Uzasadnienie

I. Potrzeba i cel regulacji

Stale rosnący wpływ technologii teleinformatycznych na rozwój społeczno-gospodarczy państw członkowskich Unii Europejskiej oraz wzrost ich wykorzystania w zarządzaniu, produkcji, sektorze usług oraz przez podmioty publiczne sprawia, że oferowane produkty i usługi są obecnie coraz silniej zależne od zapewnienia cyberbezpieczeństwa. Rozbudowana architektura systemów teleinformatycznych, w tym operacje na dużych zasobach danych, oraz rosnąca liczba transakcji dokonywanych za pomocą środków komunikacji elektronicznej służą rozwojowi komunikacji, handlu, transportu i stanowią podstawę funkcjonowania usług kluczowych, cyfrowych i usług świadczonych przez administrację publiczną. Niestety możliwości jakie oferują nowoczesne technologie cyfrowe wykorzystywane są też w celu popełniania przestępstw z wykorzystaniem Internetu, czy też prowadzenia działań o charakterze terrorystycznym. Powyższe uwarunkowania wymagały rozbudowy systemu cyberbezpieczeństwa państw członkowskich Unii Europejskiej.

W świetle powyższych wyzwań w dniu 14 lutego 2013 r. Komisja przedstawiła wraz z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa komunikat w sprawie europejskiej strategii bezpieczeństwa cybernetycznego: „Otwarta, bezpieczna i chroniona cyberprzestrzeń”[1]. Strategii towarzyszył wniosek legislacyjny w sprawie dyrektywy dotyczącej cyberbezpieczeństwa. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*[2] została przyjęta dnia 6 lipca 2016 r. Dyrektywa zobowiązuje wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa poprzez ustanowienie organów właściwych do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości i instytucjach

[1] Join (2013) 1 Final, 7.2.2013.
[2] Dz. U. UE 2016 L194

finansowych, sektorach zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej[3]. Wprowadza pojęcie operatora usługi kluczowej, czyli podmiotu dostarczającego poprzez system informacyjny usługę kluczową, w przypadku której incydenty bezpieczeństwa teleinformatycznego mogłyby mieć istotny wpływ na jej świadczenie. Zgodnie z dyrektywą operatorzy usług kluczowych mają być zobowiązani do stosowania odpowiednich zabezpieczeń, szacowania ryzyka, oraz do zgłaszania organom właściwym lub CSIRT wszelkich incydentów poważnie zagrażających ich systemom informacyjnym oraz mogących znacząco zakłócić ciągłość działania usług kluczowych.

Organy właściwe ds. cyberbezpieczeństwa winny mieć uprawnienia do badania przypadków niewypełniania przez operatorów zobowiązań z zakresu cyberbezpieczeństwa i wprowadzenia sankcji za nieprzestrzeganie przepisów. Przepisy dyrektywy przewidują ustanowienie jednolitego punktu kontaktowego służącego wymianie informacji międzysektorowej i międzynarodowej. Przewidują także stworzenie sieci wymiany informacji na poziomie strategiczno-politycznym między państwami członkowskimi UE (Grupy Współpracy), jak również mechanizmu współpracy na poziomie operacyjnym w postaci Sieci CSIRT pochodzących z państw członkowskich UE.

Podjęcie prac związanych z kompleksowym uregulowaniem krajowego systemu cyberbezpieczeństwa wynika zatem z jednej strony z potrzeby zapewnienia systemowego podejścia do krajowego systemu cyberbezpieczeństwa w obliczu stale rosnących i dynamicznie się zmieniających zagrożeń cyberbezpieczeństwa dla funkcjonowania państwa, gospodarki i społeczeństwa, a z drugiej strony konieczności wdrożenia do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady 2016/1148/UE.

W kwietniu 2017 roku został przyjęty uchwałą nr 52/2017 Rady Ministrów dokument strategiczny dotyczący bezpieczeństwa cyberprzestrzeni w postaci *Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*. Powstał on w efekcie prac zespołu międzyresortowego pod kierunkiem Ministerstwa Cyfryzacji. Jednym z podstawowych zadań wskazanych w *Krajowych Ramach Polityki Cyberbezpieczeństwa* jest uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, służących świadczeniu usług kluczowych, usług cyfrowych oraz usług administracji publicznej. Zamierzeniem jest rozbudowa krajowego systemu cyberbezpieczeństwa w taki sposób, aby był ukierunkowany na zbudowanie zdolności w zakresie bieżącego monitorowania zagrożeń oraz zarządzania cyberbezpieczeństwem w skali kraju.

[3] Infrastruktura cyfrowa obejmuje punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen, rejestrów nazw domen najwyższego poziomu.

Działania powyższe, podjęte przez Ministerstwo Cyfryzacji we współpracy z innymi resortami wynikają także ze zmiany ustawy o działach administracji rządowej w grudniu 2015 r.[4], która przypisała do działu informatyzacja kompetencje w zakresie bezpieczeństwa cyberprzestrzeni, Podjęcie działań organizacyjnych w celu ustanowienia kompleksowego systemu bezpieczeństwa teleinformatycznego państwa znalazło się również wśród zaleceń pokontrolnych skierowanych do byłego Ministerstwa Administracji i Cyfryzacji, w związku z kontrolą przeprowadzoną przez Najwyższą Izbę Kontroli w 2014 r. w instytucjach publicznych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

Projekt ustawy ustanawia krajowy system cyberbezpieczeństwa, którego zadaniem jest zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług. Efektem będzie podniesienie odporności kluczowych usług świadczonych z wykorzystaniem technologii informacyjnych na ataki pochodzące z cyberprzestrzeni. Tym samym projektowana regulacja przyczyni się do lepszego zapewnienia ciągłości działania tych usług, tak, aby zarówno obywatele jak i przedsiębiorcy mieli do nich stały dostęp. System będzie obejmować operatorów usług kluczowych, dostawców usług cyfrowych, zespoły CSIRT poziomu krajowego, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa. Ustawa wdroży do polskiego porządku prawnego przewidzianą dyrektywą 2016/1148/UE procedurę identyfikacji operatorów usług kluczowych.

Projekt ustawy formułuje obowiązki w zakresie bezpieczeństwa teleinformatycznego operatorów usług kluczowych. Operatorzy usług kluczowych będą zobowiązani do wdrożenia i stosowania środków technicznych i organizacyjnych, aby zapewnić bezpieczeństwo systemów informacyjnych służących do świadczenia usług kluczowych, szacowania ryzyka związanego cyberbezpieczeństwem oraz przekazywania CSIRT poziomu krajowego informacji o zaistniałych incydentach, podejrzeniu wystąpienia incydentu oraz ich obsługi we współpracy ze wspomnianym CSIRT. Operatorzy usług kluczowych będą mogli realizować obowiązki z zakresu cyberbezpieczeństwa samodzielnie bądź poprzez delegowanie realizacji obowiązków z tym związanych na podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Ustawa określa szczegółowo obowiązki w zakresie monitorowania, kontrolowania, audytów i testowania wdrożonych zabezpieczeń.

[4] Dz. U. z 2015 r., poz. 2281.

Wymaganiami z zakresu cyberbezpieczeństwa zostaną również objęci dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Z racji międzynarodowej specyfiki tych podmiotów obowiązki dla dostawców usług cyfrowych będą objęte łagodniejszym reżimem regulacyjnym. Ustawa odwołuje się tutaj do decyzji wykonawczej Komisji Europejskiej.

Do krajowego systemu cyberbezpieczeństwa będą również włączone organy administracji publicznej, sądy i trybunały, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, dyrektor Rządowego Centrum Bezpieczeństwa, jednostki podległe i nadzorowane przez organy administracji rządowej, jednostki samorządu terytorialnego oraz ich związki i zrzeszenia, uczelnie publiczne i Polską Akademię Nauk, państwowe osoby prawne, utworzone na podstawie ustaw w celu wykonywania zadań publicznych. Powyższe podmioty będą zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obsługi i zgłaszania incydentów oraz udostępniania użytkownikom wiedzy na temat stosowania odpowiednich zabezpieczeń przed zagrożeniami cyberbezpieczeństwa. Będzie to doprecyzowanie realizowanych działań z zakresu cyberbezpieczeństwa, które dotychczas wynikają głównie z przepisów wykonawczych wydanych do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz zadań realizowanych w ramach *„Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, z lat 2013-2016”*. Do systemu zostaną włączeni również przedsiębiorcy telekomunikacyjni, którzy są objęci obowiązkami stosowania odpowiednich zabezpieczeń i zgłaszania incydentów zgodnie z ustawą z dnia 16 lipca 2004 r. - *Prawo telekomunikacyjne.* W związku z powyższym ustawa będzie zawierać stosowne przepisy zmieniające ustawę - *Prawo telekomunikacyjne*, mające na celu harmonizację mechanizmów zgłaszania incydentów w krajowym systemie cyberbezpieczeństwa.

Projekt ustawy tworzy nowe rozwiązania systemowe i określa kompetencje podmiotów zajmujących się cyberbezpieczeństwem, a więc CSIRT poziomu krajowego i formułuje w tym zakresie nowe obowiązki dla ministra właściwego do spraw informatyzacji. CSIRT-y poziomu krajowego będą współpracować ze sobą, aby zapewnić spójny i kompletny system zarządzania ryzykiem w zakresie cyberbezpieczeństwa państwa oraz obsługę zgłoszonych incydentów, w tym zwłaszcza incydentów poważnych i krytycznych, najpoważniejszych z punktu widzenia państwa. Ustawa nadaje nowe robowiązki dla ministra właściwego do spraw informatyzacji w zakresie organizacji krajowego systemu cyberbezpieczeństwa. Minister właściwy ds. informatyzacji będzie zatem opracowywał Strategię Cyberbezpieczeństwa, prowadził politykę informacyjną na temat krajowego systemu cyberbezpieczeństwa, realizował obowiązki sprawozdawcze wobec instytucji

unijnych. Nowe role techniczne ministra właściwego ds. informatyzacji będą związane z uruchomieniem z dniem 1 stycznia 2021 r. systemu teleinformatycznego wspierającego realizację zadań podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności umożliwiającego zgłaszanie i obsługę incydentów, szacowanie ryzyka teleinformatycznego i ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Projekt ustawy powołuje organy właściwe ds. cyberbezpieczeństwa, które mają uprawnienia do wydawania decyzji w sprawie uznania bądź odebrania statusu operatora usługi kluczowej, wydawania wytycznych sektorowych w zakresie cyberbezpieczeństwa, w tym wytycznych dotyczących zgłaszania incydentów oraz wprowadzenia kar za nieprzestrzeganie przepisów. Wobec ustanowienia organów właściwych w różnych sektorach ustawa powołuje również pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa, prowadzony przez ministra właściwego do spraw informatyzacji, odpowiedzialny za wymianę informacji związanych z cyberbezpieczeństwem na poziomie kraju oraz współpracę transgraniczną na poziomie Unii Europejskiej.

Celem projektowanej regulacji jest również określenie sposobów sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy. Nadzorem będzie objęta realizacja przez operatorów usług kluczowych i dostawców usług cyfrowych obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, jak również jakość usług świadczonych przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

II. Stan rzeczywisty w dziedzinie regulacji

1. Prawo materialne krajowe

Minister Cyfryzacji zgodnie z obowiązującym stanem prawnym odpowiada za zapewnienie minimalnych wymagań z zakresu bezpieczeństwa teleinformatycznego w administracji publicznej – ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[5] oraz rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[6]. Wymogi dotyczące interoperacyjności, dostępności oraz bezpieczeństwa zawarte są w art. 13-16 ustawy, natomiast §20 rozporządzenia określa wymagania systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji. W 2015 r. Minister

[5] Dz. U. z 2017 r. poz. 570.
[6] Dz. U. z 2016 r. poz. 113.

Cyfryzacji zatwierdził również *Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych.* Celem *Wytycznych* jest zapewnienie wsparcia przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych, w tym ww. wymagań w obszarze bezpieczeństwa informacji.

Do Urzędu Komunikacji Elektronicznej zgłaszane są zgodnie z ustawą z dnia 16 lipca 2004 r. - *Prawo telekomunikacyjne*[7] najważniejsze incydenty w sieciach telekomunikacyjnych. Ustawa- *Prawo telekomunikacyjne* oraz wydane na jej podstawie akty wykonawcze zawierają również przepisy związane z kwestiami bezpieczeństwa lub integralności sieci i usług telekomunikacyjnych, ciągłości działania, bezpieczeństwa danych osobowych, realizacją obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego[8]. Minister Cyfryzacji zgodnie z ustawą z dnia 5 września 2016 r. *o usługach zaufania i identyfikacji elektronicznej*[9] zapewnia również funkcjonowanie krajowej infrastruktury zaufania oraz sprawuje nadzór nad dostawcami usług zaufania.

Pewne wymagania w zakresie bezpieczeństwa informacji, dotyczące zarówno przedsiębiorców, jak i jednostek sektora finansów publicznych znajdują się w ustawie z dnia 6 czerwca 1997 r. - *Kodeks karny*[10], ustawie z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*[11], ustawie z dnia 27 sierpnia 2009 r. *o finansach publicznych*[12], ustawie z dnia 29 września 1994 r. *o rachunkowości*[13], ustawie z dnia 6 września 2001 r. *o dostępie do informacji publicznej*[14], ustawie z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*[15], ustawie z dnia 28 kwietnia 2011 r *o systemie informacji w ochronie zdrowia*[16], ustawie z dnia 14 lipca 1983 r. *o narodowym zasobie archiwalnym i archiwach*[17], ustawie z dnia 29 sierpnia 1997 r. - *Prawo bankowe*[18], ustawie z dnia 5 września 2016 r. *o usługach zaufania i identyfikacji elektronicznej*, ustawie z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną*[19], ustawie z dnia 29

[7] Dz. U. z 2017 r. poz. 1907.
[8] Obowiązki w dziedzinie cyberbezpieczeństwa zostały określone w Dziale VII i Dziale VIII Prawa telekomunikacyjnego.
[9] Dz. U. poz. 1579.
[10] Dz. U. z 2016 r. poz. 1137.
[11] Dz. U. z 2016 r. poz. 922.
[12] Dz. U. z 2016 r. poz. 1870.
[13] Dz. U. z 2016 poz. 1047.
[14] Dz. U. z 2016 r. poz. 1764.
[15] Dz. U. z 2016 r. poz. 1972.
[16] Dz. U. z 2017 r. poz. 1845.
[17] Dz. U. z 2016 r. poz. 1506.
[18] Dz. U. z 2017 r. poz. 1876.
[19] Dz. U. z 2017 r. poz. 1219.

czerwca 1995 r. *o statystyce publicznej*[20] oraz ustawie z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*[21].

2. Zakres podmiotowy

W polskim systemie prawnym nie ma przepisów regulujących szczegółowo zagadnienie cyberbezpieczeństwa w sektorach objętych zakresem dyrektywy 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 UE*. Pewne elementy o charakterze bezsankcyjnym regulujące wymagania bezpieczeństwa teleinformatycznego odnoszące się do sfery infrastruktury krytycznej zostały zawarte w załączniku nr 1 do *Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)*, przyjmowanego na podstawie ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*[22]. Rządowe Centrum Bezpieczeństwa weryfikuje plany operatorów infrastruktury krytycznej m.in. pod kątem oceny ryzyka, stosowanych zabezpieczeń i przyjętych w obiektach zasad ochrony teleinformatycznej. Należy jednak podkreślić, że inna jest podstawa prawna dyrektywy 2016/1148/UE, którym jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej odnoszący się do wspólnego rynku. Kwestia ochrony krajowej infrastruktury krytycznej jest natomiast kompetencją wyłączną państw członkowskich, ściśle powiązaną ze sferą bezpieczeństwa narodowego.

Dyrektywa 2016/1148/UE wskazuje następujące sektory i podsektory wraz z rodzajami podmiotów w ich obszarze, które mają zostać objęte regulacją. Poniższej wymieniono, jakimi pojęciami posługuje się Dyrektywa w poszczególnych sektorach oraz zaznaczono, czy (i w jakim akcie prawnym) zostały one zdefiniowane w polskim systemie prawa.

2.1 Sektor energetyki

a) podsektor energii elektrycznej; regulacja ma, zgodnie z wytycznymi z Dyrektywy 2016/1148, obejmować przedsiębiorstwa energetyczne, operatorów systemu dystrybucyjnego, operatorów systemu przesyłowego. Regulacje dotyczące tego sektora zostały zawarte w ustawie - *Prawo energetyczne*[23]. Przepisy wspomnianej ustawy zawierają definicje przywołanych pojęć,

[20] Dz. U. z 2017 r. poz. 1068.
[21] Dz. U. 2003 Nr 153, poz. 1503 z późn. zm.
[22] Dz. U. z 2017 r. poz. 209.
[23] Dz.U. z 2017 r. poz. 220.

b) podsektor ropy naftowej; regulacją mają być objęci operatorzy ropociągów oraz operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej. Nie ma definicji tych pojęć w polskim ustawodawstwie. Pojęciem, które zdaje się zawierać w sobie wymienione wyżej, jest „przedsiębiorstwo energetyczne" zdefiniowane w ustawie *Prawo energetyczne*,

c) podsektor gazu; regulacja ma objąć: przedsiębiorstwa dostarczające gaz, operatorów systemu przesyłowego, operatorów systemu dystrybucyjnego, operatorów systemu magazynowania, operatorów systemu LNG, przedsiębiorstwa gazowe, operatorów instalacji służących do rafinacji i przetwarzania gazu ziemnego. W polskim systemie prawnym regulacje dotyczące omawianego sektora znajdują się w ustawach: *Prawo energetyczne* i ustawie *o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym*[24]. Przedsiębiorstwo dostarczające gaz, przedsiębiorstwo gazowe i operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego nie są zdefiniowane w powyższych ustawach. Podobnie jak w podsektorze ropy naftowej, pojęcie „przedsiębiorstwa energetycznego" z ustawy - *Prawo energetyczne,* obejmuje je swoim zakresem znaczeniowym.

2.2 Sektor transportu

a) podsektor transportu lotniczego; regulacja ma obejmować: przewoźników lotniczych, zarządzających portem lotniczym, jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych, operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC). Ta materia uregulowana jest w ustawie *Prawo lotnicze*[25]. Z powyższych pojęć, w wymienionej ustawie, zdefiniowani zostali przewoźnicy lotniczy i zarządzający portami lotniczymi. Nie ma definicji jednostek obsługujących urządzenia pomocnicze. W tym wypadku tożsamym pojęciem może być „obsługa naziemna", uregulowana w przedmiotowej ustawie. Brakuje też definicji operatorów zarządzających ruchem lotniczym. Zagadnienie kontroli bezpieczeństwa jest uregulowane w ustawie - *Prawio lotnicze*,

b) podsektor transportu kolejowego; regulacja, zgodnie z wytycznymi Dyrektywy 2016/1148/UE, ma obejmować zarządców infrastruktury, przedsiębiorstwa kolejowe

[24] Dz.U. z 2016 poz. 1899.
[25] Dz.U. z 2016 poz. 605.

i operatorów obiektów infrastruktury usługowej. Sektor ten, w polskim systemie prawnym regulowany jest u*stawą o transporcie kolejowym*[26]. Spośród wymienionych pojęć wszystkie zostały zdefiniowane w przedmiotowej ustawie. Pojęcie przedsiębiorstwa kolejowego nie pojawia się literalnie w ustawie, jednak pojęcie „przewoźnika kolejowego" zdaje się być pojęciem tożsamym,

c) podsektor transportu wodnego ma obejmować: armatorów śródlądowego, morskiego i przybrzeżnego, wodnego transportu pasażerów i towarów, organy zarządzające portami, operatorów systemów ruchu statków. Omawiany sektor jest regulowany w polskim systemie prawnym w następujących ustawach: *Kodeks morski*[27], *o żegludze śródlądowej*[28], *o portach i przystaniach morskich*[29], *o bezpieczeństwie morskim*[30]. Poza pojęciem „operatorów systemów ruchu statków" wszystkie powyższe są zdefiniowane. Przyjęto, że zagadnienie operatorów ruchu statków zostało uregulowane pod postacią Służby Kontroli Ruchu Statków w u*stawie o bezpieczeństwie morskim,*
d) podsektor transportu drogowego; objęte regulacją mają być organy administracji drogowej oraz operatorzy inteligentnych systemów transportowych. Sektor transportu drogowego regulują w polskim systemie prawnym: u*stawa o transporcie drogowym*[31] *i ustawa - Prawo o ruchu drogowym*[32]. Operatorzy inteligentnych systemów transportowych nie są zdefiniowani w żadnej z ustaw.

2.3 Sektor bankowości

Regulacja krajowa ma obejmować instytucje kredytowe. W polskim systemie prawa regulacje dotyczące tego sektora znajdują się w ustawie - *Prawo bankowe.* Zawarta w tej ustawie definicja instytucji kredytowej ma węższy zakres, niż to samo pojęcie w prawie UE. Szersza definicja tego samego pojęcia, oparta jednak na pojęciach z ustawy - *rawo bankowe,* znajduje się w u*stawie o nadzorze uzupełniającym nad instytucjami kredytowymi, zakładami ubezpieczeń, zakładami reasekuracji i firmami inwestycyjnymi wchodzącymi w skład konglomeratu finansowego*[33].

[26] Dz.U. z 2016 poz. 1727.
[27] Dz. U. z 2016 poz. 66.
[28] Dz. U. z 2013 poz. 1458.
[29] Dz. U. z 2017 poz. 1933.
[30] Dz. U. z 2016 poz. 281.
[31] Dz. U. z 2016 poz. 1907.
[32] Dz. U. z 2017 poz. 128.
[33] Dz.U. z 2016 poz. 1252.

2.4 Sektor infrastruktury rynków finansowych.

Regulacja ma objąć: operatorów systemu obrotu i kontrahentów centralnych. Omawiany sektor jest regulowany w polskim systemie prawa przez *ustawę o obrocie instrumentami finansowymi* [34]. Ustawa ta nie zawiera definicji operatorów systemu obrotów. Kontrahentów centralnych zdefiniowano poprzez odwołanie do rozporządzenia UE.

2.5 Sektor służby zdrowia

Regulacja ma obejmować ośrodki opieki zdrowotnej – świadczeniodawców. Regulacje dotyczące tego sektora w prawie polskim znajdują się w u*stawie o działalności leczniczej*[35]. Ustawa zawiera definicję „podmiotów wykonujących działalność leczniczą". Nie ma definicji „świadczeniodawcy" jako takiego, przyjąć można, że zakres tego pojęcia został wyczerpany w definicji podmiotów wykonujących działalność leczniczą.

2.6 Sektor zaopatrzenia w wodę pitną i jej dystrybucja

Regulacja ma obejmować dostawców i dystrybutorów „wody przeznaczonej do spożycia przez ludzi". Sektor ten uregulowany jest w polskim systemie prawnym w u*stawie o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków*[36]. *W* ustawie tej znajduje się definicja przedsiębiorstwa wodno-kanalizacyjnego, które można uznać za dostawcę wody przeznaczonej do spożycia przez ludzi w prawie unijnym.

2.7 Sektor infrastruktury cyfrowej

Regulacja ma obejmować punkty wymiany ruchu internetowego (IXP), dostawców usług DNS, rejestry nazw TLD. Powyższe pojęcia zostaną uregulowane wprowadzaną ustawą.

2.8 Dostawcy cyfrowi

Dostawcy cyfrowi są szczególnym typem usługodawcy świadczącym usługi drogą elektroniczną, o których mowa w ustawie *o świadczeniu usług drogą elektroniczną*. Ustawa o *świadczeniu usług drogą elektroniczną* nie obejmuje szczegółowych wymagań bezpieczeństwa teleinformatycznego i parametrów istotności incydentów zgłaszanych przez dostawców usług cyfrowych objętych zakresem dyrektywy 2016/1148/UE. Zostaną one określone w ramach

[34] Dz.U. z 2016 poz. 1636.
[35] Dz.U. z 2016 poz. 1638.
[36] Dz.U. z 2015 poz. 139.

procedury komitetowej przez Komitet do spraw Bezpieczeństwa Sieci i Systemów Informatycznych. Zgodnie z art. 16 ust. 8 dyrektywy ww. akt wykonawczy miał zostać przyjęty do dnia 9 sierpnia 2017 r., jednak według harmonogramu prac Komitetu zostanie on przyjęty do końca 2017 r.

3. Podmioty odpowiedzialne za cyberbezpieczeństwo na poziomie technicznym

W polskim prawie nie zostały do tej pory uregulowane obowiązki w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych i usług cyfrowych, zapewnienia cyberbezpieczeństwa systemów informacyjnych służących do świadczenia tych usług, ich monitorowania i zarządzaniem ryzykiem w sytuacjach standardowych, niezwiązanych ze zwalczaniem cyberprzestępczości, zagrożeniami o charakterze terrorystycznym bądź zarządzaniem kryzysowym. Nie zostały również określone sposoby realizacji usług obsługi incydentów, zasady współpracy podmiotów realizujących takie usługi oraz sposoby postępowania zespołów CSIRT poziomu krajowego w okresie trwania incydentów. Ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych*[37] jest ograniczona do zasad prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań. Przepisy ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* odnoszą się do działań związanych z zapobieganiem i zarządzaniem w sytuacjach kryzysowych. Ustawy regulujące pracę organów ścigania np. ustawa z dnia 6 kwietnia 1990 r. *o Policji*[38] czy też *Kodeks karny* obejmują kwestie związane z zapobieganiem i zwalczaniem przestępstw w cyberprzestrzeni. System ochrony cyberprzestrzeni w Polsce ma więc charakter zdecentralizowany, a kompetencje dotyczące cyberbezpieczeństwa mogą być realizowane przez Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Ministra Spraw Wewnętrznych i Administracji, Policję, Rządowe Centrum Bezpieczeństwa, czy też Ministra Cyfryzacji. Cyberbezpieczeństwem zajmują się także zespoły CSIRT utworzone przez operatorów telekomunikacyjnych oraz środowiska naukowo-badawcze. Wymienione podmioty realizują zadania w zakresie cyberbezpieczeństwa w sferze cywilnej, zwalczania cyberprzestępczości, zapobiegania zdarzeniom terrorystycznym i obrony narodowej.

Wraz ze zmianą ustawy o działach administracji rządowej w grudniu 2015 r., przypisującą do działu informatyzacja kompetencje z zakresu bezpieczeństwa cyberprzestrzeni, Ministerstwo

[37] Dz. U. z 2016 r. poz. 904
[38] Dz. U. z 2016 r. poz. 1782.

Cyfryzacji podjęło się działań związanych z uregulowaniem problematyki cyberbezpieczeństwa dla administracji jak i dla całej cywilnej części kraju. W nowym statucie Ministerstwa Cyfryzacji[39] utworzony został departament cyberbezpieczeństwa. Dodatkowo Ministerstwo Cyfryzacji od 2016 r. nadzoruje Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, podmiot realizujący wiele zadań dotyczących przeciwdziałania i reagowania na zagrożenia i incydenty w polskiej przestrzeni internetowej. W NASK funkcjonuje m.in. powstały jako pierwszy w Polsce zespół CSIRT – CERT Polska.

W lipcu 2016 r. w ramach NASK, powołane zostało Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). NC Cyber pomyślane jest jako centrum szybkiego reagowania na zagrożenia i zgłaszane incydenty w cyberprzestrzeni, a w razie ewentualnych ataków – podejmowania koniecznych działań we współpracy z ośrodkami w kraju i za granicą w celu przeanalizowania natury, sposobu, zasięgu incydentu i wymiany informacji w celu ostrzeżenia kluczowych sektorów i instytucji i wydania rekomendacji postepowania w obliczu zagrożenia oraz koniecznych działań minimalizujących skutki. Centrum operacyjne NC Cyber funkcjonuje w trybie 24/7 przez 365 dni w roku. NC Cyber oparte jest na kilku filarach: operacyjnym, analitycznym badawczo-rozwojowym, szkoleniowym oraz obszarze polityk i standardów. Założeniem powołania NC Cyber była dalsza rozbudowa funkcji operacyjnych i analityczno-technicznych, tak aby można było zarządzać bezpieczeństwem cyberprzestrzeni w krytycznych dla państwa i gospodarki obszarach działalności oraz budowa kompetencji w obszarze strategicznym.

Podmioty publiczne i prywatne mogą współpracować z NC Cyber na podstawie zawartych porozumień w zakresie cyberbezpieczeństwa, mogą również delegować swoich przedstawicieli do bieżącej współpracy. Porozumienia o współpracy zostały już podpisane z ok. 40 podmiotami, przedstawicielami sektora telekomunikacyjnego, finansowego (banków i instytucji finansowych), energetycznego, kolejowego, dostawcami usług cyfrowych. Zostały zbudowane kanały komunikacji pomiędzy uczestniczącymi podmiotami (strefa partnera, system informatyczny).

Przewiduje się, że po wejściu w życie ustawy NASK-PIB będzie realizował zadania CSIRT NASK tj. Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego przy wykorzystaniu dotychczasowej struktury organizacyjnej NASK–PIB, w tym NC Cyber. W efekcie w ramach NASK-PIB, będzie nadal działał pion NC Cyber, który realizując swoją dotychczasową funkcję, będzie wykonywał ustawowe zadania CSIRT NASK w oparciu o nabyte już doświadczenia.

[39] M.P. z 2015 r., poz. 1290.

Ustawa zobowiązując ministra właściwego do spraw informatyzacji do realizacji funkcji operacyjnych i technicznych w krajowym systemie cyberbezpieczeństwa dopuszcza możliwość delegacji uprawnień do realizacji tych funkcji jednostkom mu podległym lub przez niego nadzorowanym. W przyszłości w ramach zadań delegowanych zostanie również uruchomiony system teleinformatyczny służący wymianie o zagrożeniach i incydentach współpracujących podmiotów, prowadzeniu rejestru incydentów, wspierający analizę ryzyka na poziomie krajowym, dystrybuujący ostrzeżenia i rekomendacje techniczne.

4. Organy właściwe, warstwa strategiczno-polityczna krajowego systemu cyberbezpieczeństwa

Dyrektywa 2016/1148/UE zobowiązuje państwa członkowskie do wyznaczenia organów właściwych ds. cyberbezpieczeństwa, odpowiedzialnych za monitorowanie stosowania jej przepisów w sektorach objętych jej zakresem stosowania. Z uwagi na różnice w krajowych strukturach zarządzania, państwa członkowskie mogą wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z cyberbezpieczeństwem operatorów usług kluczowych i dostawców usług cyfrowych. W przypadku wyznaczenia kilku organów właściwych państwa członkowskie są zobowiązane wyznaczyć krajowy pojedynczy punkt kontaktowy odpowiedzialny za wymianę informacji w kwestiach związanych z cyberbezpieczeństwem oraz współpracę transgraniczną na poziomie Unii. W Polsce nie ma przepisów ustawowych określających szczegółowy zakres kompetencji organów w obszarze cyberbezpieczeństwa w odniesieniu do wskazanych w dyrektywie sektorów. *Krajowe Ramy Polityki Cyberbezpieczeństwa* przewidują określenie zakresu odpowiedzialności, obowiązków i uprawnień uczestników systemu, sposobów wzajemnego oddziaływania na innych uczestników systemu. *Krajowe Ramy* zakładają w szczególności określenie kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.

Projektowana ustawa nie jest jedynym działaniem zmierzającym do rozwoju krajowego systemu cyberbezpieczeństwa. Służą temu również dokumenty strategiczne i programowe takie jak: *Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, czy przygotowywany *Plan działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa*. Jak już wspomniano na wstępie zamierzeniem wynikającym z uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie *Krajowych Ram Polityki Cyberbezpieczeństwa*

Rzeczypospolitej Polskiej na lata 2017-2022 jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów infrastruktury krytycznej, usług kluczowych, dostawców usług cyfrowych, administracji publicznej, a także obywateli na ryzyko wynikające z zagrożeń występujących lub mogących wystąpić w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym w cyberprzestrzeni.

Krajowe Ramy przewidują przyjęcie w terminie do sześciu miesięcy od przyjęcia *Planu działań* zawierającego zestawienie projektów szczegółowych realizowanych przez poszczególne resorty/podmioty. Tym samym *Plan działań* będzie obejmować działania o charakterze legislacyjnym, projekty związane z budową systemów informacyjnych służących bieżącemu zarządzaniu cyberbezpieczeństwem, projekty o charakterze organizacyjnym jak ćwiczenia, treningi i testy, czy też działania ciągłe związane choćby z rozbudową polskiego potencjału technologicznego i dotyczące udziału Polski we współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa. W ramach realizacji *Krajowych Ram Polityki Cyberbezpieczeństwa* przygotowano i rozesłano w ramach prekonsultacji do poszczególnych ministerstw projekt ustawy o krajowym systemie cyberbezpieczeństwa. Opracowana została koncepcja funkcjonalna projektu Narodowa Platforma Cyberbezpieczeństwa, w tym centralna warstwa analityczna, przeprowadzono ćwiczenia z zakresu cyberbezpieczeństwa CEREX, jak również we współpracy z Ministerstwem Rozwoju rozpoczęto realizację projektu Cyberpark ENIGMA.

III. Opis proponowanych zmian – przewidywane skutki prawne wejścia aktu w życie

Projektowana ustawa ma na celu określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakresu oraz trybu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Jak zostało wskazane powyżej, obecnie brak jest przepisów służących zapewnieniu bezpieczeństwa teleinformatycznego i ciągłości świadczonych usług cyfrowych i usług kluczowych w sektorach usług kluczowych dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienionych w dyrektywie 2016/1148/UE w sytuacjach standardowych, niezwiązanych ze zwalczaniem cyberprzestępczości, zagrożeniami o charakterze terrorystycznym bądź zarządzaniem kryzysowym. Nie ma ustanowionych obowiązków w zakresie zarządzania ryzykiem, stosowania

zabezpieczeń, zgłaszania i obsługi incydentów, objęcia świadczonych usług systemem monitorowania w trybie ciągłym. W szczególności nie zostały uregulowane sposoby realizacji usług obsługi incydentów, zasad współpracy i sposobów postępowania zespołów CSIRT poziomu krajowego, realizujących takie usługi między sobą oraz wymianę informacji na potrzeby organów państwowych. Ponadto nie został określony szczegółowy zakres kompetencji organów administracji w obszarze cyberbezpieczeństwa do wskazanych w dyrektywie 2016/1148/UE sektorów. Projektowany akt będzie więc pierwszym dokumentem, który określi zasady funkcjonowania krajowego systemu cyberbezpieczeństwa.

Projekt ustawy definiuje podstawowe pojęcia niezbędne dla krajowego systemu cyberbezpieczeństwa. W obecnym stanie prawnym brak normatywnych definicji sprawia, że obszar ten jest zarazem niedostatecznie identyfikowany, jak i regulowany. Projektowane definicje są zgodne z treścią dyrektywy 2016/1148/UE, co pozwoli również ocenić osiągnięcie celów tej dyrektywy i *Krajowych Ram Polityki Cyberbezpieczeństwa*. Projektowana ustawa wprowadza do polskiego porządku prawnego nowe pojęcia takie m.in. CSIRT, obsługa incydentu, cyberbezpieczeństwo, system informacyjny, operator usługi kluczowej, usługa cyfrowa, różne kategorie incydentów.

Wypełniając dyspozycje, o których mowa w dyrektywie 2016/1148/UE projekt ustawy określa obowiązki dla operatorów usług kluczowych dotyczące wdrożenia efektywnego systemu zarządzania bezpieczeństwem, obejmującego m.in. zarządzanie ryzykiem, procedury i mechanizmy zgłaszania i postępowania z incydentami, organizację struktur na poziomie operatora. W załączniku do ustawy znajdą się natomiast wszystkie potencjalne kategorie podmiotów w poszczególnych sektorach gospodarki i działalności państwa, z których mogą być wyłaniani operatorzy usług kluczowych.

Jedną z najistotniejszych części proponowanych zmian jest określenie w projektowanej ustawie systemu reagowania na incydenty i włączenie w ten proces wszystkich zainteresowanych podmiotów. Istotą systemu reagowania na incydenty jest jego kompletność (ustanowienie we wszystkich kluczowych sektorach), transparentność i kompleksowość. Po pierwsze zakłada się określenie zadań CSIRT-ów poziomu krajowego, odpowiedzialnych za przeciwdziałanie zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa państwa, a także koordynację obsługi poważnych incydentów. Po drugie ustawa przewiduje włączenie aspektów cyberbezpieczeństwa do sfery zarządzania państwem. CSIRT-y poziomu krajowego informują się wzajemnie oraz informują Rządowe Centrum Bezpieczeństwa (zwane dalej „RCB") o incydencie, który może spowodować

wystąpienie sytuacji kryzysowej. Dodatkowo ustawa przewiduje utworzenie Zespołu do spraw Krytycznych Incydentów jako organu pomocniczego, powoływanego w sprawach obsługi i koordynacji krytycznych incydentów na poziomie krajowych CSIRT i RCB. Projekt zakłada również w przyszłości przypisanie nowych obowiązków ministrowi właściwemu do spraw informatyzacji realizującemu najważniejsze funkcje techniczne, na potrzeby krajowego systemu cyberbezpieczeństwa. Związane są one z prowadzeniem systemu teleinformatycznego wykorzystywanego do zgłaszania i obsługi incydentów, do szacowania ryzyka teleinformatycznego na poziomie krajowym oraz do ostrzegania o zagrożeniach cyberbezpieczeństwa.

Projekt określa zasady dotyczące sposobu przekazywania do publicznej wiadomości komunikatów nt. cyberbezpieczeństwa, o ile przekazywanie tych informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców.

Projekt ustawy ustanawia organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych w sektorach wymienionych w dyrektywie 2016/1148/UE. Organy właściwe są elementem krajowego systemu cyberbezpieczeństwa odpowiedzialnym również za opracowywanie we współpracy z CSIRT-ami wytycznych bezpieczeństwa teleinformatycznego w wymiarze sektorowym. Jednocześnie projekt ustawy ustanawia pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa prowadzony przez ministra właściwego ds. informatyzacji. Według zamierzeń pojedynczy punkt kontaktowy realizowałby funkcje swoistego „łącznika" i zajmowałby się wymianą informacji na rzecz organów właściwych, organów władz publicznych i CSIRT-ów. Pojedynczy punkt kontaktowy pełnić będzie funkcje łącznika na potrzeby reprezentacji RP w Grupie Współpracy, współpracy z Komisją Europejską, współpracy między organami właściwymi w Rzeczpospolitej Polskiej i organami właściwymi państw członkowskich Unii Europejskiej, współpracy pomiędzy organami władzy publicznej w Rzeczpospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej. Projektowana regulacja określi również ustawowe zasady realizacji i tworzenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Szczegółowy opis proponowanych zmian

Rozdział 1: Przepisy ogólne

W przepisach ogólnych został określony słowniczek pojęć ustawowych , katalog podmiotów tworzących krajowy system cyberbezpieczeństwa oraz cele projektowanej ustawy. Definiowane pojęcia, co do zasady nie pojawiają się w innych aktach prawnych, a ich określenie na poziomie ustawy pozwoli na dokładne wyznaczenie ram przedmiotowych projektowanego aktu. Najważniejsze pojęcia zdefiniowane w art. 2 projektu zostały przedstawione poniżej:

1. **CSIRT** – zgodnie z wprowadzaną przez ustawę definicją, CSIRT jest Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym. Projektowana ustawa wyodrębnia następujące CSIRT:
    a. **CSIRT MON** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Ministra Obrony Narodowej,
    b. **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy,
    c. **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.
2. **cyberbezpieczeństwo –** projektodawca zdefiniował cyberbezpieczeństwo, jako stan systemów informacyjnych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne.
3. **incydent –** zgodnie z definicją znajdującą się w projekcie ustawy jest nim każdy incydent zakwalifikowany jako krytyczny, poważny, istotny lub zwykły.
4. **poważny incydent –** zgodnie z definicją stworzoną przez projektodawcę, poważnym incydentem jest taki incydent zwykły, który powoduje lub może spowodować krytyczne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej albo usługi świadczonej przez podmiot publiczny.
5. **incydent krytyczny –** to incydent poważny, incydent istotny lub incydent zwykły, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, zaufania do instytucji publicznych, praw i wolności obywatelskich lub zdrowia publicznego.
6. **system informacyjny** – projektodawca zdefiniował system informacyjny jako system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej. Definicja systemu teleinformatycznego została z kolei zaczerpnięta z obowiązującej

ustawy (ustawa z dnia 17 lutego 2005 r. – o informatyzacji działalności podmiotów realizujących zadania publiczne Dz.U. z 2017 r. poz. 570).

7. **obsługa incydentu** – projektodawca definiuje ją jako czynności umożliwiające wykrywanie, klasyfikowanie, analizowanie, priorytetyzację, podejmowanie działań naprawczych oraz ograniczenie skutków incydentu.

W artykule 3 zostały określone cele krajowego systemu cyberbezpieczeństwa, którymi będą niezakłócone świadczenie usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Jednocześnie artykuł ten wprowadza zasadę, że informacje o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa mogą być przekazywane przez te podmioty w niezbędnym zakresie do publicznej wiadomości w przypadku, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę trwającego incydentu lub w przypadku gdy ujawnienie incydentu z innych względów jest w interesie publicznym. Przekazywanie niezbędnych informacji do publicznej wiadomości nie narusza przepisów o ochronie tajemnic oraz o ochronie danych osobowych, wyłączone jest również stosowanie ustawy *o dostępie do informacji publicznej*.

Artykuł 4 wskazuje podmioty, które obejmuje krajowy system cyberbezpieczeństwa, a więc podmioty zobowiązane, podmioty realizujące techniczne, organizacyjne i administracyjno-regulacyjne zadania w systemie, jednostki sektora finansów publicznych. System będzie obejmować operatorów usług kluczowych, dostawców usług cyfrowych, przedsiębiorców telekomunikacyjnych, zespoły CSIRT poziomu krajowego, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa oraz jednostki administracji publicznej i sektora finansów publicznych objęte zakresem ustawy.

Rozdział 2: Usługi kluczowe i operatorzy usług kluczowych

Artykuł 5 projektu ustawy wprowadza do porządku prawnego pojęcie operatora usługi kluczowej. Projektodawca wzoruje się na definicji z dyrektywy 2016/1148/UE z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*. Będą nimi przedsiębiorstwa bądź podmioty

publiczne należące do jednego z sektorów wymienionych w załączniku do ustawy, które świadczą usługę kluczową wymienioną w wykazie usług kluczowych, jej świadczenie zależy od systemów teleinformatycznych, a incydent miałby istotny skutek zakłócający dla jej świadczenia. Wykaz usług kluczowych miałby być określony rozporządzeniem Rady Ministrów (art. 6 projektu), natomiast progi istotności skutku zakłócającego dla świadczenia usług kluczowych uchwałą Rady Ministrów i miałyby charakter niejawny (art. 7 projektu). Projektodawca przewidział tryb decyzji administracyjnych w sprawach identyfikacji operatorów usług kluczowych przez organ właściwy dla danego sektora. W przypadku zaprzestania spełniania przez podmiot warunków będących podstawą wydania decyzji administracyjnej, przewidziane zostało wydanie decyzji o wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej.

Artykuł 8 projektowanej ustawy zawiera kompetencję ministra właściwego do spraw informatyzacji do prowadzenia wykazu operatorów usług kluczowych. Wykaz ten ma zostać utworzony z uwzględnieniem podziału na sektory, podsektory i rodzaje podmiotów, który wprowadza implementowana dyrektywa. Wpisanie do wykazu lub wykreślenie z niego będzie czynnością materialno-techniczną, realizowaną w oparciu o decyzje administracyjne organów właściwych, w zakresie identyfikacji operatorów usług kluczowych we właściwych sektorach. Przepis ten określa również tryb udostępniania informacji i katalog podmiotów, którym będą udostępniane informacje z wykazu. Zgodnie z art. 9 operator usługi kluczowej, w terminie 14 dni od każdej zmiany danych wpisanych do wykazu operatorów usług kluczowych ma obowiązek poinformować o tym organ właściwy. Informacje te przekazywane są niezwłocznie ministrowi właściwemu do spraw informatyzacji.

W artykule 10 określone zostały obowiązki operatorów usług kluczowych dotyczące stosowania zabezpieczeń systemów informacyjnych służących do świadczenia usług kluczowych, zarządzania ryzykiem i realizowania procedur dotyczących zarządzania incydentem. Zgodnie z treścią projektowanego przepisu operatorzy są odpowiedzialni za zapewnienie bezpieczeństwa świadczonych usług kluczowych oraz ciągłości ich świadczenia. Ich głównym obowiązkiem jest wdrożenie systemu zarządzania bezpieczeństwem. W ust. 2 tego artykułu zamieszczony został także minimalny zakres, jaki ma obejmować tworzony system zarządzania bezpieczeństwem.

Artykuł 11 precyzuje obowiązki operatorów usług kluczowych związanych z opracowywaniem dokumentacji dotyczącej cyberbezpieczeństwa systemów teleinformatycznych wykorzystywanych do świadczenia usług kluczowych. Zawiera

upoważnienie do wydania przez Radę Ministrów rozporządzenia określającego sposób tworzenia i aktualizacji powyższej dokumentacji. Przepis zawiera wyłączenie w zakresie realizacji tego obowiązku przez właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o *zarządzaniu kryzysowym*, którzy realizują obowiązki tego typu na podstawie tej ustawy. Powyższe rozwiązanie ogranicza tym samym obowiązki administracyjne tworzenia dokumentacji dotyczącej cyberbezpieczeństwa, o ile dany operator usług kluczowych został już objęty obowiązkami, o których mowa w przepisach o zarządzaniu kryzysowym.

Na operatorów usług kluczowych zostaną nałożone obowiązki związane ze zgłaszaniem i obsługą incydentu (art. 12). Operatorzy będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. Przepisy nakładają obowiązki zgłaszania incydentów poważnych niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia. Operator w procesie obsługi incydentu będzie zobowiązany zapewniać, w razie potrzeby, dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT poziomu krajowego, a także informować właściwy CSIRT o usunięciu podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu. W projektowanych przepisach znajduje się upoważnienie ustawowe do określenia progów uznania incydentu za poważny w poszczególnych sektorach określonych w załączniku do ustawy. Uzupełnieniem pakietu przepisów dotyczących notyfikacji incydentów jest art.13 zawierający określenie zakresu danych zawartych w zgłoszeniu. Zgodnie z art. 14 notyfikacja incydentów będzie mogła odbywać się za pośrednictwem systemu teleinformatycznego, prowadzonego od 1 stycznia 2021 r. przez ministra właściwego ds. informatyzacji.

Artykuł 15 zawiera zamknięty katalog obowiązków o charakterze organizacyjnym, które musi realizować operator usług kluczowych. Projektodawca wymienia – wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo oraz zapewnienie użytkownikom usługi kluczowej świadczonych przez danego operatora dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczeń. Projektodawca dopuszcza możliwość budowy wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, bądź „outsourcingu" usług z zakresu cyberbezpieczeństwa. Celem zapewnienia świadczenia przez podmioty świadczące usług z zakresu cyberbezpieczeństwa na rzecz operatorów usług kluczowych na odpowiednim poziomie ustawa określa wymagania dla takich podmiotów. Zakłada się, że wymienione podmioty winny dysponować odpowiednim

potencjałem organizacyjno-technicznym, pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi, stosować zabezpieczenia w celu zapewnienia dostępności, integralności, poufności i rozliczalności przetwarzanych informacji z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów. Sposób realizacji tych wymagań zostanie określony w rozporządzeniu ministra właściwego do spraw informatyzacji.

Artykuł 16 określa zasady, tryb i cele audytów bezpieczeństwa teleinformatycznego przeprowadzanych przez operatorów usług kluczowych. Operatorzy usług kluczowych są zobowiązani do przeprowadzania audytów bezpieczeństwa teleinformatycznego co najmniej raz nad dwa lata. Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. Celem audytu jest potwierdzenie, na podstawie przeprowadzonej analizy ryzyka, że operatorzy usług kluczowych spełniają wymogi określone w ustawie. Z przeprowadzonego audytu audytor sporządza pisemne sprawozdanie, przekazywane audytowanemu operatorowi usługi kluczowej. Konstrukcja przepisów umożliwia wykorzystanie jego wyników przez organy właściwe i dyrektora Rządowego Centrum Bezpieczeństwa. Na podstawie wyników audytu organ właściwy może wydawać wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych w audycie uchybień. W przypadku, w którym operator usługi kluczowej jest również podmiotem realizującym obowiązki na podstawie ustawy *o zarządzaniu kryzysowym* polecenia wydawane są po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa.

Rozdział 3: Dostawcy usług cyfrowych

Definicja dostawcy usług cyfrowych znajduje się w słowniczku ustawowym i opiera się na regulacjach ustawy z dnia 18 lipca 2002 r. – o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), natomiast artykuł 17 zawiera przepisy jurysdykcyjne odnoszące się do dostawców usług cyfrowych. Wskazuje tym samym jacy dostawcy cyfrowi będą podlegać przepisom w Polsce i organowi właściwemu w Polsce – ministrowi właściwemu ds. informatyzacji. Przepisy formułują ogólne obowiązki podjęcia przez dostawców usług cyfrowych środków organizacyjnych i technicznych na rzecz bezpieczeństwa systemów teleinformatycznych służących do świadczenia usług cyfrowych. Dostawcy usług cyfrowych są odpowiedzialni za zapewnienie cyberbezpieczeństwa świadczonych przez siebie usług

cyfrowych (art. 18), oraz zobowiązani są do informowania CSIRT NASK o incydencie istotnym, w tym dotyczącym dwóch lub większej liczby państw członkowskich UE (art. 19). Artykuł 20 zawiera natomiast katalog obowiązków nakładanych na dostawców usług cyfrowych, związanych ze zgłaszaniem i obsługą incydentów istotnych. Natomiast w art. 21 określone zostały elementy jakie powinno spełniać zgłoszenie incydentu istotnego.
Szczegółowym uzupełnieniem przepisów dotyczących stosowanych zabezpieczeń teleinformatycznych i obowiązków w zakresie zgłaszanych incydentów będzie wydana do końca 2017 r. decyzja wykonawcza Komisji Europejskiej 2017/XX/UE. Decyzja będzie zawierać katalog szczegółowych wymagań służących tworzeniu zabezpieczeń systemów teleinformatycznych, dotyczących m.in. bezpieczeństwa fizycznego i środowiskowego, kontroli dostępu, procedur zgłaszania incydentów, zapewnienia ciągłości działania. Decyzja określi jakie działania należy podjąć celem monitorowania, audytów i testowania wdrożonych zabezpieczeń. Będzie zawierać parametry określające, jakie incydenty z zakresu cyberbezpieczeństwa będą musiały być zgłaszane do CSIRT NASK.

Rozdział 4: Podmioty publiczne

Przepisy rozdziału definiują obowiązki podmiotów publicznych objętych zakresem ustawy. Podmioty publiczne objęte wymogami z zakresu cyberbezpieczeństwa będą zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obsługi i zgłaszania incydentów (art. 25) oraz udostępniania wiedzy na temat stosowania odpowiednich zabezpieczeń przed zagrożeniami cyberbezpieczeństwa. Podmioty publiczne będą włączone do krajowego systemu cyberbezpieczeństwa dzięki ustanowionemu obowiązkowi zgłaszania incydentów, jak również innych informacji istotnych z punktu widzenia cyberbezpieczeństwa państwa, czyli także o zagrożeniach cyberbezpieczeństwa, dotyczących szacowania ryzyka teleinformatycznego, podatnościach na incydenty systemów informacyjnych, o wykorzystywanych technologiach informatycznych. W przypadku podmiotów publicznych, wobec których została wydana decyzja o uznaniu za operatora usług kluczowych, miałyby zastosowanie przepisy rozdziału 2 ustawy definiujące m.in. obowiązki w zakresie wdrożenia systemu zarządzania bezpieczeństwem, opracowywania dokumentacji związanej z cyberbezpieczeństwem oraz przeprowadzania audytów bezpieczeństwa teleinformatycznego przez akredytowane jednostki certyfikujące.

Rozdział 5: Zadania CSIRT

Przepisy rozdziału ustanawiają strukturę CSIRT-ów poziomu krajowego i porządkują kwestię zakresu odpowiedzialności poszczególnych CSIRT-ów. Przyjęte rozwiązanie ma na celu jednoznaczne umocowanie w obowiązujących przepisach zasady współpracy takich CSIRT-ów. Projektodawca zakłada równocześnie, że z uwagi na usytuowanie CSIRT – jest to poziom krajowy – podmioty powyższe spełniają wymogi określone w załączniku nr 1 do dyrektywy 2016/1148/UE określającym minimalne wymogi dla CSIRT poziomu krajowego. Zgodnie z projektem CSIRT poziomu krajowego realizują zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniają koordynację obsługi poważnych incydentów. CSIRT-y poziomu krajowego monitorują zagrożenia i incydenty na poziomie krajowym, odpowiadają za szacowanie ryzyka, przekazują podmiotom tworzącym krajowy system cyberbezpieczeństwa wczesne ostrzeżenia, informacje dotyczące incydentów i ryzyk, a także rekomendacje działań minimalizujących skutki incydentu. CSIRT-y poziomu krajowego dokonują klasyfikacji incydentów jako krytyczne oraz koordynują ich obsługę, a w razie potrzeby zapewniają wsparcie w obsłudze incydentu poważnego i krytycznego operatorom usług kluczowych lub dostawcom usług cyfrowych. CSIRT-y poziomu krajowego będą odpowiedzialne za przyjmowanie zgłoszeń o incydentach z innych państw, w tym państw członkowskich Unii Europejskiej i dokonywanie dystrybucji tych informacji do pozostałych CSIRT i do Pojedynczego Punktu Kontaktowego.

Zadania CSIRT-ów poziomu krajowego uwzględniają przypisane poszczególnym CSIRT zakresy odpowiedzialności na potrzeby zarządzania bezpieczeństwem państwa. I tak do CSIRT GOV należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez organy państwowe, w tym Kancelarię Sejmu, Kancelarię Senatu, Kancelarię Prezydenta Rzeczypospolitej Polskiej, Krajową Radę Radiofonii i Telewizji, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, organy administracji rządowej, sądy i trybunały, prokuraturę, organy kontroli państwowej, Narodowy Fundusz Zdrowia, Zakład Ubezpieczeń Społecznych, Kasę Rolniczego Ubezpieczenia Społecznego. Zakres właściwości CSIRT GOV obejmuje również podmioty objęte ustawą *o zarządzaniu kryzysowym*, czyli podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne są wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ww. ustawy. Do zadań CSIRT NASK będzie należeć obsługa lub koordynacja obsługi incydentów zgłaszanych przez państwowe osoby prawne, utworzone na

podstawie odrębnych ustaw w celu wykonywania zadań publicznych w tym przedsiębiorstwa, banki i spółki prawa handlowego, operatorów usług kluczowych i dostawców usług cyfrowych, których systemy teleinformatyczne lub sieci teleinformatyczne nie zostały wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, osoby fizyczne, część jednostek sektora finansów publicznych (m.in. agencje wykonawcze, państwowe instytucje kultury, jednostki podległe i nadzorowane przez organy administracji rządowej, jednostki sfery samorządowej). Do zadań CSIRT MON będzie należeć obsługa incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa.

Mając na uwadze charakter cyberprzestrzeni przejawiający się między innymi brakiem występujących w niej granic, a przez to przenikaniem oddziaływań z jednego sektora na gospodarki narodowej na inne, ustawa określa zasady wymiany informacji pomiędzy poszczególnymi CSIRT poziomu krajowego i zobowiązuje do przyjęcia jednolitych procedur w zakresie obsługi incydentów i szacowania ryzyka. W związku z opisanym powyżej brakiem granic w cyberprzestrzeni może powstać potrzeba zmiany zakresu odpowiedzialności podmiotowej poszczególnych CSIRT, co będzie możliwe poprzez zawieranie stosownych porozumień pomiędzy zespołami CSIRT poziomu krajowego. W celu zachowania transparentności porozumienia będą publikowane w Dziennikach Urzędowych.

Art. 29 zapewnia uspójnienie przepisów projektowanej ustawy z innymi aktami prawnymi rangi ustawowej, a w szczególności z przepisami ustawy z dnia 10 czerwca 2016 r. o *działaniach antyterrorystycznych*[40], ustawy z dnia 21 listopada 1967 r. *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej*[41] oraz ustawy z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*[42].

Przepisy art. 30 ust. 1 – 3 nakładają na właściwe CSIRT-y obowiązek informowania innych państw członkowskich UE o incydentach zaistniałych na terytorium Polski, o ile incydenty te miałyby oddziaływanie w tych innych państwach członkowskich, a także zobowiązuje do przekazywania informacji, które mogą być pomocne w złagodzeniu skutków incydentu poza

[40] Dz. U. 2016 poz. 904.
[41] Dz. U. z 2017 r. poz. 1430.
[42] Dz. U. z 2017 r. poz. 1932.

granicami Polski. Przepis ust. 4 dopuszcza możliwość podania do publicznej wiadomości informacji związanych z incydentem, po uprzedniej konsultacji z operatorem usługi kluczowej zgłaszającym incydent. Konsekwentnie art. 31 nakłada na CSIRT NASK obowiązek informowania innych państw członkowskich UE o transgranicznym charakterze incydentu w obszarze usług cyfrowych.

Art. 32 ustanawia mechanizm współpracy CSIRT poziomu krajowego w celu opracowania informacji na potrzeby tworzonego przez dyrektora Rządowego Centrum Bezpieczeństwa raportu o zagrożeniach bezpieczeństwa państwa.

Art. 33 umożliwia obsługiwanie przez CSIRT NASK innych incydentów niż pochodzące od podmiotów wymienionych w art. 28 ust. 6, zapewniając przy tym, że obsługa takich incydentów nie zaburzy realizacji przez ten CSIRT działań na rzecz podmiotów wymienionych w powyższym przepisie.

Art 34 umożliwia uczestniczenie CSIRT-ów poziomu krajowego w bezpośrednim usuwaniu skutków incydentów poważnych, incydentów krytycznych lub incydentów o charakterze ponadsektorowym i transgranicznym. W trakcie obsługi takich incydentów CSIRT poziomu krajowego może zwracać się do organu właściwego o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej do określonego zachowania, które doprowadzi do ograniczenia skutku incydentu i zapobiegnie mu w przyszłości. Przepis ust. 4 zobowiązuje CSIRT, operatorów usług kluczowych i dostawców usług cyfrowych do współpracy z organami ścigania, a przepis ust. 5 zobowiązuje w/w podmioty do współpracy z organem ochrony danych osobowych, o ile w trakcie incydentu naruszone zostały przepisy w zakresie ochrony danych osobowych.

Art. 35 określa, iż CSIRT-y poziomu krajowego wraz z ministrem właściwym ds. informatyzacji i dyrektorem RCB mogą w zakresie i w celu niezbędnym do realizacji zadań wynikających z projektu ustawy przetwarzać dane, w tym dane osobowe.

Art. 36 określa sposób współpracy CSIRT poziomu krajowego z Rządowym Centrum Bezpieczeństwa w sytuacji gdy incydent może przekształcić się w kryzys w rozumieniu ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*. CSIRT poziomu krajowego może wystąpić z rekomendacją zwołania Rządowego Zespołu Zarządzania Kryzysowego. Przepis umożliwia wymianę informacji pomiędzy CSIRT poziomu krajowego w sytuacji gdy incydent lub zagrożenie może dotyczyć podmiotów znajdujących się w zakresie kompetencji różnych CSIRT poziomu krajowego.

Przepisy art. 37 umożliwiają skuteczną koordynację działań poszczególnych CSIRT poziomu krajowego w przypadku skomplikowanych incydentów lub zagrożeń. Koordynację zapewnia się poprzez powołanie Zespołu do spraw Incydentów Krytycznych, który w szczególności może rekomendować zwołanie Rządowego Zespołu Zarządzania Kryzysowego lub rekomendować Szefowi ABW wnioskowanie o wprowadzenie stopni alarmowania CRP. Istotnym przepisem jest wskazanie na konieczność wyłonienia w drodze konsensusu jednego z CSIRT poziomu krajowego odpowiedzialnego za koordynację obsługi incydentu w przypadku gdy incydent dotyka podmiotów znajdujących się w kompetencji różnych CSIRT. Przepis określa także, że incydent o rozległym oddziaływaniu jest przesłanką obligatoryjnego zwołania posiedzenia Rządowego Zespołu Zarządzania Kryzysowego.

Rozdział 6: Organy właściwe do spraw cyberbezpieczeństwa

W rozdziale powyższym zostały określone organy właściwe dla poszczególnych sektorów wymienionych w dyrektywie 2016/1148/UE. Przyjęty w ustawie model regulacyjny zakłada poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym. Obowiązki o charakterze administracyjnym, regulacyjnym i kontrolnym zostały przypisane właściwym ministrom dla wymienionych w dyrektywie 2016/1148/WE sektorów, czyli sektora energetycznego, transportowego, bankowości i instytucji finansowych, zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej i dostawców cyfrowych (art. 38). W art. 39 został wskazany katalog zadań, który będą realizować organy właściwe. Zadania te obejmują prowadzenie analiz, wydawanie decyzji administracyjnych pod kątem uznania za operatora usług kluczowych, wygaśnięcia decyzji o uznaniu za operatora usług kluczowych, monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych we właściwych im sektorach. Organy właściwe mogą żądać od operatorów usług kluczowych przekazania określonych informacji niezbędnych do oceny bezpieczeństwa ich systemów teleinformatycznych, w tym dokumentów dotyczących polityki w zakresie cyberbezpieczeństwa, uzasadniając cel ich przekazania, a po dokonaniu ich oceny wydawać wiążące polecenia wprowadzenie środków zaradczych w odniesieniu do stwierdzonych nieprawidłowości

Organy właściwe przygotowują rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów.

Ustawodawca zakłada tutaj, że z uwagi na dynamizm środowiska normatywnego i specyfikę poszczególnych sektorów, organy właściwe określą w wytycznych szczegółowych w jaki sposób należy np. realizować obowiązki w zakresie wdrożenia systemu zarządzania bezpieczeństwem przez operatorów usług kluczowych z danego sektora. Ponadto, organy te mają też przewidzianą dyrektywą możliwość prowadzenia współpracy z właściwymi organami państw członkowskich Unii Europejskiej.

W artykule 40 projektodawca reguluje kwestie związane z transgranicznymi operatorami usług kluczowych. W tym kontekście, projektodawca nakłada na organy właściwe we współpracy z Pojedynczym Punktem Kontaktowym obowiązek bieżącego rozpoznawania potencjalnych transgranicznych operatorów usług kluczowych. Procedura uznania za transgranicznego operatora usługi kluczowej uwzględnia konieczność prowadzenia uzgodnień z organami właściwymi państw członkowskich Unii Europejskiej.

Rozdział 7: Zadania ministra właściwego do spraw informatyzacji

Ustawa określa nowe role ministra właściwego do spraw informatyzacji w ramach krajowego systemu cyberbezpieczeństwa. Artykuł 41 projektu ustawy nakłada na ministra właściwego do spraw informatyzacji realizację pakietu zadań o charakterze organizacyjnym i sprawozdawczym. Minister właściwy do spraw informatyzacji jest odpowiedzialny za przygotowanie i monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, realizacji planów działań na rzecz jej wdrożenia oraz prowadzenie polityki informacyjnej dotyczącej krajowego systemu cyberbezpieczeństwa. Minister właściwy ds. informatyzacji opracowuje roczne sprawozdania dotyczące poważnych incydentów zgłaszanych przez operatorów usług kluczowych oraz incydentów istotnych zgłaszanych przez dostawców usług cyfrowych. Z drugiej strony w ramach pełnienia funkcji Pojedynczego Punktu Kontaktowego minister właściwy do spraw informatyzacji będzie odpowiadać za zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, wymianę informacji na rzecz organów władz publicznych, organów właściwych w Polsce i za granicą, CSIRT, realizację obowiązków sprawozdawczych wobec Grupy Współpracy i Komisji Europejskiej.

Projektowany artykuł 42 zawiera regulacje dotyczące systemu teleinformatycznego prowadzonego przez ministra właściwego do spraw informatyzacji. Określa on funkcjonalności systemu, którypowinien umożliwiać zbieranie informacji o incydentach i zagrożeniach,

agregowanie i korelowanie pozyskanych informacji, aby określić ryzyko wystąpienia incydentu, ostrzegać o zagrożeniach cyberbezpieczeństwa, prognozować skutki materializacji zagrożeń, dystrybuować rekomendacje dotyczące działań technicznych. Zgodnie z przyjętymi rozwiązaniami użytkownikami systemu będą CSIRT poziomu krajowego, operatorzy usług kluczowych, dostawcy usług cyfrowych, Prezes Urzędu Komunikacji Elektronicznej. Informacje z systemu będą mogły być udostępniane na wniosek, o ile są one niezbędne do realizacji ustawowych zadań organom państwowym w związku z realizowanymi funkcjami, wynikającymi z innych regulacji, m.in. na rzecz zapobiegania zdarzeniom o charakterze terrorystycznym, z zarządzaniem kryzysowym czy zwalczaniem cyberprzestępczości. Informacje z systemu będą mogły być udostępniane również sądom i prokuraturze, organom właściwym na potrzeby realizowania funkcji nadzoru w zakresie bezpieczeństwa teleinformatycznego nad operatorami usług kluczowych, Przepisy precyzują zasady przetwarzania danych w systemie w świetle regulacji dotyczących ochrony danych, w tym ogólnego rozporządzenia o ochronie danych[43].

Przepisy rozdziału zawierają również upoważnienie ustawowe do wydania przez ministra właściwego do spraw informatyzacji rozporządzenia precyzującego sposób i tryb zakładania i obsługi konta użytkownika systemu teleinformatycznego, zakres uprawień użytkowników systemu oraz wymogów bezpieczeństwa teleinformatycznego, które muszą spełnić użytkownicy.

Przepisy art. 43 dopuszczają możliwość delegowania realizacji zadań o charakterze organizacyjnym i technicznym na jednostki podległe lub nadzorowane przez ministra właściwego do spraw informatyzacji.

W art. 44 określono, iż minister właściwy do spraw informatyzacji prowadzi Pojedynczy Punkt Kontaktowy, jak również określony został katalog jego zadań. Uregulowany został także zakres informacji przekazywanych przez PPK Grupie Współpracy (art. 45) oraz Komisji Europejskiej (art. 46).

Rozdział 8: Nadzór i kontrola

[43] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

W rozdziale 8 uregulowano kwestie związane z nadzorem i kontrolą. Systemem nadzoru, zgodnie z art. 47 objęte zostaną podmioty świadczące usługi z zakresu cyberbezpieczeństwa, operatorzy usług kluczowych oraz dostawcy usług cyfrowych.

W ustawie przewidziano rozdzielenie kompetencji nadzorczych z uwagi na charakter podmiotów podlegających nadzorowi. W zakresie podmiotów świadczących usługi z zakresu cyberbezpieczeństwa nadzór będzie pełnił minister właściwy do spraw informatyzacji. W ramach nadzoru minister właściwy do spraw informatyzacji będzie zapewniał przestrzeganie obowiązków dotyczących cyberbezpieczeństwa przewidzianych w ustawie, m.in. wymogu powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia odpowiednich umów z podmiotami profesjonalnie świadczącymi te usługi.

Z kolei nadzór w odniesieniu do operatorów usług kluczowych dotyczył będzie spełniania wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, związanych ze świadczonymi usługami kluczowymi. Nadzór ten będzie sprawowany przez organy właściwe.

Natomiast nadzór w odniesieniu do dostawców usług cyfrowych dotyczył będzie spełniania wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych i zgłaszania incydentów i sprawowany będzie przez organ właściwy dla dostawców cyfrowych.

W projekcie ustawy wskazano jakie uprawnienia w ramach nadzoru przysługiwały będą organom właściwym oraz ministrowi właściwemu do spraw informatyzacji. Warto zauważyć, że wskazane uprawnienia występują w sposób niezależny od siebie. Organy nadzorujące w ramach sprawowanego nadzoru mogą prowadzić kontrole a także stosować uprawnienia o charakterze władczym wobec kontrolowanych podmiotów, polegające na zobowiązaniu do usunięcia nieprawidłowości ustalonych w wyniku kontroli oraz nakładać administracyjne kary pieniężne. W określonych przypadkach, z uwagi na charakter naruszeń organy nadzoru będą mogły z pominięciem kontroli wszczynać postępowanie administracyjne w celu nałożenia administracyjnej kary pieniężnej.

W projekcie wskazano także, że do kontroli podmiotów będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyłączeniem art. 79. Powyższe oznacza, że nie będą miały zastosowania do tej kontroli przepisy dotyczące zawiadomienia o zamiarze wszczęcia kontroli. W opinii projektodawcy zastosowanie ww. przepisu mogłoby uniemożliwić rzetelne i przeprowadzone we właściwym czasie postępowanie kontrolne w zakresie przestrzegania przepisów dotyczących zapewnienia cyberbezpieczeństwa. Jednocześnie wskazano, że do podmiotów niebędących

przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Z uwagi na braki w ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej w zakresie dotyczącym sposobu prowadzenia kontroli w art. 49 – 53 projektu ustawy uregulowano niezbędne zagadnienia w tym zakresie.

W art. 49 w punktach od 1 do 5 wskazano zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zauważyć, że w celu uniknięcia sytuacji w której podmiot kontrolowany zwleka z wydaniem przepustki osobie przeprowadzającej kontrolę wskazano, że osoba prowadząca czynności kontrolne ma prawo do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki.

Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli. W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, iż protokół podpisują osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany, osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole. W celu zapewnienia skutecznego przeprowadzenia czynności kontrolnych przewidziano w projekcie możliwość skorzystania z pomocy funkcjonariuszy innych organów kontroli lub Policji. Przewidziano także możliwość skorzystania z udziału eksperta w przeprowadzeniu kontroli, którego wiadomości specjalne, mogą istotnie wpłynąć na jej wynik.

W art. 54 wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie, poinformować organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń lub przyczynie ich niewykonania. Wskazana powyżej regulacja jest istotna z punktu widzenia regulacji zwartych w rozdziale 10 dotyczących nakładania administracyjnych kar pieniężnych. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej.

Rozdział 9: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Niniejszy rozdział zawiera regulacje dotyczące wydawania przez Radę Ministrów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Przepisy tego artykułu zawierają wyliczenie przykładowe elementów treści, jakie mają znaleźć się w dokumencie. Zgodne z projektem Strategia uwzględnia w szczególności cele i priorytety w zakresie cyberbezpieczeństwa, podmioty zaangażowane w jej wdrażanie i realizację, środki służące realizacji jej celów, środki w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym. Strategia ma też uwzględniać podejście do oceny ryzyka, działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Przepisy rozdziału wskazują okres na jaki jest przyjmowana Strategia oraz zasady współdziałania podmiotów włączonych w proces jej opracowywania,

Rozdział 10: Przepisy o karach pieniężnych

W rozdziale 10 zawarto przepisy regulujące nakładanie administracyjnych kar pieniężnych. Przewiduje się, iż organ właściwy dla danego sektora będzie mógł nałożyć na operatorów usług kluczowych administracyjną karę pieniężną za brak realizacji obowiązków wynikających z ustawy. Przykładowo administracyjną karą pieniężną będzie mógł zostać ukarany operator usługi kluczowej, który nie wyznaczył osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych, uniemożliwia lub utrudnia osobie przeprowadzającej czynności kontrolnych, nie przeprowadził audytu bezpieczeństwa teleinformatycznego albo mimo nałożenia takiego obowiązku nie realizuje wniosków z niego wynikających.

Zgodnie z zasadą proporcjonalności wysokość kar administracyjnych została odpowiednio zróżnicowana. Za niewypełnianie obowiązków administracyjnych tj. zgłoszenie zmiany danych, za brak podejmowania środków zaradczych przewiduje się najniższe kary do 1 do 5 tysięcy złotych. Z kolei z tytułu nie wypełniania obowiązków o istotnym charakterze z punktu widzenia cyberbezpieczeństwa przewiduje się odpowiednio wyższe. Przykładowo od 10 tysięcy złotych z tytułu nie wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług u operatora, po karę do 50 tysięcy złotych za nie przeprowadzenie audytu,

aż do kary wysokości 100 tysięcy złotych za brak nie wdrożenia systemu zarządzania bezpieczeństwem.

Oddzielnie należy wspomnieć o administracyjnej karze pieniężnej w wysokości do 200 tysięcy złotych, którą może nałożyć organ właściwy dla danego sektora na operatora usługi kluczowej, który uporczywie narusza przepisy ustawy powodując bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, bądź zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych.

W niektórych przypadkach może dojść do sytuacji w której uporczywe naruszenie przepisów ustawy, o którym mowa powyżej będzie też stanowiło naruszenie przepisów prawa karnego. Przykładowo, gdy naruszenie przepisów ustawy będzie skutkowało narażeniem na niebezpieczeństwo życia lub zdrowia, zgodnie z przepisami art. 160 ustawy – Kodeks Karny.

Należy wskazać, że operatorzy usług kluczowych obowiązani są do realizacji określonych obowiązków w ustawie na podstawie decyzji administracyjnej o uznaniu za operatora usługi kluczowej. Świadczy to o tym, iż w stosunku do tych podmiotów należy stosować podwyższony wymóg zachowania profesjonalizmu i jakości działania w zakresie przestrzegania (z punktu widzenia ustawodawcy) zasadniczych reguł cyberbezpieczeństwa. Przewidzenie w treści ustawy możliwości zastosowania wobec ww. podmiotów sankcji administracyjnej jest zasadne z punktu widzenia celów projektu ustawy oraz nie narusza zasad demokratycznego państwa prawnego. Należy też podkreślić, że wszystkie z przewidzianych kar stanowią górną granicę sankcji. Organy właściwe dla danego sektora będą mogły różnicować w ramach ww. granic wysokość kar dostosowując wysokość sankcji do sytuacji faktycznej w jakiej doszło do naruszenia.

Mając na uwadze charakter potencjalnych naruszeń przewidziano w ustawie mechanizm prewencji, zgodnie z którym przed wszczęciem postępowania w sprawie nałożenia kary pieniężnej, organ właściwy dla danego sektora może wezwać operatora usługi kluczowej do usunięcia naruszenia w wyznaczonym terminie, jeżeli przemawia za tym charakter naruszenia. Powyższa instytucja pozwoli to na zdyscyplinowanie operatorów usług kluczowych w wypełnianiu swoich podstawowych obowiązków, a jednocześnie nie będzie generowało konieczności wszczynania postępowań administracyjnych i ich formalnego prowadzenia oraz zakończenia. Redakcja przepisów wskazuje, że w niektórych przypadkach obsługa (w tym wystosowanie) wezwania do usunięcia naruszenia będzie mogła być realizowana w sposób

zautomatyzowany jeżeli środki techniczne zapewnią identyfikację, dokumentowanie oraz rozliczalność tych działań.

Od 1 czerwca 2017 r. w Kodeksie postępowania administracyjnego uregulowano kwestie nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu. Z uwagi na powyższe w projekcie ustawy wskazano wprost, iż w sprawach administracyjnych kar pieniężnych nakładanych na operatorów usług kluczowych zastosowanie znajdzie Dział IVa *Kodeksu postępowania administracyjnego* (kpa)[44]. Przemawia za tym fakt, iż obecnie przepisy Działu IVa Kpa w sposób kompleksowy regulują aspekty proceduralne nakładania i wymierzania administracyjnych kar pieniężnych ale też kwestie o charakterze materialnym. Co najistotniejsze z punktu widzenia niniejszej ustawy Dział IVa Kpa zawiera rozbudowany katalog przesłanek wymiaru administracyjnej kary pieniężnej.

Należy wskazać, że w rozdziale 10 przewidziano wyłącznie przepisy regulujące przesłanki (rodzaje naruszeń) oraz wysokość kar administracyjnych. Wskazano także na tryb ich nakładania i wymierzenia. Zagadnienia działania organów właściwych dla danego sektora przed zainicjowaniem wszczęcia postepowania w celu nałożenia kary administracyjnej regulują przepisy całej ustawy, w tym w szczególności przepisy rozdziału 8 – Nadzór i kontrola. W zależności od rodzaju naruszenia nałożenie administracyjnej kary pieniężnej i wszczęcie postępowania w celu jej wymierzenia będzie poprzedzone wynikiem przeprowadzonej kontroli, w innym zaś przypadku może to być wynikiem samodzielnego organu nadzoru np. po analizie wykazu operatów kluczowych.

Rozdział 11: Zmiany w przepisach obowiązujących, przepisy przejściowe, dostosowujące i końcowe

W art. 72 projektu ustawy zawarto regułę wydatkową zgodnie z art. 50 ustawy z dnia 27 sierpnia 2009 r. *o finansach publicznych*. Wskazane kwoty zostały oparte na zawartych w dołączonej do projektu ocenie skutków regulacji i wskazują one różnice w wydatkach budżetu państwa w stosunku do kwot zaplanowanych w ustawie budżetowej.

Ustawa wejdzie w życie po upływie 14 dni od dnia ogłoszenia, z uwzględnieniem faktu, że operatorzy usług kluczowych realizują obowiązki związane z wdrożeniem systemu monitorowania w trybie ciągłym, systemu ciągłości działania, procedur obsługi i zgłaszania

[44] Dz. U. z 2017 r. poz. 1257.

incydentów w terminie 6 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej. Inne obowiązki związane z wdrożeniem systemu bezpieczeństwa mają być realizowane przez operatora usługi kluczowej w terminie 3 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej.

Projekt ustawy będzie miał wpływ na sytuację małych i średnich przedsiębiorców świadczących usługi kluczowe, jeżeli zostanie w stosunku do nich wydana decyzja o uznaniu za operatora usługi kluczowej oraz średnich przedsiębiorców świadczących usługi cyfrowe. Projekt nie będzie miał wpływu na mikroprzedsiębiorców i małych przedsiębiorców świadczących usługi cyfrowe. Szczegółowy wpływ regulacji zawartych w projekcie przedstawiono w pkt 4 oceny skutków regulacji. W projekcie przewidziano możliwość nakładania kar pieniężnych na operatorów usług kluczowych w przypadku naruszenia przepisów ustawy.

Projekt ustawy o krajowym systemie cyberbezpieczeństwa jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Ustawa zawiera przepisy zmieniające do ustawy z dnia z dnia 7 września 1991 r. *o systemie oświaty*, ustawy z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne* oraz ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*. Zamierzeniem zmian w ustawie *Prawo telekomunikacyjne* jest włączenie Prezesa UKE w przekazywanie informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług u przedsiębiorców telekomunikacyjnych na potrzeby wymiany informacji w ramach krajowego systemu cyberbezpieczeństwa, o którym mowa w niniejszej ustawie. Zmiany w ustawie *o zarządzaniu kryzysowym* mają z kolei na celu ograniczenie obowiązków

w zakresie przygotowania dokumentacji w zakresie cyberbezpieczeństwa, w przypadku gdy właściciele, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w ustawie *o zarządzaniu kryzysowym* są jednocześnie operatorami usług kluczowych. Przepisy zmieniające ustawę o zarządzaniu kryzysowym mają również na celu umocowanie odpowiednio Rządowego Zespołu Zarządzania Kryzysowego i dyrektora Rządowego Centrum Bezpieczeństwa do realizacji niektórych funkcji w krajowym systemie cyberbezpieczeństwa.

Ustawa wprowadza również przepisy przejściowe umożliwiające sprawną realizację obowiązków sprawozdawczych w pierwszym roku obowiązywania ustawy wobec Komisji Europejskiej i Grupy Współpracy. W przypadku systemu teleinformatycznego, o którym jest mowa w art. 33, przewidziane jest uruchomienie systemu do eksploatacji z dniem 1 stycznia 2021 r.