ZARZĄDZANIE BEZPIECZEŃSTWEM KRAJOWYCH SYSTEMÓW TELEINFORMATYCZNYCH

NATIONAL TELEINFORMATION SYSTEMS SECURITY MANAGEMENT

Grzegorz MĄKOSA

Wojskowa Akademia Techniczna

Abstrakt. Celem artykułu jest przegląd i ocena krajowych systemów teleinformatycznych z perspektywy zagrożeń i ataków cybernetycznych oraz działalności krajowych jednostek cyberbezpieczeństwa realizujących zadania dla podmiotów gospodarki i administracji publicznej i rządowej – CERT Polska i CSIRT GOV, zaprezentowanej z perspektywy zestawienia i analizy danych z ich corocznych raportów, dotyczących stanu cyberbezpieczeństwa kraju. Raporty pokazują jednoznacznie, że niezależnie od charakteru ujawnionych incydentów środowisko krajowych systemów teleinformatycznych jest w trybie ciągłym poddawane różnorodnym szkodliwym i przestępczym działaniom oraz atakom i wymaga zapewnienia stałej ochrony. Zagadnienie zapewnienia bezpieczeństwa systemów teleinformatycznych podejmują regulacje dotyczące zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów publicznych. Ww. regulacje prawne definiują m.in. wymagania wobec podmiotów nimi objętych odnośnie wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa. Autor przedstawia proponowane przez siebie podejście do zastosowania spójnego i kompletnego zbioru norm ISO adresujących kwestie zarządzania bezpieczeństwem informacji, wdrażanego jako zintegrowany system zarządzania bezpieczeństwem

Abstract. The article presents the security issues of national ICT systems from the perspective of cyber threats and attacks as well as the activities of national cybersecurity units performing tasks for economic entities and public and government administration – CERT Polska and CSIRT GOV, presented from the perspective of the compilation and analysis of data from their annual reports on the state of cybersecurity country. The reports clearly show that regardless of the nature of the disclosed incidents, the environment of national ICT systems is constantly subjected to various and harmful and criminal activities and attacks by various actors, and requires constant protection. The issue of ensuring the security of ICT systems is addressed in the regulations on crisis management, the national cybersecurity system and the computerization of public entities. The above-mentioned legal regulations define, among others requirements for entities covered by them regarding the implementation of appropriate organizational and technical security solutions and the security management system of ICT systems and information in order to ensure an appropriate level of their security. The author presents his proposed approach to the application of a consistent and complete set of ISO standards addressing the issues of information security management, implemented as an integrated security management system

Słowa kluczowe: cyberbezpieczeństwo, zarządzanie bezpieczeństwem, bezpieczeństwo teleinformatyczne, bezpieczeństwo państwa

Keywords: cybersecurity, safety management, ICT security, national security

Wstęp

Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi stanowią cyberprzestrzeń. W cyberprzestrzeni realizowane są usługi cyfrowe obywateli – jako społeczeństwa informacyjnego, podmiotów gospodarczych i różnych organizacji, usługi wspomagające działalność administracji 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).

Domeną i odpowiedzialnością państwa jest zapewnienie bezpieczeństwa w 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 2020b, s. 115). Najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane i kompleksowe, obejmujące wszystkie obszary łączące wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny[1].

Cyberbezpieczeństwo jest składową bezpieczeństwa narodowego i międzynarodowego i jest coraz istotniejszym ich komponentem, a zapewnienie odpowiednio wysokiego poziomu cyberbezpieczeństwa jest kluczowym wyzwaniem stojącym przed państwami.

Organizacja i zarządzanie bezpieczeństwem systemów teleinformatycznych przedstawiona jest w artykule z trzech perspektyw – w ujęciu wybranych aspektów, zdefiniowanych przez stosowne regulacje prawne dotyczące zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i informatyzacji podmiotów realizujących zadania publiczne.

Zagrożenia i ataki na systemy teleinformatyczne

Zagrożenia cybernetyczne dla systemów teleinformatycznych są powiązane z rozwojem technologii informatycznych i komunikacyjnych. Dzięki ogromnym możliwościom komunikacyjnym współczesnych mediów i przeniesieniu do Internetu aktywności biznesowej i prywatnej, cyberprzestępczość rozwija się szczególnie dynamicznie. W wyniku cyberprzestępczości podmioty gospodarcze, instytucje publiczne tracą ważne dla swojej działalności dane, co negatywnie wpływa na ich działalność, a ponadto skutkuje stratami wizerunkowymi, reputacyjnymi i relacyjnymi względem klientów. Ataki komputerowe bywają także wymierzone w systemy teleinformatyczne organizacji strategicznych dla gospodarki narodowej, co może

[1] https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html (dostęp: 15.04.2018).

wywoływać ogromne szkody systemowe, finansowe i wizerunkowe, ale również technologiczne, ekologiczne czy zdrowotne w skali kraju.

Postęp w teleinformatyce sprawił, że cyberprzestrzeń nie tylko przyczynia się do rozwoju podmiotów państwowych i pozapaństwowych czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa (Żebrowski 2013, s. 453). Rozwój technologii teleinformatycznych korzystnie wpływa na rozwój społeczeństwa informacyjnego oraz rozwój gospodarczy i niestety wpływa również na rozwój negatywnych zjawisk w cyberprzestrzeni, tj. cyberprzestępczości, cyberkonfliktów, cyberwalki (walki informacyjnej) czy cyberwojny.

Prowadzone ataki na systemy teleinformatyczne są formą materializacji zagrożeń stwarzanych przez ich źródła, którymi mogą być hakerzy, przestępcy komputerowi, terroryści, szpiedzy przemysłowi. Działają oni z własnej motywacji lub na zlecenie innych osób, podmiotów czy nawet państw. Źródła zagrożeń i odpowiadające im możliwe następstwa przedstawia tabela 1.

Tabela 1. Źródła zagrożeń i możliwe następstwa

Źródła zagrożeń	Możliwe następstwa
Haker, cracker	Haking, inżynieria społeczna, wtargnięcie do systemu, włamania, nieautoryzowany dostęp do systemu
Przestępca komputerowy	Przestępstwa komputerowe (np. cybernetyczne prześladowanie), czyn przestępczy (np. powtórne odtworzenie, podszycie się, przechwycenie), przekupstwo informacyjne, atak sieciowy (np. sfałszowanie adresu źródłowego), wtargnięcie do systemu
Terrorysta	Bomba, terroryzm, wojna informacyjna, atak na system (np. rozproszona odmowa usługi DoS), penetracja systemu, naruszenie bezpieczeństwa systemu
Szpiedzy przemysłowi (wywiad, firmy, zagraniczne rządy, inne służby rządowe)	Przewaga obronna, przewaga polityczna, wykorzystanie ekonomiczne, kradzież informacji, naruszenie prywatności, inżynieria społeczna, penetracja systemu, nieautoryzowany dostęp do systemu (dostęp do informacji klasyfikowanej, wewnętrznej i/lub związanej z technologią)
Osoby wewnętrzne (źle wyszkolone, niezadowolone, złośliwe, niedbałe, nieuczciwe, zwolnieni pracownicy)	Napaść na pracownika, szantaż, przeszukiwanie informacji stanowiących własność, nadużycie komputerowe, oszustwo, kradzież, przekupstwo informacyjne, wprowadzanie fałszywych, zniekształconych danych, przechwycenie, złośliwy kod (np. wirus, bomba logiczna, koń trojański), sprzedaż danych osobowych, błędy w systemie, wtargnięcie do systemu, sabotaż systemu, nieautoryzowany dostęp do systemu

Źródło: Opracowanie własne na podstawie Mąkosa 2020a, s. 125; PN-ISO/IEC 27005

Możliwe skutki przeprowadzonych cyberataków na systemy teleinformatyczne mogą być bardzo rozległe i szkodliwe nie tylko dla podmiotów życia gospodarczego, ale i całych gospodarek krajowych. Należy zdawać sobie sprawę, że ogromna liczba zdarzeń nie zostaje nigdy wykryta, a zdarzenia wykryte często są nieujawniane z obawy przed negatywnymi konsekwencjami takiego ujawnienia.

Niezwykle istotne jest prowadzenie stałego monitoringu zdarzeń, analiz podatności i zabezpieczania systemów teleinformatycznych dla zapewnienia bezpieczeństwa cyberprzestrzeni. Monitorowanie i zabezpieczanie polskiej cyberprzestrzeni realizowane jest w Polsce przez wyspecjalizowane, przeznaczone do tego jednostki. Są to CERT Polska – prowadzony przez NASK-PIB (Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy) i CSIRT GOV – prowadzony przez Agencję Bezpieczeństwa Wewnętrznego, w której w kręgu zainteresowań są podmioty administracji rządowej i jednostki centralne oraz operatorzy infrastruktury krytycznej.

Jednostka CERT Polska publikuje corocznie raporty dotyczące obsłużonych przez nią incydentów bezpieczeństwa i informacje na temat stanu polskiego cyberbezpieczeństwa. Zgodnie z przedstawionymi w Raporcie (CERT, 2019) danymi w 2018 r. CERT Polska zanotował 19 439 zgłoszeń. Najbardziej popularne wśród przestępców były fałszywe sklepy internetowe, gdzie w odniesieniu do 2017 r. odnotowano prawie trzykrotny wzrost tego typu działalności. Następnym rodzajem szkodliwej działalności jest spam, który w porównaniu z 2017 rokiem podwoił swoją liczbę. Miało miejsce wiele incydentów z próbami włamań do systemów, urządzeń i aplikacji. Część z tych ataków została przeprowadzona na słabo zabezpieczone urządzenia Internetu Rzeczy (ang. *Internet of Things*, IoT), które często posiadają niezmienianą, standardową konfigurację producenta z domyślnym hasłem dostępowym (CERT, 2018). Przedstawione przez CERT Polska zestawienie incydentów bezpieczeństwa wg typów pokazuje, że najliczniej występowały: oszustwa komputerowe – 50,23%, złośliwe oprogramowanie – 23%, obraźliwe i nielegalne treści – 11,53%. Łącznie te trzy typy stanowiły 85% wszystkich incydentów. Dane dotyczące zestawienia typów incydentów występujących w polskiej cyberprzestrzeni w 2018 r. zawiera tabela 2.

Tabela 2. Incydenty obsłużone przez CERT Polska w 2018 r. według typów

Typ incydentu	Liczba incydentów	[%]
Obraźliwe i nielegalne treści	431	11,53
Złośliwe oprogramowanie	862	23,05
Gromadzenie informacji	101	2,70
Próby włamań	153	4,09
Włamania	125	3,34
Dostępność zasobów	49	1,31
Atak na bezpieczeństwo informacji	46	1,23
Oszustwa komputerowe	1878	50,23
Podatne usługi	69	1,85
Inne		0,67

Źródło: Opracowanie własne na podstawie Mąkosa 2020a, s. 129; CERT 2019, s. 11-12

Spośród sektorów polskiej gospodarki, najczęstsze zdarzenia miały miejsce w sektorze bankowym – 17,2%. Zestawienie klasyfikacji incydentów ze względu na sektor gospodarki przedstawiono w tabeli 3.

Tabela 3. Incydenty obsłużone przez CERT Polska w 2018 r. wg klasyfikacji ze względu na sektor gospodarki

Sektor gospodarki	**Liczba incydentów**	[%]
Infrastruktura cyfrowa	29	0,78
Służba zdrowia	13	0,35
Bankowość	643	17,20
Finanse	62	1,66
Energetyka	20	0,53
Transport	51	1,36
Sektor publiczny	85	2,27
Wodociągi	2	0,05
Inne	2834	75,80
Razem	3739	100,00

Źródło: Opracowanie własne na podstawie Mąkosa 2020a, s. 129; CERT 2019, s. 13

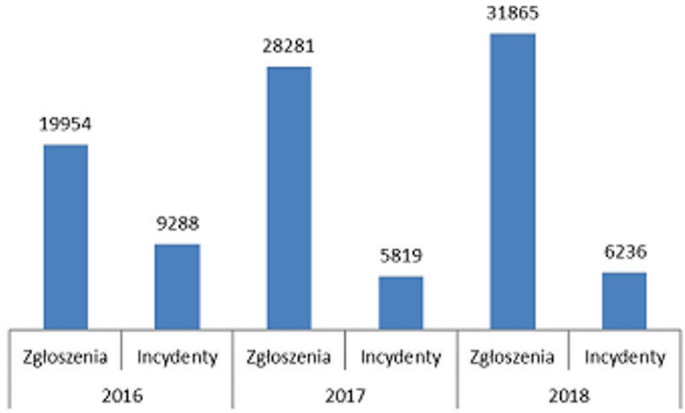
Skalę i dynamikę wzrostu liczby incydentów obsłużonych przez zespół CERT Polska w latach 1996-2018 zawiera tabela 4.

Tabela 4. Liczba incydentów obsłużonych ręcznie przez CERT Polska na przestrzeni lat 1996-2018

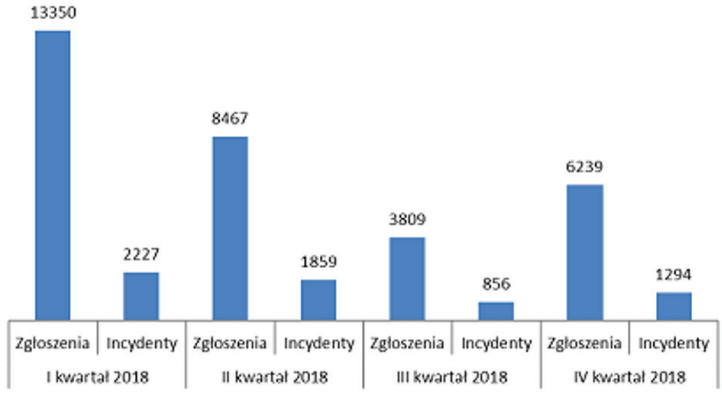
Rok	Liczba incydentów	Rok	Liczba incydentów	Rok	Liczba incydentów
2018	3739	2010	674	2002	1013
2017	3182	2009	1292	2001	741
2016	1926	2008	1796	2000	126
2015	1456	2007	2108	1999	105
2014	1282	2006	2427	1998	100
2013	1219	2005	2516	1997	75
2012	1082	2004	1222	1996	50
2011	605	2003	1196		

Źródło: Opracowanie własne na podstawie Mąkosa, 2020a, s. 130; 2 CERT, 2019, s. 13

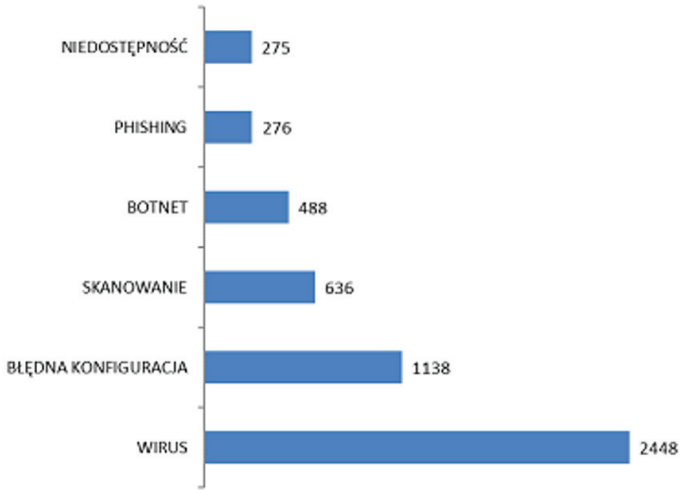
Bezpieczeństwem systemów teleinformatycznych administracji publicznej zajmuje się zespół CSIRT Agencji Bezpieczeństwa Wewnętrznego – Zespół SCIRT GOV. Zespół ten publikuje corocznie raporty o stanie bezpieczeństwa cyberprzestrzeni RP. Raporty mają na celu podnoszenie świadomości użytkowników o zagrożeniach i podatnościach bezpieczeństwa systemów teleinformatycznych. Zgodnie z przedstawionymi w Raporcie (CSIRT-GOV ABW 2019) danymi w 2018 roku Zespół CSIRT GOV odnotował 31 865 zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych. Stanowi to znaczący wzrost względem 2017 roku, w którym zarejestrowano 28 281 zgłoszeń. Liczba zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych stale rośnie. Dane na temat incydentów bezpieczeństwa obsłużonych przez specjalistów CSIRT GOV przedstawione zostały na rysunkach 1-6.



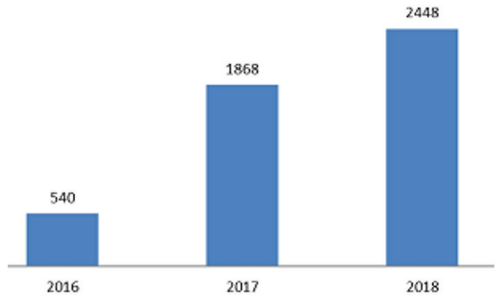
Rys. 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2016-2018
Źródło: Mąkosa 2020a, s. 134; CSIRT-GOV ABW, 2019, s. 11



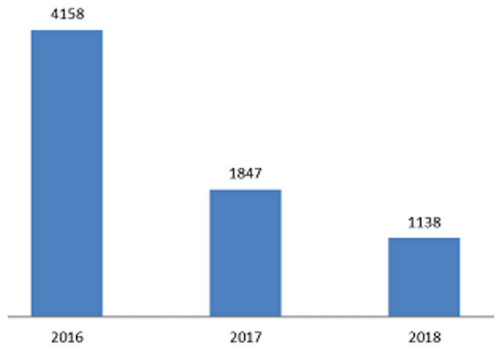
Rys. 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2018 r.
Źródło: Mąkosa 2020a, s. 134; CSIRT-GOV ABW, 2019, s. 12



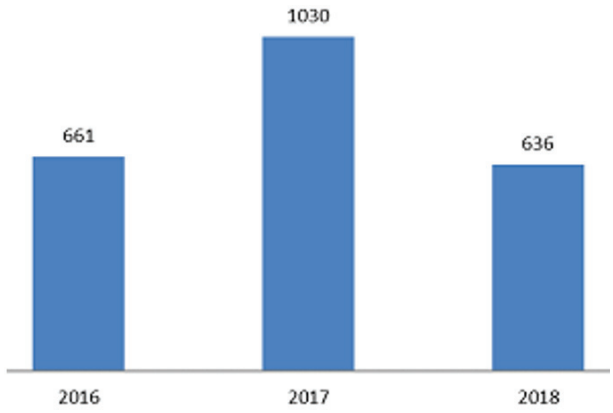
Rys. 3. Klasyfikacja najczęstszych incydentów zgłoszonych do CSIRT GOV w 2018 r.
Źródło: Mąkosa 2020a, s. 134; CSIRT GOV ABW 2019, s. 13



Rys. 4. Liczba zarejestrowanych incydentów w kategorii „wirus" w latach 2016-2018
Źródło: Mąkosa 2020a, s. 135; CSIRT GOV ABW 2019, s. 14



Rys. 5. Liczba zarejestrowanych incydentów w kategorii „błędna konfiguracja" w latach 2016-2018
Źródło: Mąkosa 2020a, s. 135; CSIRT GOV ABW 2019, s. 15

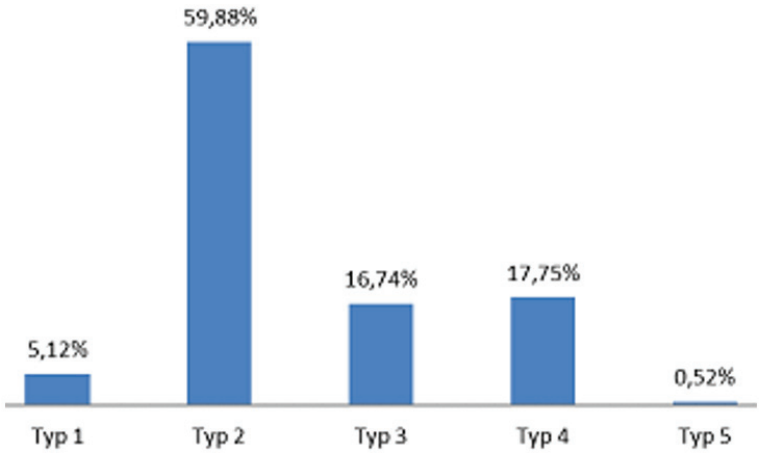


Rys. 6. Liczba zarejestrowanych incydentów w kategorii „skanowanie" w latach 2016-2018
Źródło: Mąkosa 2020a, s. 135; CSIRT GOV ABW 2019, s. 15

Zespół CSIRT GOV obsługuje zdarzenia incydentów manualnie przez swoich operatorów, jak również wykorzystuje do realizacji swoich zadań specjalistyczny system teleinformatyczny ARAKIS 3.0 GOV. Jest to rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowana analiza zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł. W 2018 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 3.0 GOV zanotowano łącznie 319 943 424 przepływów, co przełożyło się na 454 207 wygenerowanych przez system alarmów. Wśród zanotowanych alarmów:

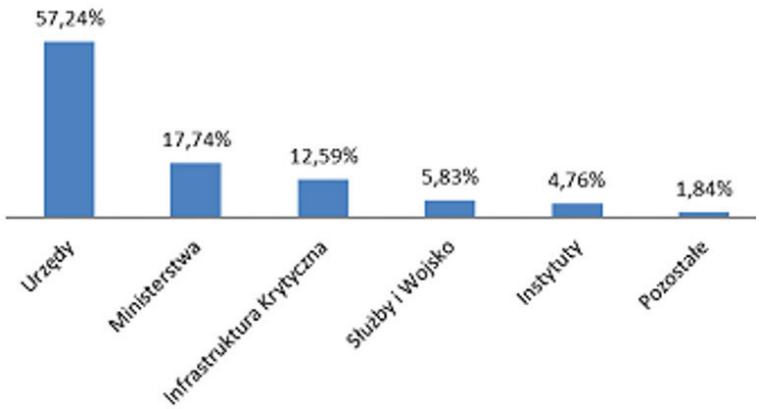
- 62 365 alarmów miało priorytet pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- 104 502 alarmów miało priorytet wysoki, tzn. wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- 15 412 alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- 271 928 alarmów miało priorytet niski, tzn. były to alarmy czysto informacyjne dotyczące aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.

Dane na temat incydentów bezpieczeństwa obsłużonych przez system ARAKIS 3.0 GOV przedstawiono na rysunkach 7-9.



Rys. 7. Procentowy podział alarmów systemu ARAKIS 3.0 GOV ze względu na typ gdzie: typ 1 – komunikacja do złośliwych adresów, typ 2 – skanowanie, typ 3 – wykryte znane ataki, typ 4 – wykryte nieznane ataki, typ 5 – infekcje wewnętrzne

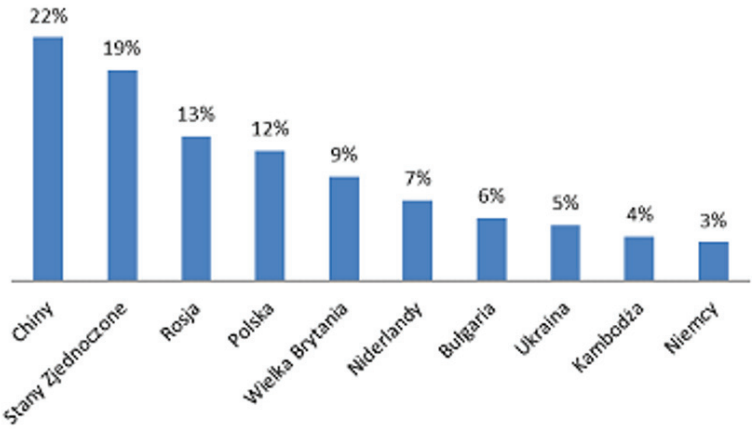
Źródło: Mąkosa G 2020a, s. 136; CSIRT GOV ABW 2019, s. 20



Rys. 8. Procentowy podział przepływów alarmów typu 2 w instytucjach

Źródło: Mąkosa, 2020a, s. 137; CSIRT GOV ABW 2019, s. 21

Próbom infiltracji poddawane są również systemy teleinformatyczne urzędów – 57,24%, ministerstw – 17,74% i infrastruktury krytycznej – 12,59%, co w sumie stanowi 88% wszystkich zaobserwowanych działań tego typu.



Rys. 9. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS 3.0 GOV pod kątem liczby generowanych przepływów

Źródło: Mąkosa 2020a, s. 137; 2CSIRT GOV ABW 2019, s. 22

Raport wskazuje, że 22% ataków pochodzi z Chin, 19% z USA, a 13% z Rosji. Ataki przeprowadzone z Polski na polskie systemy administracji to 12% ataków na sieci monitorowane przez system ARAKIS 3.0 GOV.

Zaprezentowane analizy raportów prezentowanych przez jednostki CERT/CSIRT realizujące zadania dla podmiotów gospodarki oraz 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 i wymaga zapewnienia stałej ochrony.

Cyberprzestrzeń jest polem konfliktu, na którym przychodzi nam zmierzyć 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). Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni RP, 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 (Strategia 2014, s. 35).

Systemy zarządzania bezpieczeństwem teleinformatycznym i normy międzynarodowe

Kwestie bezpieczeństwa krajowych systemów teleinformatycznych, z racji swojego znaczenia dla bezpieczeństwa państwa, są przedmiotem zainteresowania i wpływu regulacji prawnych, w tym w szczególności 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). Ww. regulacje prawne definiują m.in. wymagania wobec podmiotów nimi objętych odnośnie wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa.

Ustawa o krajowym systemie cyberbezpieczeństwa wraz z towarzyszącymi rozporządzeniami zobowiązuje operatorów usług kluczowych, dostawców usług cyfrowych i podmioty świadczące usługi w zakresie cyberbezpieczeństwa do wdrożenia systemu zarządzania bezpieczeństwem na podstawie wskazanych międzynarodowych i krajowych norm ISO (Dz.U. z 2018 r., poz. 1560). Należy zwrócić uwagę, że tylko wybrane typy podmiotów objętych ustawą muszą zrealizować ten obowiązek.

Regulacje wynikające z ustawy o zarządzaniu kryzysowym – Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje – wymagają wdrożenia rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo systemów teleinformatycznych stanowiących teleinformatyczną infrastrukturę krytyczną i systemów wspierających usługi kluczowe infrastruktury krytycznej, jednakże wskazują normy międzynarodowe i krajowe tylko jako zalecenie, czy sugestię (NPOIK, 2018).

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych wskazuje wprost wymagania wdrożenia systemu zarządzania usługami informatycznymi realizowanymi przez systemy teleinformatyczne i systemy zarządzania bezpieczeństwem informacji, wskazują**c** wprost międzynarodowe i krajowe normy ISO.

Do realizacji wymaganych przez przepisy systemów zarządzania usługami informatycznymi i systemów zarządzania bezpieczeństwem podmioty powinny zastosować najnowsze normy międzynarodowe w tym zakresie, w szczególności europejskie i krajowe normy ISO.

W związku z wymaganiami regulacji krajowego systemu cyberbezpieczeństwa operatorzy usług kluczowych, w ramach wdrażania systemu zarządzania bezpieczeństwem w systemie informacyjnym, powinni zastosować normę PN-EN ISO/IEC 27001 – w zakresie systemu zarządzania bezpieczeństwem informacji.

W związku z regulacjami systemu zarządzania kryzysowego operatorzy infrastruktury krytycznej, w ramach zapewnienia bezpieczeństwa teleinformatycznego, mogą wdrożyć system zarządzania bezpieczeństwem z wykorzystaniem następujących norm, wskazanych w NPOIK:

- PN-EN ISO 27002 – zbiór dobrych praktyk i zasad zapewnienia bezpieczeństwa informacji;
- IEC 62443 / ISA 62433 – zbiór standardów zawierających rekomendacje co do zakresu i realizacji programów poprawy bezpieczeństwa w przedsiębiorstwach będących operatorami przemysłowych systemów sterowania, wskaźników dla oceny stanu bezpieczeństwa w organizacji, definicji pojęć z zakresu bezpieczeństwa;
- NIST 800-82 – zawiera wiele rekomendacji z zakresu bezpieczeństwa teleinformatycznego systemów automatyki, w tym w szczególności w obszarze architektury sieci i separacji sieci IK od pozostałych sieci przedsiębiorstwa;
- NERC CIP – amerykański standard poświęcony bezpieczeństwu teleinformatycznemu infrastruktury krytycznej w segmencie energetyki;
- API-1164 „Pipeline SCADA Security" – zbiór zasad bezpieczeństwa systemów ICS opracowany przez American Petroleum Institute specjalnie dla sektora rafineryjnego. Wytyczne w nim zawarte mogą być także zastosowane w systemach przemysłowych innych sektorów;
- TIA-942 – amerykański standard opisujący minimalne wymagania dla infrastruktury telekomunikacyjnej i centrów przetwarzania;
- ISO/IEC 24762 – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie;
- Protecting Industrial Control Systems – Recommendations for Europe and Member States (ENISA), dokument, który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz siedem głównych kroków, jak podnieść poziom bezpieczeństwa w takim środowisku.

W związku z wymaganiami regulacji systemu informatyzacji podmiotów publicznych podmioty te powinny wdrożyć systemy zarządzania usługami informatycznymi i systemu zarządzania bezpieczeństwem informacji z zastosowaniem norm ISO wskazanych w Rozporządzeniu w sprawie krajowych ram interoperacyjności (…), a mianowicie:

- PN-EN ISO/IEC 27001 – system zarządzania bezpieczeństwem informacji;
- PN-EN ISO 27002 – zbiór dobrych praktyk i zasad zapewnienia bezpieczeństwa informacji;
- ISO/IEC 27005 – zarządzanie ryzykiem w bezpieczeństwie informacji;
- ISO/IEC 24762 – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie;
- ISO 20000-1 – system zarządzania usługami IT;
- ISO 20000-2 – wytyczne wdrażania systemu zarządzania usługami IT.

Zestawienie norm zalecanych lub wymaganych do wdrożenia przez podmioty objęte regulacjami obu systemów bezpieczeństwa zostały przedstawione w tabeli 5.

Tabela 5. Normy ISO i standardy wskazane do wdrożenia przez regulacje cyberbezpieczeństwa

ZK [Zarządzanie kryzysowe]	KSC [Krajowy system cyberbezpieczeństwa – dot. operatorów usług kluczowych]	IPP [Informatyzacja podmiotów publicznych]
ISO 27002	ISO 27001	ISO 27001
IEC 62443 / ISA 62433		ISO 17799 (27002)
NIST 800-82	ISO 22301	
NERC CIP		ISO 20000-1, 20000-2
API-1164 Pipeline SCADA Security		ISO 27005
TIA-942		
ISO 24762		ISO 24762
Protecting Industrial Control Systems		

Źródło: Opracowanie własne na podstawie Dz.U. z 2007 r., poz. 590; NPOIK 2018; Dz.U. z 2018 r., poz. 1560; Dz.U. z 2005 r. Nr 64, poz. 565, Mąkosa 2020b, s. 125

W ramach regulacji systemu zarządzania kryzysowego Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) i Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje wskazują normy międzynarodowe i krajowe jako podstawę wdrożenia systemu zarządzania bezpieczeństwem tylko jako zalecenie czy sugestię. Jednocześnie jest to lista najobszerniejsza i otwarta na nowe pozycje standardów. Takie podejście z jednej strony daje podmiotom możliwość rozwoju swoich rozwiązań i implementowania nowych standardów, a z drugiej strony brak obowiązkowego stosowania konkretnych norm może powodować brak ustandaryzowanego podejścia podmiotów do zarządzania bezpieczeństwem teleinformatycznym.

W regulacjach związanych z krajowym systemem cyberbezpieczeństwa, gdzie, choć wymagają one od wskazanych podmiotów wdrożenia systemu zarządzania bezpieczeństwem opartego na normach międzynarodowych i krajowych, to spośród szerokiej palety takich rozwiązań, jako wymagane wskazano tylko jedną normę. Regulacje krajowego systemu cyberbezpieczeństwa zostały ustanowione jako te, które porządkują i mają wznieść na wysoki poziom krajowe cyberbezpieczeństwo, co nie jest w pełni odzwierciedlone w postawionych wymaganiach, co do systemu zarządzania bezpieczeństwem dla operatorów usług kluczowych.

W regulacjach informatyzacji podmiotów publicznych wskazany został wprost wykaz sześciu norm, które należy zastosować do opracowania i wdrożenia systemu zarządzania usługami informatycznymi i systemu zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów publicznych. Takie podejście stwarza podstawę i warunki do zbudowania kompletnego i skutecznego systemu zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów publicznych.

Zaprojektowanie i wdrożenie kompletnego i skutecznego systemu zarządzania bezpieczeństwem systemów teleinformatycznych i przetwarzanych w nich danych wymaga podejścia holistycznego i zastosowania możliwie dużej i spójnej puli norm i standardów dających odpowiednie wymagania i wytyczne.

W ramach prowadzonych badań, autor zidentyfikował wiele międzynarodowych i krajowych norm ISO dotyczących kwestii bezpieczeństwa teleinformatycznego, które z powodzeniem mogłyby być zastosowane we wdrażanych przez podmioty systemach zarządzania bezpieczeństwem. Są to normy:

1. ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji. Norma definiująca wymagania w zakresie planowania, wdrożenia, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji. Zawiera opis procesów zarządzania oraz procesów i rozwiązań organizacyjnych i technicznych bezpieczeństwa, tzw. zabezpieczeń.
2. ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Zasady zabezpieczenia informacji. Norma definiująca i opisująca najlepsze praktyki w zakresie rozwiązań organizacyjnych i technicznych bezpieczeństwa, tzw. zabezpieczeń.

3. ISO/IEC 27005 Information technology – Security techniques – Information security risk management. Norma opisująca proces zarządzania ryzykiem bezpieczeństwa informacji oraz katalogi zagrożeń, podatności i zabezpieczeń dla rozwiązań bezpieczeństwa.
4. ISO/IEC 27014 Information technology – Security techniques – Governance of information security. Norma opisująca system ładu bezpieczeństwa informacji, model zarządzania nadzorczego – governance, wyższego poziomu niż zarządzanie operacyjne – management.
5. ISO/IEC 27031:2010 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. Norma opisująca całościowy proces zarządzania ciągłością działania technologii informacyjno-komunikacyjnej lub inaczej systemów teleinformatycznych.
6. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. Norma opisująca zagadnienia i aspekty bezpieczeństwa w cyberprzestrzeni oraz rozwiązania bezpieczeństwa.
7. ISO/IEC 27033 Information technology – Security techniques – Network security. Norma opisująca kwestie bezpieczeństwa sieci teleinformatycznej.
8. ISO/IEC 27034 Information technology – Security techniques – Application security. Norma opisująca kwestie bezpieczeństwa aplikacji (oprogramowania).
9. ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management. Norma opisująca proces zarządzania incydentami bezpieczeństwa informacji.
10. ISO/IEC 27040:2015 Information technology – Security techniques – Storage security. Norma opisująca proces i rozwiązania bezpieczeństwa systemów składowania i przechowywania danych.

Zastosowanie ww. norm z obszaru zarządzania bezpieczeństwem informacji i systemów teleinformatycznych do wdrożenia przez podmioty systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa wymaganego systemu zarządzania, szczególnie w formie zintegrowanego systemu zarządzania, zdaniem autora byłoby najbardziej efektywnym rozwiązaniem realizującym zamierzone cele bezpieczeństwa.

Wnioski

Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone z rozległymi sieciami komputerowymi stanowią cyberprzestrzeń, w której realizowane są usługi cyfrowe obywateli – jako społeczeństwa informacyjnego, podmiotów gospodarczych i różnych organizacji, usługi wspomagające działalność administracji i podmiotów realizujących zadania publiczne.

Równolegle wraz z rozwojem technologii informatycznych i komunikacyjnych w cyberprzestrzeni realizowane są ataki na systemy teleinformatyczne i działalność przestępczą.

Wnioski wynikające z analizy raportów prezentowanych przez jednostki CERT/CSIRT realizujące zadania cyberbezpieczeństwa dla podmiotów gospodarki oraz administracji publicznej i rządowej pokazują jednoznacznie, że niezależnie od charakteru ujawnionych incydentów środowisko krajowych systemów teleinformatycznych jest w trybie ciągłym poddawane różnorodnym szkodliwym i przestępczym działaniom oraz atakom i wymaga zapewnienia stałej ochrony. Liczba ataków stale z roku na rok wrasta, wywołując stan zwiększającego się zagrożenia.

Odpowiedzią w zakresie bezpieczeństwa krajowych systemów teleinformatycznych z racji ich znaczenia dla bezpieczeństwa państwa są regulacje prawne, w tym w szczególności ustawa o zarządzaniu kryzysowym, ustawa o krajowym systemie cyberbezpieczeństwa i ustawa o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącymi im aktami wykonawczymi i pomocniczymi, formułujące m.in. wymagania wobec podmiotów nimi objętych odnośnie wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa. Do realizacji tego celu ww. regulacje wskazują na konieczność zastosowania międzynarodowych i krajowych norm ISO, jednakże każda z regulacji wskazuje inny ich zbiór, co w połączeniu z niespójnością rozwiązań bezpieczeństwa teleinformatycznego zawartego w tych regulacjach tworzy nieprecyzyjne i niedostateczne podstawy do budowy wysokiego poziomu bezpieczeństwa krajowych systemów teleinformatycznych.

Zastosowanie jednorodnego i spójnego zbioru norm ISO kompleksowo adresujących kwestie zarządzania bezpieczeństwem informacji i systemów teleinformatycznych do wdrożenia wymaganego przez regulacje prawne systemu zarządzania bezpieczeństwem, szczególnie w formie zintegrowanego systemu zarządzania bezpieczeństwem, zdaniem autora byłoby najbardziej efektywnym rozwiązaniem realizującym zamierzone cele bezpieczeństwa.

BIBLIOGRAFIA

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

[2] Doktryna Cyberbezpieczeństwa RP, 2015.

[3] 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.

[4] https://pl.wikipedia.org/wiki/Bezpieczenstwo za: Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2008 (dostęp: 15.04.2018).

[5] https://pl.wikipedia.org/wiki/Bezpieczenstwo_teleinformatyczne (dostęp: 15.04.2018).

[6] https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html (dostęp: 15.04.2018).

[7] https://www.cybsecurity.org/pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa.

[8] https://www.gov.pl/web/cyfryzacja.

[9] iso.org (dostęp: 3.01.2020).

[10] ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji.

[11] ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Zasady zabezpieczenia informacji.

[12] ISO/IEC 27005 Information technology – Security techniques – Information security risk management.

[13] ISO/IEC 27014 Information technology – Security techniques – Governance of information security.

[14] ISO/IEC 27031:2010 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.

[15] ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

[16] ISO/IEC 27033 Information technology – Security techniques – Network security.

[17] ISO/IEC 27034 Information technology – Security techniques – Application security.

[18] ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management.

[19] ISO/IEC 27040:2015 Information technology – Security techniques – Storage security.

[20] Kowalkowski, S. (red.), 2011. *Niemilitarne zagrożenia bezpieczeństwa publicznego*, AON Warszawa.

[21] Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, 2017.

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

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

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

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

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

[27] Plan działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, 2017.

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

[29] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 2013.

[30] 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.

[31] 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. z 2012 r., poz. 526.

[32] 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.

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

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

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

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

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

[38] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r., poz. 590.

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

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

[41] Warszawa PN-EN ISO 22301 System zarządzania ciągłością działania.

[42] Więcaszek-Kuczyńska, L., 2014. Zagrożenia bezpieczeństwa informacyjnego, *Obronność. Zeszyty Naukowe* 2(10)/2014.

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

DOI: HTTPS://DOI.ORG/10.37055/SBN/144283