacji – i to są najważniejsze zadania dla władzy państwowej.

Ustawa o krajowym systemie cyberbezpieczeństwa w zakresie swojej regulacji wdrożyła dyrektywę Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Jej głównym celem było utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym, w szczególności niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług. Czy cel ten został osiągnięty?

Bezpieczeństwo w cyberprzestrzeni to najnowsza i współcześnie najbardziej wymagająca dziedzina bezpieczeństwa narodowego, łącząca wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny. Zapewnianie cyberbezpieczeństwa w Polsce i budowanie odpornego na zagrożenia systemu to nieustanny proces. Warto zauważyć, że staje się on coraz bardziej świadomy i zaplanowany, mimo pojawiających się nowych wyzwań i trudności. Również Strategia Bezpieczeństwa Narodowego z 2020 r. kładzie zdecydowany nacisk na podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji poprzez: „zwiększanie poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnie zdolności do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia; wzmacnianie defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa; uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni; rozwój krajowej zdolności w obszarze testowania, badań, oceny i certyfkacji rozwiązań i usług z obszaru cyberbezpieczeństwa; rozwijanie kompetencje, wiedzy oraz świadomości zagrożeń i wyzwań zarówno wśród kadr administracji publicznej jak i w społeczeństwie – w obszarze cyberbezpieczeństwa; wzmacnianie i rozbudowywanie potencjału państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie fnansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego”[32].

Literatura

Banasiński C., Nowak W., *Europejski i krajowy system cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.

[32] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej…*, s. 20.

Borkowski M., *Cyberprzestrzeń a bezpieczeństwo jednostki*, Warszawa 2013.
Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.
Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań, Raport przygotowany przez: Cyfrowa Polska, Warszawa 2019.
Dawidziak P., Łęcki B., Stolarski M.P., *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
Kamiński M.A., *Prawo bezpieczeństwa narodowego*, „Wiedza Obronna" 2019, nr 3, t. 268.
Kamiński M.A, *Military Law in the Republic of Poland*, „Safety& Defense" 2019, nr 2, t. 5.
Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011.
Suchorzewska A, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Śledziewska K., Levai A., Zięba D., *Use of e-government in Poland in comparison to other European Union member states*, „Information Systems in Management" 2016, nr 5 (1).
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. W. Kitler, J. Taczkowska-Olszewska i F. Radoniewicz, Warszawa 2019.