Studia Bezpieczeństwa Narodowego
Zeszyt 22 (2021)
ISSN 1508-5430, s. 79-98
DOI:

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 22 (2021)
ISSN 1508-5430, pp. 79-98
DOI:

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

BEZPIECZEŃSTWO CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ

CYBERSPACE SECURITY OF REPUBLIC OF POLAD

Grzegorz Mąkosa[1]
ORCID: 0000-0003-4232-1251
Wojskowa Akademia Techniczna

Abstrakt. **Artykuł przedstawia cyberprzestrzeń i jej bezpieczeństwo, jako jedno z najistotniejszych zadań** i wyzwań państw i organizacji je zrzeszających. Przedstawione zostały definicje i pojęcia związane z problematyką cyberbezpieczeństwa. Cyberbezpieczeństwo jest jednym z najistotniejszych i coraz istotniejszym komponentem bezpieczeństwa narodowego. Cyberbezpieczeństwo państwa obejmuje bezpieczeństwo systemów teleinformatycznych oraz danych w nich przetwarzanych, stosowanych w przestrzeni cyfrowej, tak przez administrację, podmioty publiczne i gospodarcze, jak i przez obywateli. Cyberprzestrzeń jest obszarem działań konfrontacyjnych nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi. Artykuł porusza kwestie odpowiedzialności za zapewnienie cyberbezpieczeństwa systemów teleinformatycznych kluczowych krajowych podmiotów, organizacji i instytucji oraz jego wpływu na rozwój działalności państw. Wskazana została odpowiedzialność poszczególnych państw za zapewnienie bezpieczeństwa swojej cyberprzestrzeni. Zapewnienie bezpieczeństwa kraju w cyberprzestrzeni, w tym bezpieczeństwa jego cyberprzestrzeni, to

[1] Grzegorz Mąkosa – doktorant w dziedzinie nauk społecznych w dyscyplinie nauk o bezpieczeństwie na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej. Posiada wieloletnie doświadczenie zawodowe związane z systemami zarządzania ISO - jakością, systemami i usługami IT, bezpieczeństwem informacji oraz ochroną danych osobowych, jako audytor i konsultant systemów zarządzania ISO przeprowadził wiele audytów i projektów wdrożeniowych w ww. zakresie, pełnił również m.in. funkcje administratora bezpieczeństwa informacji i inspektora ochrony danych, zajmował stanowiska menedżerskie i eksperckie w podmiotach gospodarczych i budżetowych.

jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Cyberbezpieczeństwo powinno być realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Artykuł prezentuje międzynarodowy (europejski) i krajowy kontekst prawny cyberbezpieczeństwa poprzez wskazanie właściwych w tym zakresie regulacji prawnych, takich jak dyrektywy unijne oraz ustawy i rozporządzenia krajowe, i dokumentów strategicznych – takich jak strategie bezpieczeństwa i cyberbezpieczeństwa, tak Unii Europejskiej, jak i Polski. Zaprezentowano także stan bezpieczeństwa cyberprzestrzeni RP w ujęciu ilości i rodzajów incydentów i zdarzeń bezpieczeństwa, stanu podatności systemów teleinformatycznych instytucji państwowych i podmiotów gospodarczych. Przegląd oparty jest na analizie i syntezie informacji przedstawionych w corocznych raportach CSIRT GOV i CSIRT NASK, odpowiedzialnych za bezpieczeństwo najważniejszych, z perspektywy bezpieczeństwa państwa, systemów teleinformatycznych w Polsce.
Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, system teleinformatyczny, zagrożenia cyberbezpieczeństwa, incydenty cyberbezpieczeństwa
Abstract. The article presents cyberspace and its security as one of the most important tasks and challenges of states and organizations associating them. Definitions and concepts related to cybersecurity are presented. Cybersecurity is one of the most important and increasingly important components of national security. State cybersecurity covers the security of ICT systems and the data processed in them, used in the digital space, both by the administration, public and economic entities, and by citizens. Cyberspace is an area of confrontation not only with other countries, but also with hostile organizations, such as extremist and terrorist groups or organized crime groups. The article addresses the issues of responsibility for ensuring the cybersecurity of ICT systems of key national entities, organizations and institutions and its impact on the development of states' activities. The responsibility of individual countries for ensuring the security of their cyberspace was indicated. Ensuring the security of the country in cyberspace, including the security of its cyberspace, is one of the basic tasks in the field of state security. Cybersecurity should be implemented both through the development of defensive capabilities (including the protection of entities operating in cyberspace and the cyberspace itself) and offensive. The article presents the international (European) and national legal context of cybersecurity by indicating the relevant legal regulations, such as EU directives and national laws and regulations, and strategic documents - such as security and cybersecurity strategies, both for the European Union and Poland. The state of cyberspace security of the Republic of Poland was also presented in terms of the number and types of security incidents and events, and the state of vulnerability of ICT systems of state institutions and business entities. The review is based on the analysis and synthesis of information presented in the annual CSIRT GOV and CSIRT NASK reports, responsible for the security of the most important, from the national security perspective, ICT systems in Poland.
Keywords: cyberspace, cybersecurity, ICT system, cybersecurity threats, cybersecurity incidents

Wprowadzenie

Właściwością i odpowiedzialnością państwa jest zapewnienie bezpieczeństwa cyberprzestrzeni RP. Cyberbezpieczeństwo państwa obejmuje bezpieczeństwo systemów teleinformatycznych oraz danych w nich przetwarzanych, stosowanych w przestrzeni cyfrowej, tak przez administrację, podmioty publiczne i gospodarcze, jak i przez obywateli (Mąkosa 2019, s. 231). Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi stanowią cyberprzestrzeń. W cyberprzestrzeni realizowane są usługi cyfrowe społeczeństwa informacyjnego, podmiotów gospodarczych i innych organizacji, usługi administracji publicznej i podmiotów realizujących zadania publiczne. Równolegle do realizowanych działań o charakterze rozwojowym w cyberprzestrzeni realizowane są szkodliwe działania i działalność przestępcza,

wywołująca ogromne szkody procesowe, finansowe, społeczne, w tym ograniczenie wzajemnego zaufania (Mąkosa 2020a, s. 123). Bezpieczeństwo cyberprzestrzeni RP zapewniają organy państwa na podstawie unijnych i polskich regulacji prawnych, dokumentów strategicznych i standardów branżowych. Powołane zostały specjalistyczne jednostki do monitorowania i reagowania na zdarzenia i incydenty bezpieczeństwa w cyberprzestrzeni RP oraz oceny stanu bezpieczeństwa systemów teleinformatycznych kluczowych polskich podmiotów i instytucji.

Bezpieczeństwo polskiej cyberprzestrzeni

Cyberbezpieczeństwo jest coraz istotniejszym elementem składowym bezpieczeństwa narodowego i międzynarodowego, a zapewnienie jego odpowiednio wysokiego poziomu jest kluczowym wyzwaniem stojącym przed państwami (Mąkosa 2020b, s. 111). Cyberbezpieczeństwo odnosi się do bezpiecznego funkcjonowania państwa, jego struktur administracyjnych, podmiotów gospodarczych i osób w cyberprzestrzeni. Zgodnie z ujęciem Doktryny cyberbezpieczeństwa RP, cyberprzestrzeń jest jednym z obszarów aktywności państwa, podmiotów prywatnych i obywateli. Cyberprzestrzeń jest przestrzenią konfliktu, w której kraje mierzą się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi (BBN 2015, s. 4).

Podstawowe pojęcia związane z cyberbezpieczeństwem i cyberprzestrzenią, zdefiniowane w Doktrynie cyberbezpieczeństwa RP, które wyznaczają kierunek i sposób myślenia o nich zostały przedstawione w tabeli 1.

Tabela 1. Definicje i pojęcia związane z cyberbezpieczeństwem

cyberprzestrzeń	przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami
cyberprzestrzeń RP	cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)
cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)	proces zapewniania 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

bezpieczeństwo cyberprzestrzeni RP	część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych

Źródło: Mąkosa G., *Krajowy System Cyberbezpieczeństwa RP* w: A. Chabasińska, A. Warchał (red.), Perspektywy bezpieczeństwa w teorii i praktyce, WAT, Warszawa 2019, s. 231

Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej - prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni, wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców, prowadzenie walki informacyjnej w cyberprzestrzeni, współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych (BBN 2014, s. 35). Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym (BBN 2015, s. 14).

Zapewnienie cyberbezpieczeństwa jest coraz istotniejszym i coraz trudniejszym zadaniem i wyzwaniem ze względu na dynamiczny rozwój technologii informatycznych, w tym technologii stosowanych do realizacji złośliwych i wrogich działań naruszających bezpieczeństwo cybernetyczne podmiotów, organizacji, instytucji i państw. Postęp w teleinformatyce sprawił, że cyberprzestrzeń nie tylko przyczynia się do rozwoju podmiotów państwowych i pozapaństwowych, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa. Rozwój technologii teleinformatycznych wpływa na rozwój negatywnych zjawisk w cyberprzestrzeni, tj. cyberprzestępczości, cyberkonfliktów, cyberwalki (walki informacyjnej), czy cyberwojny (Mąkosa 2020b, s. 117). Realizowane ataki na systemy teleinformatyczne są formą materializacji zagrożeń, których źródłami mogą być hakerzy, przestępcy komputerowi, terroryści, szpiedzy przemysłowi, czy specjalnie powoływane prywatne i państwowe grupy cyberprzestępcze. Działają oni z własnej motywacji lub

na zlecenie innych osób, podmiotów, czy nawet państw (Mąkosa 2020a, s. 124). Odpowiedzialność w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni spoczywa na poszczególnych państwach i, w ramach zapewnienia bezpieczeństwa regionalnego lub sojuszniczego, na organizacjach bezpieczeństwa zrzeszających te państwa, jak np. NATO, a także na związkach państwa, jak np. Unia Europejska, których członkiem jest Polska. Zapewnienie bezpieczeństwa cyberprzestrzeni jest aspektem technicznym, zależnym od technologii teleinformatycznych i telekomunikacyjnych i aspektem prawno-organizacyjnym, zależnym od regionalnych i krajowych przepisów regulacji prawnych.

Kontekst prawny i strategiczny bezpieczeństwa cyberprzestrzeni RP

Kwestie cyberbezpieczeństwa jako aspektu bezpieczeństwa narodowego, mającego coraz większy wpływ oraz coraz większy stopień dynamicznych zmian i skomplikowania technologicznego stanowią istotne wyzwanie nie tylko na poziomie poszczególnych krajów, ale także na poziomie związków państw, jak np. Unia Europejska.

Unia Europejska jako podmiot polityczny, tworzy regulacje prawne – dyrektywy i rozporządzenia – obowiązujące jej członków, również w zakresie cyberbezpieczeństwa i ochrony danych. Spośród regulacji unijnych warto wskazać na te bezpośrednio adresujące poruszane kwestie, tj.:

- 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 Akt o cyberbezpieczeństwie - 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 (Akt o cyberbezpieczeństwie), (Dyrektywa NIS);
- Strategia Cyberbezpieczeństwa UE (Budowanie odporności UE na ataki cybernetyczne, Kształtowanie skutecznej unijnej prewencji cybernetycznej, Wzmocnienie współpracy międzynarodowej w dziedzinie bezpieczeństwa cybernetycznego);
- Strategia bezpieczeństwa UE na lata 2020-2025 (EU Security Union Strategy) - adresująca również kwestie cyberbezpieczeństwa.

Polska, jako niezależny państwowy podmiot polityczny, tworzy, w ramach swojego systemu prawnego, rozwiązania strategiczne i prawne (legislacyjne), w tym również implementujące regulacje Unii Europejskiej. W ramach polskiego porządku prawnego i zarządzania strategicznego bezpieczeństwem narodowych zostały ustanowione stosowne dokumenty adresujące przedmiotową problematykę, tj.:

- Ustawa o krajowym systemie cyberbezpieczeństwa wraz z towarzyszącymi rozporządzeniami wykonawczymi,
- Strategia cyberbezpieczeństwa RP na lata 2019-24,
- Ustawa o zarządzaniu kryzysowym wraz z towarzyszącymi rozporządzeniami wykonawczymi,
- Narodowy Program Ochrony Infrastruktury Krytycznej,
- Strategia Bezpieczeństwa Narodowego RP,
- Biała Księga Bezpieczeństwa narodowego RP,
- Doktryna Cyberbezpieczeństwa RP.

W szczególny sposób kwestie cyberbezpieczeństwa na poziomie operacyjnym są przedmiotem ustawy o zarządzaniu kryzysowym, ustawy o krajowym systemie cyberbezpieczeństwa i ustawy o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącymi im aktami wykonawczymi i pomocniczymi (rozporządzeniami i dokumentami powstałymi na ich mocy). Regulacje prawne definiują zagadnienia cyberbezpieczeństwa, podmioty zaangażowane oraz ich odpowiedzialność, przedmiot zainteresowania danej regulacji oraz aspekty organizacyjne funkcjonowania systemu cyberbezpieczeństwa (Mąkosa 2020b, s. 109). Charakterystyka regulacji prawnych dotyczących cyberbezpieczeństwa przedstawiona jest w tabeli 2 poniżej.

Tabela 2. Charakterystyka regulacji prawnych dotyczących cyberbezpieczeństwa

Domena, podmiot, przedmiot regulacji	**Nazwa regulacji i dokumentów towarzyszących**
Zarządzanie kryzysowe Podmiot – operatorzy infrastruktury krytycznej Przedmiot – infrastruktura krytyczna, usługi kluczowe IK	• Ustawa o zarządzaniu kryzysowym, • Rozp. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej • Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) • Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje
Krajowy system cyberbezpieczeństwa Podmiot – operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty realizujące zadania publiczne Przedmiot – infrastruktura teleinformatyczna, usługi kluczowe, usługi cyfrowe	• Ustawa o krajowym systemie cyberbezpieczeństwa • Rozp. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo • Rozp. w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

Informatyzacja podmiotów publicznych Podmiot – podmioty realizujące zadania publiczne Przedmiot – systemy teleinformatyczne, rejestry publiczne	• Ustawa o informatyzacji podmiotów realizujących zadania publiczne, • Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Źródło: Mąkosa G., *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 109

W odniesieniu do zapisów ww. regulacji warto zwrócić uwagę na typy organizacji, które są ich podmiotami oraz na rodzaje systemów teleinformatycznych, będących przedmiotami poszczególnych regulacji. Szczegółowo systemy i sektory gospodarki, objęte wskazanymi przepisami zostały zaprezentowane w tabeli 3 poniżej.

Tabela 3. Systemy i sektory objęte regulacjami cyberbezpieczeństwa

Systemy infrastruktury krytycznej – ZK [Zarządzanie kryzysowe]		Sektor - KSC [Krajowy system cyberbezpieczeństwa]	Sektor – IPP [Informatyzacja podmiotów publicznych]
Teleinformatyczna Infrastruktura Krytyczna	Zaopatrzenia w energię, surowce energetyczne i paliwa	Energia	
	Łączności		
	Sieci teleinformatycznych		
	Finansowy	Bankowość i infrastruktury rynków finansowych	
	Zaopatrzenia w żywność		
	Zaopatrzenia w wodę	Zaopatrzenie w wodę	
	Ochrony zdrowia	Ochrona zdrowia	
	Transportowy	Transport	
	Ratowniczy		
	Zapewniający ciągłość działania administracji publicznej	Podmioty publiczne	Podmioty realizujące zadania publiczne
	Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych		
		Infrastruktura cyfrowa	

Źródło: Mąkosa G., *Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne*, [w:] Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Śmiałek K. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 110

Przepisy dotyczące zarządzania kryzysowego w najszerszym zakresie obejmują systemy bezpieczeństwa, natomiast regulacje ustawy o krajowym systemie cyberbezpieczeństwa w swoich sektorach zawarły znacznie mniejszą ilość ze strategicznie ważnych dla bezpieczeństwa narodowego gałęzi gospodarki i działalności komunalnej i publicznej. Jest to wynikiem bezpośredniej implementacji zapisów Dyrektywy NIS, której zapisy wskazały dokładnie te sektory. W projektowanej nowelizacji Dyrektywy NIS projektowane jest znaczne rozszerzenie listy sektorów, co po implementacji znacząco wpłynie na bezpieczeństwo całej Unii, jak i poszczególnych państw członkowskich.

Stan bezpieczeństwa cyberprzestrzeni RP

Regulacje ustawy o krajowym systemie cyberbezpieczeństwa[2] ustanowiły wyspecjalizowane, dedykowane do monitorowania bezpieczeństwa cyberprzestrzeni i adekwatnego reagowania na zdarzenia i incydenty jednostki CSIRT (ang. Computer Security Incident Responce Team). Wcześniej w Polsce funkcjonowały jednostki typu CERT (ang. Computer Emergency Responce Team), prowadzone przez NASK i ABW, które zmieniły status na CSIRT. Dodatkowo został powołany CSIRT sektora militarnego. Powstałe jednostki, to: CSIRT NASK (CERT Polska) - prowadzony przez NASK-PIB (Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy), CSIRT GOV - prowadzony przez Agencję Bezpieczeństwa Wewnętrznego, w której w kręgu zainteresowań są podmioty administracji rządowej i jednostki centralne oraz operatorzy infrastruktury krytycznej oraz CSIRT MON – prowadzony przez Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), dedykowana jednostkę w strukturach Wojska Polskiego.

Jednostki CSIRT GOV i CSIRT NASK corocznie opracowują raporty ze swojej działalności oraz prezentują stan bezpieczeństwa cyberprzestrzeni RP.

Jednostka CERT Polska (CSIRT NASK) publikuje corocznie raporty na temat stanu polskiego cyberbezpieczeństwa i informacje dotyczące obsłużonych przez nią incydentów bezpieczeństwa – „Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska". Zgodnie z przedstawionymi w raportach danymi od wielu lat obserwowany jest sukcesywny wzrost liczby incydentów. Zgodnie z danymi opublikowanymi w raportach z ostatnich lat, w roku 2020 CERT Polska obsłużył 34 555 zgłoszeń, które po przeanalizowaniu i pogrupowaniu wyodrębniły 10 420 incydentów, w roku 2019 – 22 343 zgłoszenia, z czego 6484 stanowiło incydenty, a w roku 2018 – 19 439 zgłoszeń, spośród których zarejestrowano 3739 incydentów. CERT Polska odnotował wzrost liczby obsłużonych incydentów na

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

poziomie 60,7% w porównaniu do roku 2019 i rekordowy wzrost liczby obsłużonych incydentów w roku 2019 na poziomie 73% w porównaniu do 2018 r. (NASK-PIB 2021, s. 24, 2020, s. 12, 2019, s. 10). Szczegółowe informacje o zgłoszeniach do i zidentyfikowanych przez CERT Polska incydentach w latach 2015-2020 zostały przedstawione w tabeli 4 poniżej.

Tabela 4. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2020 przez Cert Polska (CSIRT NASK)

Zgłoszenia / Rok	2020	2019	2018	2017	2016	2015
Liczba zgłoszeń	34 555	22 343	19 439			
Liczba incydentów	10 420	6 484	3 739	3 182	1 926	1 456

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2021, s. 24, 2020, s. 12, 2019, s. 10; Mąkosa G., *Bezpieczeństwo cybernetyczne systemów w czwartej rewolucji przemysłowej*, [w:] Czwarta rewolucja przemysłowa. Mity, paradygmaty i zastosowania. Tom 1 Kompetencje i baza narzędziowa Przemysłu 4.0, Wojciechowski Z., Zaskórski P. (red.), Wojskowa Akademia Techniczna, Warszawa 2020, s. 130

CERT Polska od roku 2018 prowadzi raportowanie w zakresie sektorów gospodarki, które były obiektami ataków. W roku 2019 została ustanowiona nowa kategoryzacja sektorów gospodarki, mająca na celu dokładne wskazanie kierunków i celów ataków cybernetycznych. Szczegółowy wykaz incydentów zidentyfikowanych w sektorach gospodarki w latach 2018-2020 został przedstawiony w tabeli 5.

Tabela 5. Incydenty obsłużone przez CERT Polska (CSIRT NASK) w latach 2018 -2020 r. wg sektorów gospodarki

	2020		**2019**		**2018**	
Sektor gospodarki	**Liczba incyd.**	**%**	**Liczba incyd.**	**%**	**Liczba incyd.**	**%**
Osoby fizyczne	959	9,20	1212	18,7		
Bankowość	1008	9,67	1057	16,3	643	17,2
Media	2568	24,64	748	11,5		
Handel hurt. i detal.	1437	13,79	624	9,6		
Infrastruktura cyfrowa	1016	9,75	550	8,5	29	0,78
Finanse	1283	12,31	500	7,7	62	1,66
Usługi inne	384	3,69	480	7,4		
Administr. publiczna	388	3,72	336	5,2	85	2,27
Oświata i wychowanie	71	0,68	62	1		
Transport	29	0,28	61	0,9	51	1,36
Służba zdrowia	112	1,07	53	0,8	13	0,35
Poczta i usługi kurier.	500	4,8	49	0,8		
Produkcja	57	0,55	46	0,7		

Sektor gospodarki	2020		2019		2018	
	Liczba incyd.	%	Liczba incyd.	%	Liczba incyd.	%
Budow. i gosp. nieruch.	29	0,28	31	0,5		
Energetyka	101	0,97	28	0,4	20	0,53
Logistyka i dystrybucja	27	0,26	19	0,3		
Kultura i ochrona dziedzictwa narodow.	7	0,07	9	0,1		
Hotele, restauracje, catering	19	0,18	9	0,1		
Turystyka	9	0,09	8	0,1		
Wodociągi	9	0,09	5	0,08	2	0,05
Działalność ubezpiecz.	2	0,2	5	0,08		
Kultura fizyczna	9	0,09	4	0,06		
Wyznania religijne i mniejszości narodowe	8	0,08	3	0,05		
Rolnictwo	4	0,04	3	0.05		
Gospodarka odpadami	1	0,01	2	0,03		
Rybołówstwo	1	0,01	2	0,03		
Izby gosp. i handlowe	3	0,03	0	0,0		
Inne	379	3,64	578	9	2834	75,8
Razem	10420	100	6484	100	3739	100

Źródło: Opracowanie własne na podstawie: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska,* NASK-PIB, 2021, s. 26, 2020, s. 14, 2019, s. 13

Zdefiniowany wykaz sektorów, dla których prowadzone są analizy i raportowanie nie pokrywa się wprost z sektorami i systemami bezpieczeństwa ustanowionymi w ramach regulacji zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, niemniej pozwala na zidentyfikowanie intensywności działań cyberprzestępczych nakierowanych na obszary wskazane w regulacjach.

Zespół CSIRT GOV (ABW) publikuje coroczny raport – „Raport o stanie bezpieczeństwa cyberprzestrzeni RP". Zgodnie z danymi przedstawionymi w raportach z ostatnich lat w roku 2020 Zespół CSIRT GOV odnotował 246107 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych, z czego jako incydenty zakwalifikowano 23 309 przypadków, wobec 226 914 zgłoszeń i 12 405 incydentów w roku 2019, 31 865 zgłoszeń i 6236 incydentów w roku 2018 i 28 281 zgłoszeń i 5819 incydentów w roku 2017 (ABW 2021, s. 9, 2020, s. 8-9, 2019, s. 11). Z analizy przedstawionych danych wynika, że liczba zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych i liczba zidentyfikowanych incydentów są dynamicznie rosnące. Dane na temat incydentów bezpieczeństwa obsłużonych przez specjalistów CSIRT GOV w ostatnich latach przedstawione zostały w tabeli 6.

Tabela 6. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2015-2020 przez CSIRT ABW

Zgłoszenia / Rok	**2020**	**2019**	**2018**	**2017**	**2016**	**2015**
Liczba zgłoszeń	246 107	226 914	31 865	28 281	19 954	16 123
Liczba incydentów	23 309	12 405	6 236	5 819	9 288	8 914

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, s. 9, 2020, s. 8-9, 2019, s. 11

CSIRT GOV od roku 2019 publikuje informacje o instytucjach, przeciwko którym zostały skierowane incydenty. Liczba zarejestrowanych incydentów w instytucjach przedstawiona jest w tabeli 7 poniżej.

Tabela 7. Liczba zarejestrowanych incydentów z podziałem na instytucje

Instytucje	**2020**	**2019**
Urzędy	8.356	3.837
Pozostałe	4.714	3.206
Infrastruktura krytyczna	2.626	685
Instytuty	2.518	-
Administracja publiczna	2.039	-
Ministerstwa	1.656	4.336
Służby i wojsko	1.400	341
Razem	*23.309*	*12.405*

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, s. 14, 2020, s. 10

Zaproponowana klasyfikacja instytucji nie pokrywa się wprost z sektorami i systemami bezpieczeństwa ustanowionymi w ramach regulacji zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa, jest znacznie węższa niż przedstawiona w raportowaniu CERT Polska i jednocześnie znacznie węższa niż wykaz sektorów i systemów powołany w regulacjach. Takie ujęcie informacji nie pozwala na zidentyfikowanie intensywności działań cyberprzestępczych nakierowanych na obszary wskazane w regulacjach, niemniej jednak choć w przybliżony, ogólny sposób umożliwia poznanie kierunków działań.

Obserwowana wysoka liczba zgłoszeń jest wynikiem przede wszystkim wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa, tym samym w latach 2019 - 2020 nastąpił zauważalny wzrost liczby zgłoszeń przesyłanych do CSIRT GOV w stosunku do wcześniejszych okresów sprawozdawczych. Jednocześnie, czynnikiem oddziaływującym na wskazaną tendencję, był wzrost liczby zgłoszeń rejestrowanych przez systemy wykrywania oraz ostrzegania przed zagrożeniami dotyczącymi systemów teleinformatycznych instytucji, podmiotów czy organów państwa znajdujących się w kompetencji Zespołu CSIRT GOV, co było podyktowane skalą cyberzagrożeń obecnych w cyberprzestrzeni RP (ABW 2021, s. 9).

Liczba zdarzeń, które zostały zarejestrowane w roku 2020 jako faktyczny incydent, wyniosła w sumie 23 309, co stanowi wzrost o około 88% w stosunku do roku 2019, kiedy zidentyfikowano 12405 incydentów przy wzroście liczby zgłoszeń tylko na poziomie około 8%. Liczba incydentów w roku 2019 wzrosła w stosunku do roku 2018 o 99%. W okresie lat 2018-2020 został utrzymany trend wskazujący na podwajanie liczby incydentów w relacji rok do roku. Zależność ta wynika przede wszystkim z alarmów systemu Arakis GOV, których liczba we wskazanych okresach wzrosła ze względu na wykryte aktywne skanowanie adresacji sieciowych należących do instytucji administracji państwowej i operatorów infrastruktury krytycznej. Dodatkowym czynnikiem kształtującym wskazaną statystykę był zwiększony poziom detekcji zagrożeń związany z rozwojem możliwości systemów wczesnego ostrzegania - Arakis GOV i N6 - działających w infrastrukturze podmiotów krajowego systemu cyberbezpieczeństwa (ABW 2021, s. 10, 2020, s. 9).

System Arakis 3.0 GOV to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł. W 2020 roku, w sieciach teleinformatycznych podmiotów uczestniczących w projekcie Arakis 3.0 GOV, zanotowano łącznie 1 813 243 995 przepływów, co przełożyło się na 1 758 813 wygenerowanych przez system alarmów, a w roku 2019 zanotowano 1 052 675 641 przepływów, z czego za alarmy uznano 844 951 (ABW 2021, s. 38). Wzrost liczby przepływów rok do roku wyniósł 72% za okres 2020-2019 r. i **330% za okres 2019-2018 r.**, a wzrost liczby zidentyfikowanych alarmów wyniósł 108% za okres 2020-2019 r. i 86% za okres 2019-2018 r. Szczegółowe informacje na temat liczby i procentowego rozkładu alarmów systemu Arakis GOV zostały przedstawione w tabeli 8.

Tabela 8. Liczba i procentowy rozkład alarmów systemu Arakis GOV CSIRT GOV ze względu na priorytety

	2020	**2019**	**2018**	**2017**	**2016**	**2015**
Przepływy	1.813.243.995	1.052.675.641	319.943.424	323.722.095	338.430.181	55.510
Alarmy	1.758.813	844.951	454.207	347.178	446.915	36.815
Alarmy priorytet pilny	187.149	266.135 31%	62.365 14%	62.292 18%	279.181 62%	Nd.
Alarmy priorytet wysoki	67.939	99.612 12%	104.502 23%	30.505 9%	52.766 12%	1.429 4%
Alarmy priorytet średni	140.303	51.721 6%	15.412 3%	15.911 4%	12.365 3%	17.548 48%

Alarmy priorytet niski	1.363.422	427.483 51%	271.928 60%	238.470 69%	102.603 23%	17.838 48%

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, 2020, 2019, 2018, 2017, 2016

Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów przedstawionych w tabeli 9 poniżej.

Tabela 9. Procentowy podział alarmów systemu Arakis GOV CSIRT GOV ze względu na typ

Typ	**2020**	**2019**	**2018**	**2017**	**2016**
1 - komunikacja do złośliwych adresów	7,34%	27,04%	5,12%	4%	52%
2 - skanowanie	77,14%	50,59%	59,88%	69%	23%
3 - wykryte znane ataki	7,80%	20,10%	16,74%	24%	17%
4 – wykryte nieopisane ataki	7,22%	1,48%	17,75%	2%	6%
5 – infekcje wewnętrzne	0,50%	0,79%	0,52%	1%	2%

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, 2020, 2019, 2018, 2017

Spośród zidentyfikowanych alarmów w roku 2020 największą intensywność miało działanie typu skanowanie portów sieciowych (typ 2) – 77%, podobnie jak latach ubiegłych – 50% w roku 2019 i 60% w roku 2018. Tego typu aktywność w największym stopniu jest kierowana w stronę takich instytucji jak: urzędy – 31,29% w roku 2020 i 32,81% w roku 2019 – oraz operatorzy infrastruktury krytycznej – 29,04% w roku 2020 i 31,21% w roku 2019. Szczegółowy procentowy rozkład przepływów alarmów typu 2 z podziałem na instytucje przedstawiony jest w tabeli 10.

Tabela 10. Procentowy podział przepływu alarmów w instytucjach - Arakis GOV CSIRT GOV

	2020	**2019**	**2018**	**2017**		**2016**	
Typ alarmu	**2**	**2**	**2**	**1**	**5**	**1**	**5**
Urzędy	31,29%	32,81%	57,24%	5,74%	42,91%	616.119	5.832.490
Infrastruktura krytyczna	29,04%	31,21%	12,59%	92,64%	39,75%	752.710 49%	160832
Ministerstwa	13,56%	19,01%	17,74%	0,60%	6,50%	160.890	4.591
Instytuty	17,06%	10,42%	4,76%	0,61%	0,98%	-	-
Służby i wojsko	5,37%	5,27%	5,83%	0,26%	6,38%	1.124	156.221
Pozostałe	3,68%	1,28%	1,84%	0,14%	3,48%	-	-

Źródło: opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, 2020, 2019, 2018, 2017

Do najbardziej aktywnych krajów pod kątem liczby generowanych przepływów w roku 2020 należały – Rosja (22%), USA (16%) i Polska (12%). W roku 2019 do najaktywniejszych należały - Rosja (28%), Stany Zjednoczone (13%), Niderlandy (12%) oraz Polska (10%). W roku 2018 do najbardziej aktywnych krajów pod względem liczby generowanych przepływów zaliczamy Chiny (22%), Stany Zjednoczone (19%), Rosję (13%) i Polskę (12%). Z kolei w roku 2017 najbardziej aktywnymi krajami w generowaniu przepływów były Chiny (35%), Stany Zjednoczone (17%), Polska (15%) i Rosja (7%). Liczba przepływów z poszczególnych krajów, należących do grupy TOP 10, stanowiła w roku 2020 - 73%, a w roku 2019 - 67% wszystkich wygenerowanych przepływów zanotowanych przez system Arakis GOV (ABW 2021, s. 41-42, 2020, s. 26). Wskazanie państw, z których generowane były przepływy w systemach teleinformatycznych polskiej cyberprzestrzeni wraz z rozkładem procentowym w ciągu ostatnich lat zostało przedstawione w tabeli 11.

Tabela 11. Rozkład źródeł ataków na sieci monitorowane przez system Arakis GOV pod kątem liczby generowanych przepływów (top 10)

Kraj	2020	2019	2018	2017	2016	2015
Rosja	22%	28%	13%	7%	4%	-
USA	16%	13%	19%	17%	15%	15,27%
Niderlandy	4%	12%	7%	4%	-	2,4%
Polska	12%	10%	12%	15%	%	0,9%
Chiny	4%	8%	22%	35%	40%	45,61%
Niemcy	3%	8%	3%	4%	9%	1,84%
Indie	2%	6%	-	4%	-	-
Japonia		5%	-	-	-	-
Ukraina	3%	5%	5%	-	-	-
Mołdawia		5%	-	-	-	-
Wielka Brytania	3%	-	9%	-	4%	0,79%
Bułgaria		-	6%	-	-	-
Kambodża		-	4%	-	-	-
Francja	3%	-	-	5%	-	1,53%
Wietnam		-	-	5%	4%	-
Brazylia		-	-	4%	3%	-
Tajwan		-	-	-	4%	-
Korea Płd.		-	-	-	4%	-
Łotwa						5,99%
Kanada						0,59%
Nieznane		-	-	-	13%	21,50%

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, 2020, 2019, 2018, 2017

Biorąc pod uwagę specyfikę sieci Internet (tzw. brak granic), infrastruktura teleinformatyczna podmiotów generujących przepływy w stronę systemu Arakis GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie. W związku z tym zaprezentowana statystyka odzwierciedla lokalizację złośliwej infrastruktury sieciowej w poszczególnych krajach, zaś duża liczba przepływów z Polski wynika ze specyfiki działania systemu Arakis GOV (ABW 2021, s. 42, 2020, s. 26).

Ocena bezpieczeństwa systemów teleinformatycznych realizowana przez zespoły ABW

Zespół CSIRT GOV corocznie przeprowadza ocenę bezpieczeństwa systemów teleinformatycznych. W ramach przeprowadzanych ocen bezpieczeństwa prowadzi szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych instytucji. W roku 2020 zespól CSIRT GOV przeprowadził ocenę bezpieczeństwa systemów teleinformatycznych w 14 instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadała w sumie 82 systemy teleinformatycznych. W roku 2019 zespól CSIRT GOV przeprowadził ocenę bezpieczeństwa systemów teleinformatycznych w 10 instytucjach administracji rządowej oraz infrastruktury krytycznej, w których przebadała w sumie 35 systemów teleinformatycznych. W ramach przeprowadzonych ocen bezpieczeństwa przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktur teleinformatycznych instytucji. Do testów należało pasywne, półpasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, wykorzystywanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej (ABW 2021, s. 46-47, 2020, s. 30). W wyniku przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV dokonał identyfikacji szeregu podatności od stopnia informacyjnego aż do błędów należących do kategorii krytycznych. W roku 2020 względem roku 2019 liczba podatności krytycznych spadła o 28%, podatności wysokich o 51%, średnich o 33%, niskich o 66%, a informacyjnych o 78%, przy jednoczesnych wzroście liczby badanych podmiotów (z 10 do 14) i systemów teleinformatycznych (z 35 do 82). Liczba podatności w systemach teleinformatycznych kluczowych podmiotów w kraju znacząco spadła względem roku poprzedniego. Liczba podatności w roku 2019 znacząco wzrosła względem roku 2018. Tak więc liczba podatności w roku 2019 była rekordowo wysoka. Liczba podatności w systemach teleinformatycznych w instytucjach poddanych ocenie bezpieczeństwa przez CSIRT GOV ze względu na kategorie w latach 2015-2020 została przedstawiona w tabeli 12.

Tabela 12. Zakres oceny bezpieczeństwa systemów teleinformatycznych i liczba incydentów wykrytych przez CSIRT GOV (ABW)

Instytucje i systemy teleinformatyczne	2020	2019	2018	2017	2016	2015
Ilość instytucji	14	10	-	-	-	-
Ilość syst. teleinform.	82	35	-	-	-	-
Klasa podatności						
Krytyczne	95	131	38	11	-	3%
Wysokie	223	457	130	88	-	13%
Średnie	1.761	2.608	1.051	530	-	Nd.
Niskie	194	571	166	255	-	77%
Informacyjne	2.056	9.268	5.690	1.098	-	7%

Źródło: Opracowanie własne na podstawie: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP,* CSIRT-GOV ABW, 2021, s. 47, 2020, 2019, 2018, 2017

W ramach prowadzonych ocen bezpieczeństwa Zespół CSIRT GOV corocznie przeprowadza również analizę źródeł otwartych, tzw. OSINT. Czynności te pozwalają na określenie ilości danych zawartych jako metadata w dokumentach publikowanych w ramach publicznych serwerów WWW oraz portalach społecznościowych, na których pracownicy posiadali aktywne konta (ABW 2021, s. 53, 2020, s. 34).

Podsumowanie

Polska cyberprzestrzeń i jej bezpieczeństwo powinna mieć oparcie w stosownych, dobrze opracowanych regulacjach prawnych oraz dokumentach strategicznych bezpieczeństwa państwa i wynikających z nich rozwiązań strukturalnych, systemowych, organizacyjnych i **technicznych. W tym kontekście warto dokonać przeglądu tych regulacji i dokumentów strategicznych pod kątem ich całościowego, holistycznego zaadresowania zagadnień bezpieczeństwa polskiej cyberprzestrzeni.**

Ataki cybernetyczne są coraz bardziej powszechne i wszechstronne. W ostatnim czasie zwiększyła się ilość działań w kierunku administracji rządowej i samorządowej oraz infrastruktury krytycznej. Zaprezentowane analizy raportów prezentowanych przez jednostki CERT/CSIRT realizujące zadania dla podmiotów gospodarki i administracji publicznej i rządowej pokazują jednoznacznie, że niezależnie od charakteru ujawnionych incydentów **środowisko krajowych systemów teleinformatycznych jest w trybie ciągłym poddawane różnorodnym oraz szkodliwym i przestępczym działaniom oraz** atakom ze strony różnych aktorów, i wymaga zapewnienia stałej ochrony. Ilość ataków stale, z roku na rok, wzrasta, wywołując stan zwiększającego się zagrożenia. Wynikać to może

z kilku powodów, m.in.: ze zwiększonej aktywności wrogich podmiotów (grup hakerskich, państw) oraz zwiększonej ilości systemów teleinformatycznych administracji, dostawców usług kluczowych i operatorów infrastruktury krytycznej włączonych do system**ów monitorowania i** wczesnego ostrzegania.

Wyniki sprawdzeń i audytów systemów teleinformatycznych realizowanych przez CSIRT GOV ABW w podmiotach administracji publicznej, u dostawców usług kluczowych i operatorów infrastruktury krytycznej wykazuje corocznie wzrost liczby podatności tych systemów we wszystkich kategoriach: od krytycznych, poprzez wysokie, średnie, niskie, do informacyjnych (niskich) do roku 2019, a w roku 2020 spadek względem 2019 przy znaczącym wzroście liczby obsłużonych instytucji i przeskanowanych systemów teleinformatycznych. Takie dane mogą świadczyć o niskim poziomie bezpieczeństwa systemów teleinformatycznych tych instytucji do roku 2019 oraz o poprawie tego bezpieczeństwa w roku 2020.

BIBLIOGRAFIA

Pozycje zwarte

[1] Kowalkowski S. (red.), 2011. Niemilitarne zagrożenia bezpieczeństwa publicznego. AON, Warszawa, za Więcaszek-Kuczyńska L., 2014. Zagrożenia bezpieczeństwa informacyjnego, Obronność. Zeszyty Naukowe 2(10)/2014 ISSN 2299-2316.

[2] Liderman K., 2012. Bezpieczeństwo informacyjne. Wydawnictwo Naukowe PWN, Warszawa.

[3] Mąkosa G., 2019. Krajowy system cyberbezpieczeństwa RP, [w:] Chabasińska A., Warchał A. (red.). Perspektywy bezpieczeństwa w teorii i praktyce, Wojskowa Akademia Techniczna, Warszawa.

[4] Mąkosa G., 2020. Bezpieczeństwo cybernetyczne systemów w czwartej rewolucji przemysłowej, [w:] Wojciechowski Z. Zaskórski P. (red.). Czwarta rewolucja przemysłowa. Mity, paradygmaty i zastosowania. Tom 1 Kompetencje i baza narzędziowa Przemysłu 4.0, Wojskowa Akademia Techniczna, Warszawa (a).

[5] Mąkosa G., 2020. Cyberbezpieczeństwo – wybrane aspekty prawne i organizacyjne, [w:] Śmiałek K. (red.). Dziedziny i sektory bezpieczeństwa narodowego – wybrane zagadnienia, Wojskowa Akademia Techniczna, Warszawa (b).

[6] Mąkosa G., 2020. Zarządzanie kryzysowe a krajowy system cyberbezpieczeństwa, [w:] Śmiałek K. (red.). Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa, Wojskowa Akademia Techniczna, Warszawa (c).

[7] Nowak E., Nowak M., 2011. Zarys teorii bezpieczeństwa narodowego, Difin SA, Warszawa, za Więcaszek-Kuczyńska L., 2014. Zagrożenia bezpieczeństwa informacyjnego, Obronność. Zeszyty Naukowe 2(10)/2014 ISSN 2299-2316.

[8] Więcaszek-Kuczyńska L., 2014. Zagrożenia bezpieczeństwa informacyjnego, Obronność. Zeszyty Naukowe 2(10)/2014 ISSN 2299-2316.

[9] Żebrowski A., 2013. Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013.

Dokumenty strategiczne, regulacje prawne i raporty

[1] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2013. BBN

[2] Doktryna Cyberbezpieczeństwa RP, 2015. BBN

[3] Strategia Bezpieczeństwa Narodowego RP, 2014. Kancelaria Prezydenta/Biuro Bezpieczeństwa Narodowego, BBN.

[4] Strategia Bezpieczeństwa Narodowego RP, 2020. Kancelaria Prezydenta/Biuro Bezpieczeństwa Narodowego, BBN.

[5] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, 2013. BBN.

[6] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r.

[7] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, 2017. RM.

[8] Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, 2017. RM.

[9] Plan działań w zakresie zapewniania bezpieczeństwa cyberprzestrzeni RP, 2015. RM.

[10] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 2013. RM.

[11] Narodowy Program Ochrony Infrastruktury Krytycznej, 2018. RCB.

[12] Załącznik 1 do Narodowy Program Ochrony Infrastruktury Krytycznej - Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, 2018. RCB.

[13] Dyrektywa PE 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. U. UE L 194/1.

[14] Ustawa z dnia 26 kwietnia 2017 o zarządzaniu kryzysowym, Dz. U. 2007 Nr 89 poz. 590 z późn. Zmianami.

[15] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. Nr 83 poz. 542.

[16] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565.

[17] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526.

[18] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.

[19] Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. poz. 1780.

[20] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz. U. poz. 2080.

[21] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2020, 2021. NASK-PIB, Warszawa.

[22] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, 2020. NASK-PIB, Warszawa.

[23] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, 2019. NASK-PIB, Warszawa.
[24] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 r., 2021.CSIRT-GOV ABW.
[25] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r., 2020. CSIRT-GOV ABW.
[26] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r., 2019. CSIRT-GOV ABW.
[27] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 r., 2018. CSIRT-GOV ABW.
[28] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 r., 2017. CSIRT-GOV ABW.
[29] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 r., 2016. CSIRT-GOV ABW.