UZASADNIENIE

Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, zwana dalej „ustawą o KSC", uchwalona w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. W tym zakresie jest to także implementacja dyrektywy NIS[1].

Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów bezpieczeństwa. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym"), który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „CSIRT"). Do zadań zespołów CSIRT poziomu krajowego należy także klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, zwanym dalej „NASK") oraz CSIRT MON (działającego w Ministerstwie Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach zespołu do spraw incydentów krytycznych.

Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół – jest to CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego.

Obecnie w krajowym systemie cyberbezpieczeństwa nie znajdują się przedsiębiorcy telekomunikacyjni ani dostawcy usług zaufania.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (zwany dalej „Pełnomocnikiem"), jest odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań w obszarze cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu lub podsekretarza stanu, jest

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE.L 2016 Nr 194, str. 1).

powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy również analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium do Spraw Cyberbezpieczeństwa

Kolegium do Spraw Cyberbezpieczeństwa (zwane dalej „Kolegium"), jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje również wymagania cyberbezpieczeństwa dotyczące decyzji Prezesa UKE w sprawie rezerwacji częstotliwości. Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów może wydać wiążące wytyczne w celu koordynacji działań w zakresie cyberbezpieczeństwa.

Potrzeba i cele projektu ustawy

Ustawa umożliwiła podjęcie prac nad dalszym rozwojem krajowego systemu cyberbezpieczeństwa, a doświadczenia zebrane przez dwa lata funkcjonowania systemu w Polsce, wskazały potrzebę dokonania zmian na poziomie ustawowym.

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Do tej pory powołano tylko jeden taki zespół – CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego, w sektorze najbardziej dojrzałym. Zespół powstał w oparciu o wewnętrzne środki i zasoby kadrowe Urzędu Komisji Nadzoru Finansowego. Dla podniesienia skuteczności reagowania na incydenty zachodzi konieczność ustanowienia CSIRT sektorowych dla każdego z kluczowych sektorów

polskich gospodarki. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami, gdyż otrzymają bezpośrednie wsparcie w reagowaniu na incydenty.

Zauważono potrzebę zwiększenia uprawnień Pełnomocnika w celu skuteczniejszej koordynacji współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa i efektywniejszej odpowiedzi na nowe cyberzagrożenia.

Jednym z najczęściej występujących problemów jest brak właściwych struktur u operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo lub zakres posiadanych kwalifikacji (w tym kadr) oraz dostępności do informacji o cyberzagrożeniach utrudnia skuteczne reagowanie na incydenty.

Należy również wskazać na konieczność uregulowania zasad współpracy pomiędzy podmiotami publicznymi funkcjonującymi na poziomie województwa. Z informacji zawartej w wystąpieniu pokontrolnym Najwyższej Izby Kontroli z 2019 r. wynika, że negatywnie oceniono aż 70% kontrolowanych jednostek samorządu terytorialnego w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji. Z analiz przeprowadzonych na zlecenie Ministra Cyfryzacji duże zastrzeżenia budzi poziom zabezpieczeń e-usług oferowanych przez samorządy.

Kluczowa jest kwestia dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń. Do tej pory powstało w Polsce tylko jedno centrum wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa – ISAC (Information Sharing and Analysis Center). Pierwsze ISAC powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku. ISAC gromadzi informacje o podatnościach i cyberzagrożeniach, a następnie przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w tym systemie. Taka formuła znacząco wpływa na poprawę cyberbezpieczeństwa i jest praktykowana w państwach Unii Europejskiej. Wskazane jest, aby więcej takich organizacji powstało w Polsce.

Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym[2]. Centra ISAC stanowią platformę takiej współpracy poprzez wymianę informacji na temat przyczyn, incydentów, cyberzagrożeń, jak również dzielenie się doświadczeniem, wiedzą i analizami.

[2] Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa, *Information Sharing and Analysis Center (ISACs) – Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, str. 7.

Akt o cyberbezpieczeństwie zachęca do tworzenia ISAC. Co więcej, jednym z obowiązków nałożonych na ENISA jest konieczność wspierania działań mających na celu wymianę informacji w ramach sektorów[3].

Przykładem sektorowego ISAC na poziomie europejskim jest European Energy Information Sharing & Analysis Centre (EE ISAC). Został zorganizowany z inicjatywy przemysłu energetycznego. W ramach EE ISAC wymieniają informacje dostawcy usług, przedsiębiorstwa użyteczności publicznej, instytucje naukowe, organizacje rządowe i pozarządowe (m.in. członkiem EE ISAC jest Polskie Sieci Elektroenergetyczne Spółka Akcyjna).

W Europie działa również amerykański *Financial Services Information Sharing and Analysis Center* zrzeszający około 7 000 instytucji finansowych z całego świata.

Coraz większe znaczenia dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe będą uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Polska brała udział w opracowaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (zwanego dalej "5G Toolbox"[4]), w którym zawarto środki na poziomie strategicznym i technicznym oraz wskazano działania wspierające. Efektywne wdrożenie tych środków znacząco ograniczy ryzyka cyberbezpieczeństwa w europejskich sieciach 5G.

Państwa członkowskie UE zobowiązały się w 5G Toolbox w szczególności do:

1) zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych,

2) oceniania profili ryzyka dostawców,

3) stosowania odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe,

4) wdrożenia strategii mających na celu zapewnienie dywersyfikacji dostawców, w celu unikania uzależnienia od dostawców stwarzających wysokie ryzyko,

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox.

Krajowy system certyfikacji cyberbezpieczeństwa

---

[3] Motyw 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.Urz. UE L 151 z 07.06.2019, str. 15.

[4] *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, Cooperation Group on Network and Information Security, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

W związku z rosnącą liczbą zagrożeń w cyberprzestrzeni jak i coraz istotniejszą rolą pełnioną przesz systemy informacyjne konieczne jest zapewnienie sprawdzonych i bezpiecznych rozwiązań technologicznych zarówno dla sektora publicznego, jak i prywatnego. W ostatnim czasie dało się także zauważyć wzrost liczby cyberprzestępstw zwłaszcza związanych z wykorzystaniem złośliwego oprogramowania takiego jak ransomware. Dlatego też konieczne jest zapewnienie każdemu zainteresowanemu dostępu do technologii umożliwiających bezpieczne przetwarzanie danych. Ze względu na wielką różnorodność wykorzystywanych technologii istotne jest stosowanie jednolitych standardów w zakresie bezpieczeństwa na terenie całej Unii Europejskiej.

Przygotowane rozwiązania zapewnią prawno-organizacyjne warunki do utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa, który zapewni wszystkim zainteresowanym podmiotom dostęp do możliwości testowania, badania produktów ICT, usług ICT i procesów ICT oraz otrzymywania certyfikatów cyberbezpieczeństwa opartych na europejskich programach, a także powszechnie uznawanych na obszarze Unii Europejskiej.

Konieczność stworzenia takiego systemu wynika również z bezwzględnie obowiązujących przepisów prawa europejskiego, zawartych w rozporządzeniu w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[5], zwanym dalej „Aktem o cyberbezpieczeństwie".

Ten akt prawny został uchwalony w 2018 roku i ustanowił europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów.

Akt o cyberbezpieczeństwie nakłada na wszystkie państwa członkowskie obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa, który będzie nadzorował rynek i kontrolował prawidłowość działań w zakresie certyfikacji. Konieczne jest również wprowadzenie przepisów związanych z akredytacją podmiotów uprawnionych do wydawania certyfikatów oraz procedury związane z działaniem tego systemu jak np. kwestie zatwierdzania certyfikatów o poziomie zaufania „wysoki".

Przyjęte rozwiązania sprawią, że polskie firmy będą mogły swobodnie konkurować na europejskim rynku. Trzeba tu wskazać, że w wielu państwach Europy Środkowej rynek ten jest mniej rozwinięty niż w

[5] Dz. Urz. UE L 151 z 07.06.2019, str. 15.

Polsce. W związku z tym, przyjęcie procedowanych przepisów może umożliwić polskim przedsiębiorcom przyciągnięcie klientów z regionu.

Przyjęte rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja w dziedzinie cyberbezpieczeństwa będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku.

Certyfikaty

Akt o Cyberbezpieczeństwie przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania, jakie musi spełniać produkt by uzyskać certyfikat określonego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Certyfikaty odwołujące się do najwyższego poziomu zaufania tj. poziomu „wysoki", w celu zagwarantowania, że proces ich wydawania przebiegał prawidłowo, będą musiały zostać zatwierdzone przez ministra właściwego do spraw informatyzacji. Procedura ta zapewnia wysoką jakość usług przy równoczesnym zachowaniu reguł konkurencji rynkowej. Dzięki temu certyfikaty najwyższego poziomu będą mogły być wydawane przez każdy podmiot działający na rynku. Gwarantuje to najwyższy możliwy poziom dostępu do usług certyfikacyjnych przy równoczesnym wykonaniu przepisów Aktu o cyberbezpieczeństwie.

Certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym. Ustawa tworzy ramy w jakich będzie wykonywana równocześnie nie nakładając żadnych obowiązków na podmioty działające na rynku. Każdy chętny będzie więc mógł rozpocząć działalność w tym zakresie jak i uzyskać certyfikację swojego produktu, usługi czy procesu ICT, równocześnie nie będąc do tego zobowiązanym.

Przyjęte rozwiązania służą również realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, zwanej dalej „Strategią". Ustanowienie krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa stanowią działania służące realizacji drugiego celu szczegółowego strategii – podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. W zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy o systemie oceny zgodności i nadzoru rynku. Polskie Centrum Akredytacji będzie zajmowało się akredytacją jednostek oceniających zgodność. Wymagania dotyczące jednostek oceniających zgodność zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. Ponadto dodatkowe wymagania dla nich mogą być też określane w konkretnych programach certyfikacji

cyberbezpieczeństwa. Również konkretne kryteria, jakie będą musiały spełniać produkty certyfikowane będą określone w krajowych i europejskich programach certyfikacji cyberbezpieczeństwa. Stosowane przepisy proceduralne będą więc dobrze znane i sprawdzone, a nowe będą jedynie stosowane przepisy materialne.

Prócz stworzenia ram dla funkcjonowania europejskich programów cyberbezpieczeństwa, ustawa tworzy też podstawę tworzenia krajowych programów certyfikacji cyberbezpieczeństwa. Umożliwi to podjęcie decyzji o certyfikowaniu produktów, które nie zostały objęte unijnymi programami certyfikacji. Zapewni to również możliwość reagowania na pojawiające się cyberzagrożenia bez konieczności czekania na powstanie programu certyfikacyjnego na poziomie europejskim.

Podjęcie prac związanych z utworzeniem krajowego systemu certyfikacji cyberbezpieczeństwa wynika zarówno z potrzeby stworzenia impulsu do rozwoju rynku w zakresie certyfikacji i zapewnienie bezpiecznych technologii dla zainteresowanych, a z drugiej strony z konieczności wdrożenia do polskiego porządku prawnego Aktu o cyberbezpieczeństwie.

Fundusz Cyberbezpieczeństwa

Utworzony zostanie Fundusz Cyberbezpieczeństwa z którego będą finansowane działania służące zapewnieniu cyberbezpieczeństwa w Polsce. W szczególności będzie z niego finansowane świadczenie teleinformatyczne dla osób pracujących na stanowiskach z tym związanych oraz Fundusz będzie finansowany m.in. z wpływów z kar za nieprzestrzeganie przepisów niniejszej ustawy.

Zgodność projektu ustawy z celami strategicznymi Rady Ministrów

Projekt ustawy służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 jakim jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Realizuje on także cel szczegółowy w postaci rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawnych dotyczących cyberbezpieczeństwa. Ponadto projekt realizuje cele Strategii szczególnie w odniesieniu do zapewnienie bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

Zmiany wprowadzane do krajowego systemu cyberbezpieczeństwa

CSIRT sektorowy

Nazwa sektorowego zespołu cyberbezpieczeństwa została zmieniona na CSIRT sektorowy. W przeciwieństwie do dotychczasowego, fakultatywnego trybu ustanawiania zespołu, w projekcie przewidziano obowiązek ustanowienia CSIRT sektorowego dla danego sektora lub podsektora przez organ właściwy.

CSIRT sektorowy będzie odpowiadał za przyjmowanie zgłoszeń o incydentach w sektorze lub podsektorze, dla którego został ustanowiony, a także za reagowanie na zgłoszone incydenty. Zakres

obowiązków zostanie, więc poszerzony – obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi kluczowej w reagowaniu na incydenty. CSIRT sektorowy będzie również dokonywał dynamicznej analizy ryzyka i incydentów, jak również gromadził informacje o cyberzagrożeniach.

CSIRT INT

W związku z rosnącą liczbą cyberataków na jednostki sektora publicznego konieczne jest dodatkowe wzmocnienie podmiotów z tego sektora. Szczególnie na ataki są narażone placówki dyplomatyczne i konsularne, których szczególne położenie i wrażliwy charakter przetwarzanych przez nie informacji sprawia, że udzielenie im wsparcia jest szczególnie utrudnione. Wychodząc naprzeciw tym problemom, powołuje się CSIRT INT, który będzie prowadzony przez szefa Agencji Wywiadu. Jego zadaniem będzie zapewnienie wsparcia placówkom dyplomatycznym i konsularnym w zakresie cyberbezpieczeństwa. W szczególności będzie wspierał je w obsłudze incydentów oraz przesyłał informacje o potencjalnych podatnościach i cyberzagrożeniach. CSIRT ten będzie opiekował się niewielką liczbą podmiotów i dzięki temu będzie w stanie zapewniać im pomoc dostosowaną ściśle do ich potrzeb. CSIRT INT zostały zapewnione uprawnienia niezbędne do realizacji przypisanych mu zadań.

ISAC

ISAC (centrum wymiany i analiz informacji), tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o cyberzagrożeniach i podatnościach oraz wymiana informacji o najlepszych praktykach.

SOC

Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: ,,SOC". Pojęcie to zastąpi struktury odpowiedzialne za cyberbezpieczeństwo u operatorów usług kluczowych. SOC posiadają ugruntowaną na rynku pozycję struktur realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek. Operatorzy usług kluczowych będą dysponowały strukturami SOC wewnątrz organizacji lub zawierali umowę z zewnętrznym podmiotem świadczącym usługi SOC. SOC m.in. będzie prowadził szacowanie ryzyka, wykrywał oraz reagował na incydenty. Minister właściwy do spraw informatyzacji będzie prowadził wykaz operacyjnych centrów bezpieczeństwa. Dotychczasowe wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo oraz podmioty zewnętrze, świadczące usługi cyberbezpieczeństwa dla operatorów usług kluczowych, staną się automatycznie SOC w rozumieniu ustawy o KSC.

Procedura uznania dostawcy za dostawcę wysokiego ryzyka

Odporność na cyberzagrożenia zależy w dużym stopniu od bezpieczeństwa sprzętu, oprogramowania i usług. Dotyczy to zarówno systemów teleinformatycznych, sieci telekomunikacyjnych oraz przemysłowych systemów sterowania. Dlatego nowelizacja przewiduje wprowadzenie postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa za dostawcę wysokiego ryzyka. Postępowanie w tej kwestii będzie prowadził minister właściwy do spraw informatyzacji. Postępowanie będzie oparte o transparentne procedury określone w Kodeksie postępowania administracyjnego. Minister właściwy ds. informatyzacji każdorazowo będzie zasięgał opinii Kolegium. Rolą Kolegium będzie sporządzenie opinii na temat dostawcy sprzętu lub oprogramowania i dostarczanych przez niego produktów ICT, usług ICT, procesów ICT. W ramach opinii brane pod uwagę zarówno aspekty techniczne, jak i pozatechniczne, mające wpływ na bezpieczeństwo narodowe. Postępowanie będzie kończyło się decyzją administracyjną w sprawie uznania dostawcy za dostawcę wysokiego ryzyka. Będzie ona podlegać zaskarżeniu do sądu administracyjnego.

Podkreślić należy, że ocena profili ryzyka dostawców jest jednym z narzędzi strategicznych (*Strategic Measure – SM03*) uzgodnionych przez państwa członkowskie Unii Europejskiej, Komisję Europejską i ENISA w 5G Toolbox.

Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych, czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorcami) w zależności od decyzji ministra właściwego do spraw informatyzacji w zakresie uznania danego dostawcy za dostawcę wysokiego ryzyka, będą musiały wycofać z użycia wskazany sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka w terminie 7 lat od wydania decyzji administracyjnej. Natomiast duzi przedsiębiorcy telekomunikacyjni będą musieli wycofać produkty, usługi i procesy ICT w ciągu 5 lat, jeżeli znajdują się one w zakresie funkcji krytycznych określonych w załączniku nr 3 do ustawy. Podkreślenia wymaga fakt, że obowiązkowi wycofania będą podlegały produkty, usługi i procesy ICT wskazane w decyzji ministra właściwego do spraw informatyzacji – a więc nie wszystkie produkty, usługi i procesy ICT oferowane przez dostawcę wysokiego ryzyka.

Zapobieganie incydentom krytycznym i zwiększenie skuteczności reagowania na incydenty krytyczne

W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne będą mogły być wydawane:

1) ostrzeżenia (wydawane przez Pełnomocnika) – w przypadku uzyskania informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,

2) polecenia zabezpieczające (wydawane przez ministra właściwego do spraw informatyzacji) – w celu zapewnienia koordynacji i odpowiedniej reakcji w sytuacji wystąpienia incydentu krytycznego.

Krajowe programy certyfikacji cyberbezpieczeństwa

Projekt ustawy przewiduje też tworzenie krajowych programów certyfikacji cyberbezpieczeństwa, na podstawie których przeprowadzana będzie certyfikacja. W dokumentach tych zawarte zostaną techniczne standardy, które produkty, usługi i procesy ICT będą musiały spełniać. Ponadto, będą określały szczegóły związane z procesem certyfikacji czy procedury sanacyjne w przypadku, gdy po samej certyfikacji ujawnią się wady produktów. Wszystkie te elementy muszą być bardzo ściśle dostosowane do konkretnego produktu, usługi czy procesu ICT. Propozycja programu będzie przygotowywany przez ministra właściwego do spraw informatyzacji, któremu pozostawiono swobodę wyboru sposobu prac nad tym dokumentem. W szczególności może on powierzyć przygotowanie takiego projektu jednostkom przez siebie nadzorowanym np. Naukowej i Akademickiej Sieci Komputerowej czy Instytutowi Łączności. Następnie przygotowana propozycja programu będzie podstawą dla rozporządzenia Rady Ministrów, ustanawiającego dany program. Na tym etapie możliwość wypowiedzenia się o kształcie danego programu będzie miał każdy zainteresowany organ administracji publicznej (art. 59d).

Elementy programu zostały sformułowane na wzór przepisów Aktu o cyberbezpieczeństwie, dotyczących europejskich programów certyfikacji cyberbezpieczeństwa. Dzięki temu wymagania i standardy wobec krajowych i europejskich programów certyfikacji będą bardzo do siebie zbliżone co sprawi, że nie będzie konieczne tworzenie osobnej terminologii dla krajowych programów certyfikacji. Umożliwi to więc wykorzystanie w jak największym stopniu praktyk wypracowanych w ramach europejskich programów certyfikacji. Ponadto certyfikaty cyberbezpieczeństwa wydane na podstawie krajowych programów certyfikacyjnych mogą, wskutek przyjętych rozwiązań, łatwo zostać uznane w innych krajach UE. Ponadto możliwe będzie rozszerzenie rynku certyfikacji przez objęcie programami produktów, usług i procesów ICT nieujętych w europejskich programach certyfikacyjnych. Bliskość z programami europejskimi umożliwi też stosunkowo łatwe przenoszenie programów krajowych na poziom europejski. Będzie to bardzo ważnym narzędziem do kreowania polskiej polityki w zakresie certyfikacji cyberbezpieczeństwa na poziomie europejskim (art. 59 f-g).

Proces certyfikacji będzie prowadzony przez jednostki oceniające zgodność akredytowane przez Polskie Centrum Akredytacji na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i systemach nadzoru rynku. Wykorzystanie już obowiązujących przepisów zapewni możliwie najsprawniejsze wprowadzenie w życie systemu certyfikacji cyberbezpieczeństwa. Polskie Centrum Akredytacji będzie sprawowało nadzór nad akredytacją jednostek oceniających zgodność. Będzie też na bieżąco wymieniać się informacjami z ministrem właściwym do spraw informatyzacji, co zapewni skuteczną kontrolę nad całym systemem. (art. 59h)

W przypadku certyfikatów odwołujących się do najniższego z poziomów uzasadnienia zaufania, sami dostawcy sprzętu lub oprogramowania będą mogli wydawać deklaracje zgodności by wskazać, że ich produkt spełnia dane wymagania (art. 59p-r). Zapewni to im możliwość skorzystania z programów certyfikacyjnych ograniczając równocześnie koszty uczestnictwa w nich.

Zmiana podziału ustawy w związku z rozbudową aktu normatywnego

W związku z dodaniem szeregu rozwiązań dotyczących strategicznej sieci bezpieczeństwa, czyli przepisów z związanych z bezpieczeństwem, ale wpisujących się również w dziedzinę prawa telekomunikacyjnego (prawa komunikacji elektronicznej) zasadne jest podział ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa na działy. Pierwszy dział zawiera ogólne postanowienia, drugi – przepisy dotyczące krajowego systemu cyberbezpieczeństwa, które stanowią niezmiennie podstawową regulację ustawy, oraz postanowienia odnoszące się do nowego zespołu norm prawnych określonych „krajowym systemem certyfikacji cyberbezpieczeństwa". Trzeci dział składać się z przepisów dotyczących funkcjonowania strategicznej sieci bezpieczeństwa.

Przewidywane skutki społeczne, gospodarcze, prawne i finansowe wprowadzanych zmian

Skutki społeczne

Dodanie CSIRT sektorowych, SOC i ISAC pozwoli na zwiększenie skuteczności funkcjonowania krajowego systemu cyberbezpieczeństwa.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, które stworzą nie tylko skuteczny system reagowania na incydenty, ale też zapewnią bazę wiedzy o cyberzagrożeniach i podatnościach danego sektora. Dzięki temu incydenty w sektorze będą obsługiwane szybciej, z uwzględnieniem szczególnych uwarunkowań danego sektora. Natomiast centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa.

Przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw. Większe wykorzystanie rozwiązań odpornych na cyberataki zwiększy też ogólne bezpieczeństwo danych obywateli.

Skutki gospodarcze

Celem krajowego systemu cyberbezpieczeństwa jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Poprzez nałożenie dodatkowych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą. Zobowiązuje bowiem tych przedsiębiorców do dbania o cyberbezpieczeństwo. Po stronie przedsiębiorców powoduje to koszty związane z koniecznością dostosowania się do wymogów ustawy. Należy jednak zauważyć, że wielu z nich już obecnie

posiada operacyjne centra bezpieczeństwa, ponieważ podobny wymóg istnieje w obowiązującej wersji ustawy. Poza tym, podmiot inwestujący we własne cyberbezpieczeństwo zyskuje zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom skuteczniej dbać o cyberbezpieczeństwo w swojej działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

Przyjęte rozwiązania będą również promowały rozwiązania, które zapewniają wysokie standardy w zakresie cyberbezpieczeństwa. Prywatni przedsiębiorcy będą mieli ułatwiony wybór bezpiecznych rozwiązań technologicznych. Ponadto nowe regulacje będą zapewniały, że firmy, które zakupią certyfikowane produkty, usługi czy procesy ICT będą miały pewność, że ich certyfikaty będą honorowane na terenie całej Unii Europejskiej. Projektowana ustawa zawiera szereg rozwiązań zapewniających właściwe standardy postępowania przy ocenie zgodności co daje dodatkowe gwarancje jakości.

Krajowy system certyfikacji cyberbezpieczeństwa będzie też stanowił cenne uzupełnienie krajowego systemu cyberbezpieczeństwa. Stworzy wyraźny system oceny produktów ICT dzięki czemu jasno wskazane będą produkty spełniające najlepsze standardy w dziedzinie bezpieczeństwie.

Przyjęte przepisy nie nałożą żadnych dodatkowych obowiązków na podmioty niezainteresowane uczestnictwem w tym systemie. Przyjęty model nie tworzy też barier dostępu do rynku.

Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa m.in. sektorowych CSIRT, będzie wymagało dodatkowych nakładów finansowych. Należy jednak podkreślić, że jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częstsze i bardziej zaawansowane. Drastycznie wzrosła liczba incydentów cyberbezpieczeństwa oraz samych cyberataków, których ofiarami padają urzędy, szpitale, ale także coraz więcej ataków obserwujemy w sektorze prywatnym oraz w stosunku do obywateli. Od początku 2020 roku do końcu listopada tylko zespół CSIRT NASK odnotował 30300 zgłoszeń. W samym listopadzie 2020 r. były to 3833 zgłoszenia. Z tej liczby CSIRT NASK zarejestrował od początku roku 2020 do końca listopada aż 9604 incydenty cyberbezpieczeństwa (w listopadzie zarejestrowano 1381). Jest to znaczący wzrost w stosunku do 2019 r., w którym CSIRT NASK odnotował 6484 incydenty.

Istnieje także stałe zagrożenie działaniami wywiadowczymi w cyberprzestrzeni. Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne, a mają one również wymiar finansowy. Inwestycja w rozbudowę krajowego systemu cyberbezpieczeństwa pozwoli ograniczyć prawdopodobieństwo powstania

tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne efekty. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Przyjęcie przepisów o krajowym systemie certyfikacji cyberbezpieczeństwa będzie miało korzystne skutki dla całego sektora przedsiębiorstw. Obecnie firmy ponoszą coraz większe straty w wyniku działalności cyberprzestępców. Wprowadzenie certyfikacji w tej dziedzinie sprawi, że firmom łatwiej będzie wybierać rozwiązania gwarantujące najwyższy poziom bezpieczeństwa. Ponadto samo stworzenie systemu przyczyni się do wzrostu świadomości cyberbezpieczeństwa. W efekcie straty ponoszone przez sektor przedsiębiorstw powinny zostać zmniejszone.

Skutki prawne

Powstaną nowe rejestry pomagające właściwym instytucjom wykonywać swoje ustawowe zadania – wykaz SOC oraz wykaz ISAC.

Minister właściwy do spraw informatyzacji będzie mógł przeprowadzić postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

Pełnomocnik i minister właściwy do spraw informatyzacji uzyskają nowe narzędzia w celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne. Przewodniczący Kolegium nabędzie szereg nowych kompetencji (wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1 ustawy; zlecić CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1 ustawy albo analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2; wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1.Ponadto przewodniczący Kolegium będzie miał kompetencję do powołania zespołu opiniującego, o którym mowa w art. 66a ust. 10 pkt 1, do wskazywania przedstawicieli członków Kolegium wchodzących w jego skład, a także będzie mógł rozstrzyga spór kompetencyjny wskazując właściwego członka zespołu opiniującego.

Umocowany krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował uprawnieniami do nadzoru nad systemem certyfikacji cyberbezpieczeństwa oraz będzie dysponował narzędziami do usuwania z obiegu prawnego certyfikatów wydanych wbrew przepisom ustawy oraz do kontrolowania podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Ponadto przepisy ustanawiają podstawę prawną i procedury dla przyjmowania krajowych programów certyfikacji cyberbezpieczeństwa.

Powstaną także dwa fundusze celowe – Funduszu Cyberbezpieczeństwa oraz Fundusz celowy na rzecz strategicznej sieci bezpieczeństwa.

Źródła finansowania projektowanych zmian

Wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki z budżetu państwa. Szczegółowy opis źródeł finansowania zawarty jest w ocenie skutków regulacji.

Wyniki przeprowadzonych konsultacji

W dniach 30.06-8.07.2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej. Zostały również przeprowadzone konsultacje wewnątrz resortu Ministerstwa Cyfryzacji.

W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium. Powtórzono również konsultacje wewnętrzne.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów na 14 dni. Jednakże, w z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni – łącznie na uwagi było 28 dni.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, pod warunkiem zgłoszenia tego faktu opiekunowi merytorycznemu.

Uzasadnienie poszczególnych przepisów

Pierwszy dział stanowić będą postanowienia ogólne (przed art. 1 zostało dodane oznaczenie działu – Postanowienia ogólne),

W art. 1 został dodany w ust. 1 pkt 1a oraz 5 i 6 w związku z rozszerzeniem zakresu przedmiotowego ustawy o:

- krajowy system certyfikacji cyberbezpieczeństwa
- zasady działania Funduszu Cyberbezpieczeństwa
- zasady wyznaczania i zadania Operatora strategicznej sieci bezpieczeństwa,
- zasady powołania i funkcjonowania Spółki Polskie 5G,
- zasady przyznania zasobów częstotliwości z zakresu 703 – 733 MHz oraz 758 – 788 MHz,
- zasady działania Fundusz celowego na rzecz strategicznej sieci bezpieczeństwa.

Zmodyfikowane zostały również wyłączenia przedmiotowe ustawy w ust. 2 pkt 1–2. Do przedsiębiorców telekomunikacyjnych będą stosowane:

1) przepisy o wycofaniu produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka,
2) przepisy o ostrzeżeniu i poleceniu zabezpieczającym,
3) przepisy o karach pieniężnych.

Z kolei do dostawców usług zaufania będą stosować się:

1) przepisy o ostrzeżeniu i poleceniu zabezpieczającym,
2) przepisy o karach pieniężnych.

Artykuł 2 obecnie obowiązującej ustawy zawiera słowniczek pojęć używanych w ustawie, stąd niezbędne było dodanie do niego w projektowanych punktach 3a-3d definicji: „CSIRT sektorowego", „CSIRT INT", „ISAC" i „SOC", a także „dostawcy". Z kolei dodanie punktów 20-32 wynikało z konieczności wprowadzenia do ustawy pojęć związanych z certyfikacją cyberbezpieczeństwa. W związku ze zmianą nazwy proponuje się w nowelizacji zamianę frazy „sektorowy zespół cyberbezpieczeństwa" na „CSIRT sektorowy".

Projekt ustawy dostosowuje katalog definicji w ustawie o KSC do zmian jakie zostały wprowadzone w Akcie o cyberbezpieczeństwie. W szczególności oznacza to konieczność przyjęcia nowej definicji cyberbezpieczeństwa, która została wprowadzona w ww. akcie prawnym.

Tam gdzie jest to konieczne, zachowano poprzednie znaczenia terminu: „cyberbezpieczeństwo" i wprowadzone zostało pojęcie „bezpieczeństwa systemów informacyjnych" (art. 2 pkt 4a), którego zakres jest identyczny z poprzednią definicją cyberbezpieczeństwa. Nie spowoduje to jednak zmian w zakresie konkretnych obowiązków jakie obecnie nakłada ustawa na podmioty krajowego systemu cyberbezpieczeństwa. W celu zachowania spójności z dyrektywą NIS pojęcie „sieci i systemów informatycznych" zastąpione zostało pojęciem „systemy informacyjne" zgodnie ze sposobem, w jakim to pojęcie zostało implementowane do polskiego porządku prawnego w 2018 roku. Nowe definicje są więc całkowicie zgodne z przepisami zawartymi w akcie o cyberbezpieczeństwie. Takie rozwiązanie zapewnia nie tylko zgodność z polskim porządkiem prawnym, ale również odpowiednią przejrzystość przepisów.

Pojęcie „zagrożenie cyberbezpieczeństwa" zostało zastąpione pojęciem cyberzagrożenia (art. 2 pkt 17). Definicja cyberzagrożenia została wprowadzona w Akcie o cyberbezpieczeństwie i jest ona bardzo zbliżona do funkcjonującej w naszym systemie prawnym definicji „zagrożenia cyberbezpieczeństwa". Nie jest zasadne utrzymywanie w systemie prawnym obu tych pojęć i dlatego pozostawiono jedynie sformułowanie „cyberzagrożenie". Nowe pojęcie jest zgodne z najnowszą terminologią w dziedzinie cyberbezpieczeństwa stosowaną w państwach członkowskich Unii Europejskiej.

Wprowadzone zostały pojęcia produktu ICT, usługi ICT oraz procesu ICT. Te trzy pojęcia służą objęciu systemem certyfikacji jak największego zakresu dostępnych na rynku świadczeń. Produkt oznacza „element lub grupę elementów systemów informacyjnych". Będzie więc obejmował praktycznie wszystkie przypadki oprogramowania oraz urządzeń podlegających certyfikacji. Usługi będą dotyczyły wszelkich działań związanych z przetwarzaniem informacji w systemach informacyjnych. Obejmują więc sytuację gdy żadne operacje nie są wykonywane w ramach systemów klienta, który jedynie otrzymuje ich końcowy efekt. Proces ICT oznacza „zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT". Są to więc wszelkiego rodzaju działania związane z tworzeniem systemów informacyjnych i ich bieżącym utrzymaniem.

Ponadto projektowana ustawa posługuje się pojęciami certyfikat oraz krajowy certyfikat cyberbezpieczeństwa. Certyfikat odnosi się do wszystkich certyfikatów w dziedzinie cyberbezpieczeństwa, tj. zarówno tych wydanych w ramach krajowych jak i europejskich programów certyfikacji. Z kolei krajowy certyfikat cyberbezpieczeństwa dotyczy tylko dokumentów wydanych na podstawie krajowych programów certyfikacyjnych. To rozróżnienie jest potrzebne dla wyodrębnienia przepisów, które dotyczą tylko krajowych certyfikatów. Certyfikaty te będą traktowane jednakowo. Wiele kwestii związanych z europejskimi certyfikatami zostało określonych w unijnym rozporządzeniu Akcie o cyberbezpieczeństwie. Natomiast przepisy te nie odnoszą się do certyfikatów krajowych. Z tego też względu w projekcie ustawy znalazły się przepisy regulujące kwestie związane z wydawaniem certyfikatów krajowych. Analogiczna sytuacja występuje w przypadku deklaracji zgodności i krajowych deklaracji zgodności. Konsekwencją tych zmian była konieczność dostosowania pozostałych przepisów ustawy.

Wprowadzone pojęcie dostawcy przesądza, że jest to producent, upoważniony przedstawiciel, importer lub dystrybutor w rozumieniu rozporządzenia unijnego o wymaganiach w zakresie akredytacji i nadzorze rynku[6)]. Definicja ta jest potrzebna przy przepisach dotyczących krajowego systemu certyfikacji cyberbezpieczeństwa oraz na potrzeby postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Wprowadzono również skrót nazwy Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA). Skrót jest powszechnie rozpoznawalny wśród osób zajmujących się cyberbezpieczeństwem – jego stosowanie w ustawie poprawi redakcję przepisów.

Po art. 2 zostaje dodane oznaczenie działu II – Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa.

[6)] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93

W związku z pojawiającymi się wątpliwościami dotyczącymi uprawnień podmiotów krajowego systemu cyberbezpieczeństwa przy obsłudze incydentu został dodany art. 3a. W przepisie tym doprecyzowano więc, że w przypadku wystąpienia incydentu mogą one, w ramach obsługi incydentów, o której mowa w art. 2 pkt 10, analizować ruch sieciowy oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu. W przypadku wielu cyberataków takie działania są niezbędne w celu ochrony systemu, a równocześnie mogą one naruszyć okresowo prawa określonych użytkowników. Z powyższych względów konieczne jest wskazanie wprost, że takie działania są dopuszczalne wyłącznie na wyraźnej podstawie prawnej.

W nowelizacji art. 4, który wymienia podmioty krajowego systemu cyberbezpieczeństwa proponuje się dodać w punktach 7a, 7b, 14a i 14b nowe podmioty: Urząd Komisji Nadzoru Finansowego (w związku ze zmianą ustawy o nadzorze nad rynkiem finansowym zmienił formę prawną działania[7]), wyszczególniono uczelnie odwołując się do ustawy z 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce. W punkcie 6a dodano także ISAC. Zgodnie ze zmianą nazewnictwa podmioty świadczące usługi cyberbezpieczeństwa zmieniono na podmioty świadczące usługi SOC, o których mowa w art. 14a ust. 1 ustawy. Do tej pory nie były objęte ustawą inne istotne dla funkcjonowania państwa podmioty – Wody Polskie oraz instytucje rozwoju: Polski Fundusz Rozwoju, Polska Agencja Rozwoju Przedsiębiorczości, Korporacja Ubezpieczeń Kredytów Eksportowych Spółka Akcyjna, Polska Agencja Inwestycji i Handlu Spółka Akcyjna, Agencja Rozwoju Przemysłu Spółka Akcyjna. Wody Polskie jako podmiot zajmujący się gospodarką wodną realizuje ważne zadania publiczne – zapobieganie suszom i powodziom oraz zapewnianie dobrej jakości wody dla mieszkańców Polski. Z kolei Polski Fundusz Rozwoju S.A. odpowiada za wsparcie polskich przedsiębiorców, w tym realizuje program Tarczy Antykryzysowej. Do krajowego systemu cyberbezpieczeństwa zostaną dodane także samodzielne publiczne zakłady opieki zdrowotnej, które podczas pandemii COVID-19 pełnią szczególną rolę. Dlatego konieczne jest objęcie tych podmiotów obowiązkami z art. 21-23 ustawy o krajowym systemie cyberbezpieczeństwa, a także zapewnienie im wsparcia właściwego zespołu CSIRT poziomu krajowego w przypadku wystąpienia incydentu.

Jak wskazuje doktryna termin sześciu miesięcy na wystąpienie organu właściwego ds. cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych nie gwarantuje aktualności wykazu[8]. Projektodawca proponuje aby organ właściwy do spraw cyberbezpieczeństwa dokonał tej czynności niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych (zmiana w art. 7 ust. 4).

[7)] Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz. U. poz. 2243 oraz z 2019 r. poz. 875 i 2217).

[8] G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), Ustawa o krajowym systemie cyberbezpieczeństwa: komentarz , Warszawa 2019., str. 113

W propozycji nowelizacji art. 7 ust. 5 dodaje się możliwość podpisania wniosku o wpisanie operatora usługi kluczowej do wykazu operatorów także podpisem osobistym. Podpis osobisty został uregulowany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych. Jest to zaawansowany podpis elektroniczny umieszczony w warstwie elektronicznej dowodu osobistego. Podpisanie danych podpisem osobistym ma taki sam skutek wobec podmiotu publicznego co podpis własnoręczny.

Podmioty krajowego systemu cyberbezpieczeństwa powinny również oceniać krytyczność aktualizacji oprogramowania oraz w stosownej sytuacji dokonywać tych aktualizacji.

W art. 9 wprowadzono zmianę, na mocy której operatorzy usług kluczowych będą musieli wyznaczyć 2 osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Następnie dane tych osób zostaną przekazane do organów właściwych do spraw cyberbezpieczeństwa, które niezwłocznie przekażą je do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego. Jest to również rozwiązanie, które ogranicza obowiązek operatorów usług kluczowych do przekazywania danych do jednego podmiotu (organu właściwego do spraw cyberbezpieczeństwa).

W nowelizowanym art. 10 ust. 2 pkt 2 rozszerzono obowiązki nadzoru nad dokumentacją o ochronę dokumentów przed przypadkowym zniszczeniem, utratą oraz nieuprawnionym dostępem.

Zgodnie z nowymi zmianami w art. 11 operator usługi kluczowej będzie zgłaszał, za pomocą systemu teleinformatycznego, o którym mowa w art. 46, incydenty poważne do CSIRT sektorowego, który następnie niezwłocznie przekaże je do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. W ten sposób zostanie ograniczony ustawowy obowiązek zgłaszania incydentów poważnych do jednego podmiotu, jednocześnie wzmacniając rolę CSIRT sektorowych.

Art. 14 zostanie całkowicie zmieniony w nowelizacji. Wskazano, że zadania operatorów usług kluczowych w zakresie cyberbezpieczeństwa realizowane są za pomocą funkcji SOC. SOC może być powołany wewnątrz organizacji danego operatora usługi kluczowej lub stanowić odrębny podmiot. W tym drugim przypadku operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o zawarciu umowy z zewnętrznym podmiotem realizującym zadania funkcji SOC, jego danych kontaktowych i zakresie świadczonej usługi na rzecz tego operatora. Wprowadza się także możliwość, aby SOC mógł być utworzony na rzecz operatora usługi kluczowy przez organ tworzący lub nadzorujący operatora.

Art. 14 ust. 3 nowelizacji nakazuje SOC wprowadzić zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Jeżeli operator usługi kluczowej zawiera z podmiotem trzecim umowę o realizację funkcji SOC to o umowie i jej szczegółach jest obowiązany niezwłocznie poinformować organ właściwy ds. cyberbezpieczeństwa.

W niezbędnych sytuacjach SOC ma zapewnić bezpieczny zdalny dostęp do swoich systemów dla obsługiwanego operatora usługi kluczowej. Istotne jest, aby opracować procedury i stosować środki, które zminimalizują zagrożenie wycieku danych z SOC.

Nawiązując do praktyki obecnej na rynku (publikowanie informacji na podstawie wzoru RFC 2350) podmioty trzecie świadczące funkcje SOC udostępniają na stronie internetowej podstawowe informacje o swojej działalności. Należy podkreślić, że każdy z operatorów usług kluczowych może swobodnie wybrać w jakim modelu prowadzony jest SOC. Nie musi on być jedną konkretną jednostką w jego strukturze, jego zadania mogą być realizowane przez pracowników różnych komórek wewnętrznych organizacji. Możliwe jest również zawarcie umowy z kilkoma podmiotami zewnętrznymi w kwestii usług SOC'owych i dowolnie rozdzielić pomiędzy je zadania. Niezależnie od wybranego modelu operator usługi kluczowej ponosi odpowiedzialność za zapewnienie jej ciągłości.

Aby odpowiednie urzędy i służby miały dostęp do danych SOC w zakresie swoich ustawowych kompetencji, minister właściwy do spraw informatyzacji będzie prowadził wykaz SOC. W wykazie znajdą się zarówno podmioty prowadzące SOC oraz podmioty, na rzecz których SOC realizują zadania. Do wykazu mogą być wpisane SOC, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk. Muszą one posiadać zdolność do ochrony informacji niejawnych. Dodatkowym wymogiem jest również podpisanie porozumienia z ministrem właściwym do spraw informatyzacji w sprawie korzystania z systemu teleinformatycznego opisanego w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Co istotne, wprowadzony zostanie obowiązek aby przy zawieraniu umowy na świadczenie usług SOC przez podmiot prowadzący SOC dla operatora usługi kluczowej umowa ta zawierała zastrzeżenie, że usługi te podlegają prawu polskiemu.

W celu umożliwienia wykonywania swoich zadań dane z wykazu SOC są udostępniane CSIRT MON, CSIRT NASK, CSIRT GOV i właściwemu ze względu na sektor CSIRT sektorowemu, jak również operatorowi usługi kluczowej w dotyczącym go zakresie. Na wniosek dane z wykazu SOC mogą być udzielane organom właściwym – służbom, sądom, prokuraturze.

Zmiana art. 21 polega na wprowadzeniu obowiązku wyznaczenia przez podmioty publiczne nie jednej, a dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dzięki temu w pełniejszy sposób zostanie zabezpieczony kontakt podmiotem publicznym podczas trwania incydentu w podmiocie publicznym.

W art. 22 dodane zostały ust. 1a oraz 3–7, które regulują zgłaszanie incydentów w podmiocie publicznym przez Agencję Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Wskazane podmioty będą zgłaszały incydenty oraz przekazywały dane osób do kontaktu do nowo utworzonego CSIRT'u INT. Specyfika tych jednostek, zwłaszcza ich działanie poza granicami RP, sprawia, że konieczne jest zapewnienie im dodatkowego wsparcia. To wsparcie zostanie zapewniony przez CSIRT INT prowadzony przez Agencję Wywiadu. Będzie on wspierał te jednostki w obsłudze incydentów oraz przekazywał informacje o ich sytuacji do CSIRT GOV. W związku z tym został on również wyposażony w uprawnienia do przetwarzania odpowiednich danych. Takie ukształtowane rozwiązanie zwiększy cyberbezpieczeństwo szczególnie wrażliwych podmiotów publicznych.

Po rozdziale 5 zostanie dodany rozdział 5a dotyczący ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Nic nie stało do tej pory na przeszkodzie, aby były tworzone podmioty na wzór ISAC, na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji. Nowelizacja tego nie zmienia, daje jedynie możliwość funkcjonowania ISAC w ramach krajowego systemu cyberbezpieczeństwa.

W projektowanym art. 25a ustawy wskazano (w otwartym katalogu) zadania ISAC wpisanych do wykazu ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Będą to: wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz wszystkich rodzai incydentów. Dodano przepisy odnośnie prowadzenia wykazu ISAC, wpisu do niego oraz wykreślenia. Wpis do wykazu będzie odbywał się na wniosek organu właściwego do spraw cyberbezpieczeństwa. ISAC ma współpracować z zespołami CSIRT poziomu krajowego, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa. Będzie musiał również złożyć sprawozdanie ze swojej działalności ministrowi właściwemu ds. informatyzacji. Minister będzie mógł przeprowadzić kontrolę działalności ISAC. Jeżeli ISAC prowadzi działalność niezgodną z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa to minister właściwy ds. informatyzacji może zwrócić się do ISAC o usunięcie nieprawidłowości w określonym terminie albo wykreślić taki podmiot z wykazu.

W nowelizacji art. 26 ust. 2 CSIRT GOV, CSIRT MON i CSIRT NASK będą mogły udzielić wsparcia w obsłudze incydentów wszystkim podmiotom krajowego systemu cyberbezpieczeństwa oraz operatorom infrastruktury krytycznej. Pełnomocnik będzie mógł zlecić zapewnienie tego wsparcia:

- CSIRT NASK;
- CSIRT GOV – za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego;
- CSIRT MON – za zgodą Ministra Obrony Narodowej.

Obydwie zgody będą mogły być wyrażone z wykorzystaniem środków porozumiewania się na odległość.

Zmiany w art. 26 ust. 3 pkt 2 zmiany polegają na uproszczeniu nazewnictwa. W ust. 3 dodane zostały nowe zadania zespołów CSIRT poziomu krajowego: gromadzenie informacji dotyczących cyberzagrożeń, podatności i incydentów, przygotowywanie dla Pełnomocnika analiz, przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa. Zespoły CSIRT otrzymają także możliwość prowadzenia działań na rzecz podniesienia poziomu cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, takich jak testy bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami. Będą mogły też identyfikować podatności systemów dostępnych w otwartych sieciach teleinformatycznych oraz informować właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożenia. Do testów bezpieczeństwa będą stosowały się odpowiednio przepisy art. 32a ust. 4–6 i 9–11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (dalej „ustawa o ABW i AW"). Natomiast art. 32 ust. 4 i 5 przywołanej ustawy będzie stosować się wprost. Stosowanie odpowiednio art. 32a ust. 4 ustawy o ABW i AW polega na tym, że prowadzenie testów bezpieczeństwa systemu teleinformatycznego ma na celu identyfikację podatności, przez które rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływających na integralność, poufność, rozliczalność i dostępność tego systemu. Stosowanie odpowiednio art. 32a ust. 5 ustawy o ABW i AW o polega na tym, że test bezpieczeństwa powinien być prowadzony z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie teleinformatycznym podlegającym tej ocenie. Art. 32a ust. 6 ustawy o ABW i AW stosuje się odpowiednio w ten sposób, że celu minimalizacji negatywnych następstw testu bezpieczeństwa, właściwy CSIRT poziomu krajowego, uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa ramowe warunki przeprowadzania testu bezpieczeństwa, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych testów bezpieczeństwa. Art. 32a ust. 9 ustawy o ABW i AW stosuje się odpowiednio w ten sposób, że informacje uzyskane przez CSIRT poziomu krajowego w wyniku przeprowadzania testu bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych przez CSIRT poziomu krajowego oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Art. 32a ust. 10 ustawy o ABW i AW stosuje się odpowiednio w ten sposób, że po przeprowadzeniu testu bezpieczeństwa CSIRT poziomu krajowego sporządza i przekazuje podmiotowi, którego system podlegał testowi bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach testu bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu teleinformatycznego. Art. 32a ust. 11 ustawy o ABW i AW stosuje się odpowiednio w ten sposób, że jeżeli wykryta podatność może wystąpić w innych systemach teleinformatycznych, CSIRT poziomu krajowego

informuje niezwłocznie ministra właściwego do spraw informatyzacji o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach teleinformatycznych.

W związku z dodaniem nowych podmiotów w skład krajowego systemu cyberbezpieczeństwa należało ustalić, który z zespołów CSIRT poziomu krajowego będzie przyjmował od nich zgłoszenia incydentów. CSIRT GOV będzie właściwy dla przyjmowania incydentów z Państwowego Gospodarstwa Wodnego Wody Polskie, a także z instytucji rozwoju. Natomiast CSIRT NASK będzie przyjmował zgłoszenia incydentów z uczelni, instytutów badawczych, Polskiej Akademii Nauk, Centrum Łukasiewicz, instytutów działających w ramach Centrum Łukasiewicz, międzynarodowych instytutów badawczych, Polskiej Akademii Umiejętności.

W związku z pismem Komisji Europejskiej Ref. Ares(2019)2130481 z dnia 26 marca 2019 r. w zakresie zmiany terminu przekazania przez państwa członkowskie sprawozdania rocznego dotyczącego informacji o zgłoszonych przez operatorów usług kluczowych incydentach poważnych i zgłoszonych przez dostawców usług cyfrowych incydentach istotnych, informacje o zgłoszonych incydentach od roku 2020, dane za rok poprzedni muszą być przekazywane do dnia 15 lutego. Dlatego też zmieniono termin przekazania tych danych przez zespoły CSIRT poziomu krajowego do Pojedynczego Punktu Kontaktowego z 30 maja na 31 stycznia.

Zmiana art. 26 ust. 9 ma celu umożliwienie finansowania działalności innej niż bieżaca CSIRT NASK z innych źródeł, niż budżet państwa, np. ze środków pozyskanych przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy w krajowych, regionalnych lub unijnych konkursach lub programach operacyjnych, czy przychodów z działalności Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

W art. 26 dodaje się ust. 12 , zgodnie z którym Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy ds. informatyzacji informują Pełnomocnika o zawarciu przez CSIRT poziomu krajowego porozumienia w sprawie powierzenia sobie wzajemnie wykonywania zadań w stosunku do niektórych rodzajów podmiotów krajowego systemu cyberbezpieczeństwa. Pełnomocnik publikuje komunikat o zawarciu porozumienia na stronie podmiotowej w Biuletynie Informacji Publicznej.

W art. 31 dodaje się obowiązek publikacji przez Pełnomocnika komunikatu o sposobie dokonywania zgłoszeń incydentów do CSIRT poziomu krajowego.

W art. 33 dodaje się obowiązek przeprowadzenia badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa przez CSIRT poziomu krajowego na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT, celem weryfikacji informacji będących w dyspozycji Kolegium, dotyczących możliwych podatności. Wprowadza się także obowiązek publikacji w Biuletynie Informacji Publicznej Pełnomocnika rekomendacji

Pełnomocnika dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

Zmiana w art. 35 ust. 5 polega na tym, że informacje o podatnościach, incydentach krytycznych i cyberzagrożeniach będą publikowane w Biuletynie Informacji Publicznej Pełnomocnika. Podobny charakter (dot. incydentów poważnych i istotnych) mają zmiany w art. 37 ustawy.

W art. 36 ust. 2 rozszerza się zakres podmiotowy Zespołu do spraw Incydentów Krytycznych (dalej: „Zespół"). W skład Zespołu wejdą także przedstawiciele Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Związane jest to z nowymi zadaniami: Pełnomocnika – wydawanie ostrzeżeń, oraz ministra właściwego do spraw informatyzacji – wydawanie poleceń zabezpieczających.

W art. 36b wprowadzony został CSIRT INT, który będzie wspierał placówki dyplomatyczne i konsularne. Przepis ten reguluje zadania jakie zostały wskazane dla nowego CSIRT'u. Przede wszystkim będzie on wspierał ww. podmioty w reagowaniu na incydenty. Zadania te są analogiczne do zadań CSIRT'ów sektorowych. Wprowadzenie tego nowego CSIRT-u zwiększy cyberbezpieczeństwo podmiotów publicznych, które ze względu na swoje szczególne położenie są szczególnie narażone na ataki. Nowy Zespół reagowania na incydenty komputerowe, prowadzony przez Agencję Wywiadu, będzie dysponował najlepszymi dostępnymi środkami do udzielania wsparcia podmiotom położonym poza granicami kraju. CSIRT INT będzie również blisko współpracował w tym zakresie z CSIRT GOV. Art. 36c reguluje obowiązek przekazywania zgłoszeń o incydentach w podmiocie publicznym do CSIRT GOV. Muszą one zostać przekazane niezwłocznie, nie później niż w ciągu 8 godzin od ich otrzymania. Termin ten ma zapewnić, że CSIRT poziomu krajowego będzie odpowiednio poinformowany o sytuacji w całym nadzorowanym przez niego obszarze. To rozwiązanie jest kluczowe dla zapewnienia prawidłowego przepływu informacji między podmiotami krajowego systemu cyberbezpieczeństwa, uwzględniając jednocześnie, aby obowiązek nałożony na ww. rodzaj podmiotów publicznych odbywał się jednotorowo.

W art. 36a wprowadzono możliwość wsparcia zespołów CSIRT poziomu krajowego przez jednostki podległe Ministrowi Obrony Narodowej. Rządowy Zespół Zarządzania Kryzysowego będzie mógł zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia przez podległe mu jednostki.

W art. 37 dodano wyłączenie stosowania ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego, do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów.

Zmiana w art. 42 polega na tym, że wnioski organu właściwego do spraw cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych będą składane bezzwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Ponadto, uchyla się przepisy o powierzeniu kompetencji organu właściwego

do spraw cyberbezpieczeństwa jednostce podległej lub nadzorowanej. Przepisy dotyczą możliwości przeniesienia kompetencji nie były do tej pory stosowane.

Proponowana w nowelizacji nowa treść art. 44 wprowadza obowiązek powołania przez organ właściwy CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał operatorów usług kluczowych tego sektora w obszarze reagowania na incydenty. Projektowane zadania CSIRT sektorowego będą szersze niż obecnych sektorowych zespołów. Zespoły te m.in. będą przyjmować zgłoszenia o wszystkich incydentach i reagować na nie. Będą mogły również gromadzić informacje o podatnościach i cyberzagrożeniach. Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze a także będą mogły, w uzgodnieniu z operatorem usługi kluczowej, wspierać go w wykonywaniu jego obowiązków określonych w rozdziale 3 ustawy .

CSIRT sektorowy będzie niezwłocznie (maksymalnie w ciągu 8 godzin) przekazywał zgłoszenie o incydencie poważnym do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK.

Uchyla się art. 44 ust. 2 ponieważ główną rolę w przekazywaniu informacji o incydentach o charakterze transgranicznym powinny być zespoły CSIRT poziomu krajowego, które są członkami sieci CSIRT Network.

Organ właściwy może powierzyć realizację tych zadań podległym lub nadzorowanym jednostkom. Wprowadza się także możliwość porozumienia się organów właściwych ds. cyberbezpieczeństwa i wyznaczenia wspólnego CSIRT sektorowego dla kilku sektorów. Organ właściwy będzie mógł także, alternatywnie, porozumieć się z organami prowadzącymi CSIRT GOV, CSIRT MON, CSIRT NASK i powierzyć im realizację zadań CSIRT sektorowego. Komunikaty o tych porozumieniach będą publikowane w dzienniku urzędowym organu właściwego oraz w Biuletynie Informacji Publicznej Pełnomocnika.

Utworzenie oraz funkcjonowanie CSIRT sektorowych będzie finansowane z rezerwy celowej, której dysponentem będzie minister właściwy do spraw informatyzacji. Zapewni to skuteczne finansowanie CSIRT sektorowych. Dodatkowo organy właściwe do spraw cyberbezpieczeństwa będą przedkładać sprawozdania z funkcjonowania CSIRT sektorowych Pełnomocnikowi.

Proponowana w nowelizacji zmiana art. 46 określa dostęp podmiotów krajowego systemu cyberbezpieczeństwa do tworzonego na podstawie tego samego artykułu systemu teleinformatycznego. Pełnomocnik oraz zespoły CSIRT poziomu krajowego będą miały stały i nieograniczony dostęp do tego systemu. Prezes UKE oraz zespoły CSIRT sektorowe będą miały dostęp do systemu w obszarze swojej właściwości. Wprowadza się obligatoryjne korzystanie przez operatorów usług kluczowych z tego systemu (od 1 stycznia 2023 r., za wyjątkiem zasady, zgodnie z którą w przypadku wyznaczenia operatora usługi kluczowej od 1 lipca 2022 r., obowiązek ten aktualizuje się w ciągu 6 miesięcy). Pozostałe podmioty

krajowego systemu cyberbezpieczeństwa będą mogły uzyskać dostęp do systemu po podpisaniu porozumienia z ministrem właściwym do spraw informatyzacji. Dostęp do systemu S46 otrzyma także Pełnomocnik.

Zmiana w art. 51 pkt 5 precyzuje, że Minister Obrony Narodowej kieruje działaniami związanymi z obsługą incydentów w czasie stanu wojennego poprzez CSIRT MON.

Po rozdziale 11 zostaje dodany rozdział 11a, zawierający przepisy 59a-59z regulujące krajowy system certyfikacji cyberbezpieczeństwa.

Projektowany art. 59a wyznacza zakres podmiotowy nowego systemu oraz wskazuje organ nadzoru nad jego działaniem. Do systemu będą należały Polskie Centrum Akredytacji, minister właściwy do spraw informatyzacji oraz zainteresowane jednostki oceniające zgodność i przedsiębiorcy certyfikujący swoje produkty. Należy tu podkreślić, że podmioty prywatne nie będą w żaden sposób zmuszone do dołączenia do tego systemu. Obowiązki z niego wynikające będą więc dotyczyć tylko tych, którzy dobrowolnie się im poddadzą. Tyczy się to zarówno jednostek oceniających zgodność jak i wytwórców.

Art. 59b wyznacza zadania dla ministra właściwego do spraw informatyzacji. Zadania te wynikają wprost z przepisów Aktu o cyberbezpieczeństwie i dotyczą nadzoru i kontroli nad podmiotami tego systemu jak również współpracy międzynarodowej w tym zakresie.

Minister właściwy do spraw informatyzacji będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w ustawie o krajowym systemie cyberbezpieczeństwa. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania nowej ustawy.

W ramach obowiązków krajowego organu minister właściwy do spraw informatyzacji będzie prowadzić szereg postępowań administracyjnych dotyczących m.in.:

- zatwierdzania certyfikatów odwołujących się do poziomu zaufania wysoki,
- wydawania zezwoleń na prowadzenie oceny zgodności w przypadku gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających,
- cofania i ograniczania, zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność
- cofnięcia certyfikatu wydanego wbrew przepisom ustawy lub wbrew postanowieniom programu certyfikacyjnego,
- nakładania kar pieniężnych.

Wszystkie rozstrzygnięcia w tym zakresie będą wydawane zgodnie z przepisami Kodeksu postępowania administracyjnego, z zastrzeżeniem, że wydawania zezwoleń na prowadzenie oceny zgodności w przypadku gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających odbędzie się w tzw. postępowaniu uproszczonym, a pozostałe – w ogólnym.

Do obowiązków krajowego organu będą również należeć kwestie współpracy z analogicznymi organami w innych państwach Unii Europejskiej, jak również będzie przeprowadzał wzajemne przeglądy z tymi organami (art. 59b ust. 1 pkt 4). W ramach tych działań organy będą nawzajem oceniać swoje działania i funkcjonowanie krajowych systemów certyfikacji cyberbezpieczeństwa. Konieczność wdrożenia tej procedury wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

Projektowany art. 59c wyznacza rolę Polskiego Centrum Akredytacji (dalej „PCA"), które będzie nadzorowało jednostki oceniające zgodność pod kątem spełnienia przez nie wymogów akredytacji. PCA będzie tu pełniło taką samą rolę jaką pełni w ogólnym systemie oceny zgodności. Zapewni to szybkie wdrożenie nowych przepisów w praktyce.

Zgodnie z projektowanym art. 59d krajowe programy certyfikacyjne będą określane w drodze rozporządzeń Rady Ministrów. Przy ich tworzeniu będzie brany pod uwagę obecny stan wiedzy w dziedzinie techniki oraz kwestia potrzeb rynku w zakresie cyberbezpieczeństwa. Dzięki temu programy certyfikacyjne będą brały pod uwagę konkretne potrzeby przedsiębiorców oraz promować w tym zakresie najlepsze rozwiązania z tej dziedziny. Podstawą działania krajowego systemu certyfikacji cyberbezpieczeństwa będą jednak europejskie programy certyfikacyjne, dlatego też niniejszy przepis został ukształtowany jako fakultatywny. Dzięki temu organy będą mogły przygotowywać krajowe programy certyfikacyjne w sytuacji gdy uznają to za korzystne dla rozwoju certyfikacji w Polsce. Przygotowanie projektu krajowego programu certyfikacji cyberbezpieczeństwa jest zadaniem ministra właściwego do spraw informatyzacji. Ze względu na konieczność szerokiego wykorzystania wiedzy specjalistycznej w ramach tych prac minister będzie mógł zlecić przygotowanie takiego dokumentu jednostkom przez siebie nadzorowanym np. instytutom badawczych takim jak NASK czy Instytut Łączności.

Art. 59e określa jakie obowiązki będą mogły określone w treści krajowych programów certyfikacyjnych. Zostały one określone w sposób ogólny tak by ich szczegóły znajdowały się już w konkretnym programie. Pozwoli to ustawodawcy dostosować te obowiązki do potrzeb związanych z konkretnymi technologiami. Dzięki temu obowiązki będą wprowadzane tylko tam gdzie będzie to absolutnie konieczne.

Celem krajowych programów certyfikacji cyberbezpieczeństwa jest zapewnienie, by produkty ICT, usługi ICT i procesy ICT, certyfikowane zgodnie z takimi programami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem

tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe na poziomie ustawy szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane. W szczególności mając na uwadze, że dotyczy to tak różnych produktów jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych, w przypadku gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów zapewni skuteczność tych programów. Trzeba wskazać, że ta różnorodność wpływa na wszelkie aspekty tych programów np. w przypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady przez jego aktualizacje podczas gdy wykrycie określonej podatności w przenośnej pamięci USB może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w programie może wymagać zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.

Projektowane art. 59 f-g wyznaczają elementy krajowych programów certyfikacyjnych oraz wskazują poziomy uzasadnienia zaufania do których będą odwoływać się certyfikaty. Przepisy te zostały przygotowane na wzór odpowiednich przepisów Aktu o cyberbezpieczeństwie przewidującym trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania jakie musi spełniać produkt by uzyskać certyfikat danego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Dzięki temu możliwa będzie promocja krajowych programów certyfikacyjnych w całej Unii Europejskiej i stosunkowo łatwe przenoszenie ich na poziom europejski. Ponadto takie rozwiązanie zapewni porównywalność certyfikatów krajowych z dokumentami z innych państwach członkowskich oraz sprawi, że certyfikaty będą bardziej przejrzyste dla zagranicznych klientów.

Projektowany art. 59h wyznacza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji. Aby prowadzić badania produktów, usług i procesów ICT podmioty będą musiały uzyskać akredytację PCA. Wymagania dla zainteresowanych zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. PCA będzie procedować na podstawie

przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Są to przepisy na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania z ich strony.

Sprawna wymiana informacji między PCA sprawującym nadzór nad akredytacją oraz ministrem właściwym do spraw informatyzacji jest niezbędna do sprawnego działania nowego systemu. W związku z tym PCA będzie informować ministra o dokonanych akredytacjach oraz o odmowie ich dokonania. Proponowane rozwiązania gwarantują, że minister właściwy do spraw informatyzacji będzie należycie poinformowany o wszystkich podmiotach wydających certyfikaty oraz będzie posiadał informacje niezbędne do prowadzenia nadzoru nad tym rynkiem.

Art. 59i reguluje sytuację, gdy program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku, oprócz akredytacji, te jednostki będą musiały uzyskać zezwolenia ministra właściwego do spraw informatyzacji. Zezwolenia określone w projektowanym art. 59i wynikają wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Jeśli bowiem europejskie lub krajowe programy certyfikacyjne będą zawierały postanowienia o szczególnych wymaganiach w zakresie jednostek oceniających zdolność musi istnieć organ sprawdzający te wymagania oraz zezwalający na ich działanie w ramach określonego programu certyfikacji. Taka regulacja wynika wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Należy podkreślić, że w związku z tym, iż postępowanie to dotyczy spełnienia formalnych kryteriów, zdecydowano o zastosowaniu w tym przypadku przepisów o postępowaniu uproszczonym. Pozwoli to maksymalnie przyśpieszyć to postępowanie oraz ograniczy formalności. Minister w ramach sprawowanego nadzoru będzie mógł również zmieniać zakres tego zezwolenia jak i cofnąć je w przypadku gdyby określona jednostka przestała spełniać określone wymagania. Gwarantuje to zachowanie odpowiedniej jakości usług świadczonych przez jednostki oceniające zgodność.

Nowo dodane przepisy art. 59 j-k wyznaczają ogólne zasady związane z oceną zgodności i zasadami wydawania certyfikatów. Są one utworzone w sposób analogiczny do przepisów dot. systemu oceny zgodności. Są one utworzone w sposób analogiczny do przepisów dotyczących systemu oceny zgodności. Wskazują one wyraźnie, że poddanie produktów, usług i procesów ICT ocenie zgodności jest całkowicie dobrowolne. Warunki przeprowadzania oceny zgodności będą określane w europejskich i krajowych programach certyfikacji.

Przepisy te określają kiedy otrzymuje się certyfikat oraz kiedy możliwe jest wydanie deklaracji zgodności. W przypadku najniższego poziomu zaufania producent może sam przeprowadzić badanie produktu, a następnie wskazać w deklaracji zgodności, że produkt spełnia wymagania. Takie rozwiązanie stanowi ważne ułatwienie dla przedsiębiorców chcących uzyskać certyfikację przy możliwie najmniejszych kosztach. Będą mogli bowiem sami przeprowadzić niezbędne badania i wystawić deklarację zgodności. Równocześnie należy tu

wspomnieć, że dalsze przepisy penalizują wprowadzanie w błąd w zakresie spełniania wymagań certyfikacyjnych. W związku z tym istnieje zabezpieczenie przed nadużywaniem tego rozwiązania. Otrzymanie certyfikatu wymaga przeprowadzenia badań produktu, usługi lub procesu ICT przez niezależny podmiot. Jest to niezbędna gwarancja dla prawidłowego przebiegu procesu certyfikacji. Należy nadmienić, że możliwość wystawienia deklaracji zgodności dotyczy jedynie najniższego poziomu uzasadnienia zaufania.

Art. 59l określa zagadnienia związane z wnioskiem o certyfikację w szczególności minimalne wymagania co do treści takiego wniosku. W celu usprawnienia działań podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa wszystkie dokumenty relewantne dla tego wniosku powinny zostać złożone wraz z nim. Projektowane przepisy mają zabezpieczyć prawidłowe i sprawne prowadzenie oceny zgodności. Art. 59m wyznacza obowiązek jednostki oceniającej zgodność do przekazania ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jej cofnięcia. Obowiązek ten jest konieczny gdyż umożliwia ministrowi sprawowanie skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa.

Projektowany art. 59n daje dodatkową gwarancję dla certyfikatów najwyższego poziomu. Taki certyfikat musi być zatwierdzony przez ministra właściwego do spraw informatyzacji. Dotyczy to zarówno certyfikatów wydanych na podstawie europejskich jak i krajowych programów certyfikacji cyberbezpieczeństwa. Odmowa zatwierdzenia jest możliwa w przypadku, gdy certyfikat został wydany wbrew przepisom lub postanowieniom programu certyfikacyjnego w ramach, którego prowadzona była ta procedura. Do tego postępowania będą stosowane przepisy Kodeksu postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe dla ich stron. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające przebieg procesu oceny zgodności. Wymóg ten służy do przyśpieszenia postępowania przez przekazanie do organu potrzebnych mu dokumentów wraz z wnioskiem wszczynającym postępowanie. Bez tego przepisu organ musiałby wystąpić o te dokumenty co przedłużyłoby cały proces. Przepis ten reguluje również kwestie cofania certyfikatów wydanych niezgodnie z ustawą lub przepisom programu certyfikacyjnego. Obowiązek wprowadzenia takiej procedury wynika z Aktu o cyberbezpieczeństwie.

Projektowany art. 59o reguluje, kiedy jednostka oceniająca zgodność odmawia dokonania certyfikacji. Może to nastąpić jedynie w przypadku gdy dany projekt nie spełnia wymagań określonych w procesie certyfikacji. Ponadto, przy odmowie certyfikacji jednostka oceniająca zgodność musi wyraźnie wskazać, które wymagania nie są spełnione przez dany produkt. Zapewnia to, że każda decyzja odmowna będzie jasno wskazywała jej przyczyny umożliwiając klientowi odwołanie się od niej.

Projektowany art. 59p reguluje jakie informacje musi zawierać certyfikat. Każdy z certyfikatów wskazuje komu został wydany, jakiego produktu dotyczy oraz kto go wydał. Ponadto każdy z nim będzie

posiadał indywidualny numer, wskazywał w ramach jakiego programu został wydany, jakiego poziomu uzasadnienia zaufania dotyczy oraz okres na jaki certyfikat został wydany. Przepis ten gwarantuje, że wydany dokument będzie zawierał wszystkie informacje niezbędne do jego wykorzystania w obrocie gospodarczym.

Projektowany art. 59q reguluje sytuację, gdy produkt, usługa lub proces ICT przestają spełniać wymagania już po otrzymaniu certyfikatu. Programy certyfikacyjne będą przewidywać zasady monitorowania produktów, usług i procesów, które uzyskały certyfikaty. W ramach tego monitoringu właściciele certyfikowanych produktów będą musieli wykazać, że ich towar wciąż spełnia wymagania określone w programie. W przypadku gdy przestanie je spełniać jednostka oceniająca zgodność obowiązana jest do cofnięcia certyfikatu. Musi również o tym poinformować ministra właściwego do spraw informatyzacji. Otrzymywanie takich informacji jest niezbędny by minister mógł wykonywać swoje obowiązki związane z nadzorem nad rynkiem certyfikacji.

Projektowany art. 59r reguluje kwestie związane z deklaracjami zgodności. Możliwość ich wydawania dotyczy tylko najniższego poziomu uzasadnienie zaufania i daje szansę skorzystania z programów certyfikacyjnych przy minimalnych kosztach. Producenci będą mogli sami wskazać, że ich produkty spełniają wymagania bez potrzeby przechodzenia przez proces certyfikacji co pozwoli im znacząco ograniczyć posiadane koszty.

Projektowany art. 59s nakłada na podmioty krajowego systemu certyfikacji cyberbezpieczeństwa obowiązek przesyłania kopii wystawionych deklaracji zgodności do ministra właściwego do spraw informatyzacji. Przepis ten gwarantuje, że minister będzie zdolny do wykonywania nadzoru nad tym rynkiem. reguluje, kiedy jednostka oceniająca zgodność odmawia dokonania certyfikacji.

Projektowany art. 59t ustanawia domniemanie zgodności z wymogami produktów dla których wystawione zostały deklaracje zgodności.

Zgodnie z projektowanym art. 59u podmiot, którego produkt, usługa czy proces ICT zostały certyfikowany jest obowiązany zapewnić by spełniał on wymogi określone w programie certyfikacji przez cały cykl życia danego produktu. Musi on również udostępniać użytkownikom wszelkie informacje niezbędne do bezpiecznego z nich korzystania. Postanowienia te są niezbędne do właściwego funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa. Produkty wymagają bowiem odpowiednio wyszkolonego personelu wsparcia by pełnić przypisaną im funkcję. Ponadto, w przypadku wielu produktów, usług i procesów ICT ciągłe aktualizacje są niezbędnym elementem zapewnienia bezpieczeństwa. Wiele z najbardziej skutecznych cyberprzestępstw dotykało urządzeń, które nie przeszły niezbędnych aktualizacji oprogramowania jak np. w czasie rozprzestrzeniania się wirusa WannaCry. Dlatego zagwarantowanie bezpieczeństwa systemów informacyjnych wymaga nałożenia takich obowiązków na ich dostawców.

Art. 59v określa obowiązki udostępniania informacji nałożone na dostawców certyfikowanych produktów. Regulacje te są niezbędne dla zapewnienia skutecznego nadzoru nad całym systemem krajowym systemie certyfikacji cyberbezpieczeństwa.

Art. 59w dodaje kolejną metodę sprawowania nadzoru przez ministra właściwego do spraw informatyzacji. Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa będę musiały przekazywać ministrowi wyjaśnienia w kwestiach związanych z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa. Daje to ministrowi możliwość sprawdzania otrzymywanych informacji bez konieczności stosowania długotrwałej i uciążliwej dla przedsiębiorcy procedury kontrolnej. Umożliwi to również ministrowi zbieranie informacji o zjawiskach zachodzących na rynku certyfikacji.

Projektowane art. 59w daje podstawę prawną dla prowadzenia kontroli u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji. Do kontroli będą stosowane dotychczasowe przepisy ustawy o krajowym systemie cyberbezpieczeństwa. Dzięki temu organ będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli. Pozwoli to na najszybsze wdrożenie się organu do nowych obowiązków. W przypadku kontroli u podmiotów administracyjnych będzie stosowana ustawa o kontroli w administracji rządowej, a w przypadku przedsiębiorców stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. W związku z tym wszelkie gwarancje dla przedsiębiorców będą zachowane w tej procedurze. Ponadto będą stosowane przepisy art. 55-59 ustawy. W art. 55 w punktach od 1 do 6 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, przesądzono, że osoba prowadząca czynności kontrolne, legitymująca się odpowiednimi dokumentami upoważniającymi do kontroli, ma prawo do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki. Warto zaznaczyć, że uprawnienia wynikające z art. 55 dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że uprawnienia te nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli.

Art. 57 wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58).

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 art. 59 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. Wskazana powyżej regulacja jest istotna z punktu widzenia regulacji zawartych w rozdziale 14 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. Zgodnie z obowiązującymi regulacjami w podobnych dziedzinach, od zaleceń pokontrolnych nie przysługują środki odwoławcze, natomiast wymierzanie kar pieniężnych będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych (z możliwością zaskarżenia w toku administracyjnym i sądowym).

Ważnym elementem zagwarantowania jakości i przejrzystości procesów oceny zgodności są przepisy dotyczące skarg. Zainteresowanym udostępniono tu dwa tryby składania skarg na jednostki oceniające zgodność. Po pierwsze, jednostki te muszą udostępniać swoim klientom procedury składania skarg do ich wewnętrznych organów (art. 59yz). Dzięki temu każdy zainteresowany będzie mógł wskazać nieprawidłowości samej jednostce z którą zawarł umowę. Przepisy wskazują też na minimalne wymagania jakie muszą spełniać wewnętrzne procedury rozpatrywania skarg tak by zapewnić prawidłowy przebieg tego procesu np. obowiązek rozpatrywania skargi przez osoby, które nie prowadziły wcześniej oceny zgodności. Równocześnie osoby zainteresowane mogą też złożyć skargę na daną jednostkę oceniającą zgodność do ministra właściwego do spraw informatyzacji (art. 59z ust. 1). Ta skarga może być podstawą do podjęcia działań nadzorczych wobec danej jednostki , przeprowadzenia audytu czy kontroli w tej jednostce.

Obie procedury dotyczące skarg są od siebie niezależne i mogą być prowadzone równolegle. Daje to zainteresowanym swobodę wyboru postępowania w przypadku niezadowolenia z postępowania jednostki oceniającej zgodność. Nie ograniczają też w żaden sposób uprawnień poszczególnych podmiotów do dochodzenia swoich praw na drodze sądowej.

Projektowany art. 59z wskazuje, że minister właściwy do spraw informatyzacji jest też organem właściwym do rozpatrywania skarg na unijne i krajowe deklaracje zgodności dotyczące cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt dla którego wystawiono deklarację zgodności nie spełnia wymagań określonych w programie certyfikacji. To uprawnienie dla ministra wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

Skargi składane do ministra właściwego do spraw informatyzacji rozpatrywane będą zgodnie z przepisami kodeksu postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra wskazano, że przepisy te będą stosowane odpowiednio.

Przepis art. 62a będzie umożliwiał wypłacanie świadczenia teleinformatycznego, które będzie dodatkiem do wynagrodzenia lub dodatkiem do uposażenia. Przysługiwać będzie osobom realizującym zadania w CSIRT poziomu krajowego, CSIRT INT, CSIRT sektorowych, w organach właściwych do spraw cyberbezpieczeństwa, Pełnomocnika, a także wykrywaniem i ściganiem sprawców tych przestępstw, zapewnienia cyberbezpieczeństwa w

- Centralnym Biurze Antykorupcyjnym,
- Kancelarii Prezesa Rady Ministra oraz urzędach obsługujących ministrów.
- Policji,
- Prokuraturze,
- Służbie Kontrwywiadu Wojskowego,
- Służbie Wywiadu Wojskowego,
- Straży Granicznej.

Wysokość wynagrodzenia za pracę albo uposażenia z uwzględnieniem świadczenia teleinformatycznego może wynosić maksymalnie do dwudziestojednokrotności kwoty bazowej dla członków korpusu służby cywilnej, ustalanej w ustawie budżetowej.

Rada Ministrów określi, w drodze rozporządzenia warunki przyznawania i ustalania świadczenia teleinformatycznego; kwalifikacje zawodowe wymagane na stanowiskach, na których realizowane są zadania, za które przysługuje świadczenie teleinformatyczne, oraz sposób ich weryfikacji przez kierownika właściwego podmiotu; sposób obliczania wysokości dodatku do uposażenia; wysokość dodatku do wynagrodzenia oraz wysokość dodatku do uposażenia.

Proponowane rozwiązanie zapewni wysoko wykwalifikowaną kadrę dla podmiotów publicznych zajmujących się cyberbezpieczeństwem państwa.

Artykuł 62b umożliwi wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania cyberbezpieczeństwa systemów informacyjnych podmiotów

krajowego systemu cyberbezpieczeństwa. Będą one publikowane na stronie podmiotowej w Biuletynie Informacji Publicznej Pełnomocnika. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej, a także inne zbiory dobrych praktyk. Rekomendacje będą formalnie niewiążące, jednak podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić je w ramach procesu zarządzania ryzykiem. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne zabezpieczenia.

W nowym art. 64a określone zostały nowe rodzaje analiz jakie będą mogły być zlecane CSIRT GOV CSIRT MON lub CSIRT NASK. Będą to analizy dotyczące wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1 oraz analizy dotyczące trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. Analizy te będą wykonywane na wniosek Przewodniczącego Kolegium ds. Cyberbezpieczeństwa i będą mogły posłużyć jako dowód w ramach postępowania o uznanie dostawcy za dostawcę wysokiego ryzyka. .

W art. 66 dokonuje się rozszerzenie składu Kolegium, poprzez dodanie jako członków: ministra właściwego do spraw energii, Przewodniczącego Komisji Nadzoru Finansowego oraz kierownika państwowej jednostki budżetowej podległej lub przez nadzorowanej przez Ministra Obrony Narodowej, właściwej w zakresie cyberbezpieczeństwa, jeżeli został wyznaczony przez Ministra Obrony Narodowej. Takim kierownikiem może być np. Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, które jest właściwe w zakresie realizacji zadań związanych z konsolidacją kompetencji i zasobów resortu obrony narodowej w obszarze związanym z cyberbezpieczeństwem, kryptologią, a także informatyzacją W posiedzeniach Kolegium będą mogli także uczestniczyć: Szef Służby Kontrwywiadu Wojskowego albo jego zastępca, Szef Służby Wywiadu Wojskowego albo jego zastępca oraz Szef Centralnego Biura Antykorupcyjnego albo jego zastępca. Ponadto, umożliwiono, aby pozostali szefowie służb (wymienieni w ust. 4) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

W ślad za odpowiednimi zmianami w przepisach, uzupełniono katalog kompetencji przewodniczącego Kolegium, który poza zwołaniami posiedzeń Kolegium i uprawnieniem do zapraszania do udziału posiedzeniach Kolegium przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych, przedstawicieli organów właściwych do spraw cyberbezpieczeństwa oraz innych osób, których uczestnictwo jest niezbędne ze względu na tematykę obrad, może także:

- pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;

- zlecić CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;
- zlecić CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;
- wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1.

Przewodniczący Kolegium ma także kompetencję do powołania zespołu opiniującego, o którym mowa w art. 66a ust. 10 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład, a także rozstrzyga spór, o którym mowa w art. 66a ust. 10 pkt 2, wskazując właściwego członka zespołu opiniującego.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka

Zawarty w rozdziale I Konstytucji[9] art. 20 stanowi o ustroju gospodarczym Rzeczpospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości podejmowania się działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym[10)]. Państwo może, więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[11)]. Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłoby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego a także prawno-międzynarodowym zobowiązaniom państwa jak również zdrowiu obywateli[12)]. Tutaj warto dodać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady

[9] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 nr 78 poz. 483, z 2001 r. nr 28 poz. 319, z 2006 r. nr 200 poz. 1471, z 2009 r. nr 114 poz. 946).
[10)] Wyrok Trybunału Konstytucyjnego z dnia 8 kwietnia 1998 r., sygn. K 10/97.
[11)] Ibidem.
[12)] Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01.

Ministrów jest również zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji).

W ślad za powyższym projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy, który zostanie uznany jako dostawca wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Wymóg ten ukierunkowany jest na zapewnienie ważnego interesu państwowego – obecnie nie ma żadnych środków prawnych umożliwiających wycofywanie z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowania państwa. Nowe rozwiązania pozwolą na wycofanie produktów, usług i procesów ICT, które m.in. w wyniku wykorzystania znanych oraz nie wykrytych jeszcze podatności przez obce służby wywiadowcze są z powodów technicznych na tyle niebezpieczne, że ich masowe użycie w kluczowej infrastrukturze państwa mogłoby poważnie zagrozić bezpieczeństwu narodowemu. Warto tutaj dodać, że podczas pandemii COVID-19 to właśnie dzięki powszechnemu wykorzystywaniu nowoczesnych technologii zapewnianych przez produkty ICT, usługi i procesy ICT administracja rządowa, gospodarka a przede wszystkim wszyscy obywatele są w stanie bezpiecznie funkcjonować, pracować, czy uczyć się. Przewidzenie więc procedury umożliwiającej uznanie dostawcy za dostawcę wysokiego ryzyka oceny ryzyka jest zatem jak najbardziej uzasadnione.

Proponowane przepisy mogą ograniczyć swobodę podejmowania decyzji gospodarczych przez podmioty zobowiązane do wycofania wskazanych w decyzji administracyjnej typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT. Wpłyną również na konkurencję na rynku typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT przez dostawcę wysokiego ryzyka. Należy przy tym zauważyć, że proponowany mechanizm zakłada przeprowadzenie transparentnego, szczególnego postępowania administracyjnego, które będzie mogło być skontrolowane przez sąd administracyjny. Wobec tego zostanie zapewniona możliwość przedstawienia swoich racji i ochrony swojego interesu przez dostawcę sprzętu lub oprogramowania. Proponowane rozwiązania są w stanie doprowadzić do zwiększenia bezpieczeństwa narodowego. Niewątpliwie wprowadzana procedura, w przypadku zastosowania, wiązać się będzie do kolizji dwóch wartości konstytucyjnych – swobody prowadzenia działalności gospodarczej (przez dostawcę sprzętu lub oprogramowania oraz podmioty zobowiązane do wycofania sprzętu) oraz bezpieczeństwa narodowego. Ważąc te dwie wartości wyraźnie należy stwierdzić, że w możliwe są konkretne sytuacje, określone przez przepisy ustawy, w których ochrona bezpieczeństwa narodowego powinna mieć prymat nad swobodą prowadzenia działalności gospodarczej. Prawidłowe funkcjonowanie obrotu gospodarczego nie jest możliwe w sytuacji, gdyby państwo, w ramach zapewniania swobody gospodarczej, dopuszczało do korzystania przez podmioty gospodarcze o kluczowym dla niego znaczeniu ze sprzętu

niebezpiecznego, z ukrytymi podatnościami, lub pochodzącego od dostawcy, na którego wpływ mają podmioty nastawione wrogo wobec państwa. Stałoby to w jaskrawej sprzeczności z zapewnieniem swobody działalności gospodarczej, ponieważ jej wykonywanie ograniczałby wpływ podmiotów zewnętrznych. Ponadto zagrażałoby to ochronie bezpieczeństwa narodowego jako elementowi dobra wspólnego jakim jest Rzeczpospolita Polska. W sposób oczywisty stałoby to w sprzeczności z wartościami konstytucyjnymi. Dlatego należy uznać, że proponowane rozwiązania są zasadne i odpowiednie, czyli umożliwiają skutecznie ochronić państwo i rynek nowych technologii przed produktami niebezpiecznymi.

W art. 66a została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia, w celu ochrony ważnego interesu państwowego, postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W rozumieniu tego artykułu dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Postępowanie nie będzie dotyczyło wszystkich produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych, czy podmioty publiczne (ok. 4000 podmiotów);

2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (ok. 100 podmiotów);

3) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej w uzasadnieniu zwani operatorami infrastruktury krytycznej (100-200 podmiotów);

4) przedsiębiorców o szczególnym znaczeniu gospodarczo obronnym.

Podmioty te są szczególnie ważne dla zapewnienia społeczno-ekonomicznego bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu w trakcie świadczenia usług na rzecz państwa i obywateli.

Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały zastosowanie przepisy Kodeksu postępowania administracyjnego (Kpa). Dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach stronnych, z odmiennościami wynikających ze szczególnych regulacji (odmienności) wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane przepisy następujących artykułów Kpa:

- Art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Katalog stron będzie więc określony przez organ wszczynający postępowanie.
- Art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
- Art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
- Art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
- Art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu;

Wyłączenia tych przepisów Kpa są niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego. Zawężenie przymiotu strony oraz udziału organizacji społecznej jest koniecznej w celu uniknięcia obstrukcji postępowania i wzmocnić trwałość rozstrzygnięć, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania.

Decyzja ministra właściwego do spraw informatyzacji będzie miała formę decyzji administracyjnej, co pozwoli dostawcy na składanie złożenie skargi na decyzję administracyjną do wojewódzkiego sądu administracyjnego.

W przypadku, gdy dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) zawiadomienie o wszczęciu postępowania publikowane jest na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Publikacja ma skutek doręczenia po upływie 14 dni od dnia jej dokonania. Przepis ten stanowi szczególną regulacją w stosunku do zasad doręczeń określonych w Kpa.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek przewodniczącego Kolegium. Gdy postępowanie zostanie wszczęte, minister właściwy ds. informatyzacji będzie zobowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy. Opinia Kolegium będzie mogła być objęta skargą do sądu łącznie z decyzją.

Art. 66a ust. 8 zawiera wskazanie elementów analizy która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[13)]. W ramach opinii będzie zawarta analiza dostawcy sprzętu lub oprogramowania na podstawie aspektów technicznych i nietechnicznych. Analizowane będą powiązania dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego oraz powiązania z podmiotami wobec których Unia Europejska zastosowała sankcje za cyberataki. Innym nietechnicznym aspektem będzie analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania.

Do technicznych aspektów opinii należy analiza:

1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

2) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów o których mowa w ust. 1 pkt. 1-4 oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

3) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.

Podkreślić należy, że nie jest możliwe ograniczenie się w analizie dostawcy sprzętu lub oprogramowania wyłącznie do aspektów technicznych oferowanych przez niego produktów ICT, usług ICT, czy procesów ICT. Postęp technologiczny nie tylko zapewnił poprawę jakości komunikacji ale także umożliwił nowe formy ingerencji państw trzecich w bezpieczeństwo narodowe. Coraz więcej urządzeń jest stale podłączonych do globalnej sieci, co powoduje że w każdej chwili jest przesyłana ogromna ilość danych. Dla służb wywiadowczych obcych państw są to potencjalnie potężne zasoby informacyjne, które mogą zostać wykorzystane przeciwko Polsce. Ponadto, dostęp do urządzeń stale podłączonych do sieci poprzez ukryte (lub celowo zaprojektowane) podatności mógłby skutkować przejęciem kontroli nad znaczną liczbą urządzeń używanych przez podmioty krajowego systemu cyberbezpieczeństwa, czy operatorów infrastruktury krytycznej. W konsekwencji niezbędne jest aby istniała prawna formuła zidentyfikowania dostawcy wysokiego ryzyka i ograniczenia używania oferowanego przez niego sprzętu lub oprogramowania.

[13)] *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

Procedura sporządzania opinii Kolegium została określona w art. 66a ust. 10. Opinia zostanie przygotowana przez zespół opiniujący w skład którego wchodzą przedstawiciele członków Kolegium. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium będzie miał kompetencję do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego.

Po przeprowadzeniu postępowania minister właściwy ds. informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Decyzja będzie zawierać wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – zagrożenie dla bezpieczeństwa narodowego – decyzja ta będzie podlegała natychmiastowej wykonalności.

Aby podmioty mogły zastosować się do obowiązków wynikających z decyzji administracyjnej, minister właściwy do spraw informatyzacji publikuje ją w Dzienniku Urzędowym Monitor Polski, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy.

Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia, a także przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów, usług i procesów, jak i używanych.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji.

Natomiast przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem

dla bezpieczeństwa Państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3.

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Podobne kompetencje będzie miał w stosunku do przedsiębiorców telekomunikacyjnych Prezes UKE.

W artykule 66d wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze *lex specialis* do ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2019 r. poz. 2325, z 2020 r. poz. 2299 i 2320, z 2021 r. poz. 54, 159, 1598) (dalej – PPSA). Jest on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[14)]. Przepis stanowi odstąpienie od zasady ustności i jawności, jednakże strona i tak będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym. Sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Ze względu na szczególny interes bezpieczeństwa państwa, zgodnie z art. 61 § 3 PPSA, dodano ust. 3 który wyłącza wstrzymanie wykonania zaskarżonej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka przez sąd administracyjny.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy

[14)] Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14.

telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia.

Art. 66e określa, że minister właściwy do spraw informatyzacji będzie prowadził wykaz decyzji o uznaniu za dostawcę wysokiego ryzyka w podziale na produkty, usługi i procesy w nich wskazane. Ułatwi to dostęp do informacji o potencjalnie niebezpiecznych produktach.

Ostrzeżenie i polecenie zabezpieczające

Przepisy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zawierają dodanie dwóch specjalnych środków – ostrzeżenia oraz polecenia zabezpieczającego (art. 67a – 67c). Ich stosowanie będzie ograniczone do niektórych grup podmiotów gospodarki i społeczeństwa. Będą mogły być stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) lub po zaistnieniu incydentu krytycznego, w celu skoordynowania efektywnej reakcji (polecenie zabezpieczające). Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie – po przeprowadzeniu należytej oceny – może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.

Przed wydaniem ostrzeżenia lub polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.

Zarówno ostrzeżenie jak i polecenie będą musiały zawierać:

1) wskazanie rodzajów ryzyk;

2) wskazanie rodzajów podmiotów, których dotyczy;

3) uzasadnienie zawierające wyniki analizy przeprowadzonej przez Zespół do spraw incydentów krytycznych.

Pełnomocnik będzie mógł wydać ostrzeżenie, które będzie miękkim, niewiążącym środkiem wskazującym na ryzyko związane z możliwością wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko wystąpienia tego incydentu. Instrument ten jest wzorowany na ostrzeżeniach wydawanych przez czeską Narodową Agencję Bezpieczeństwa Cybernetycznego i Informacji. Ostrzeżenie jako miękki środek będzie zawierało zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu. Katalog możliwych zaleceń został wskazany w art. 67a ust. 8. Decyzja o zastosowaniu się do ostrzeżenia przez operatorów usług kluczowych będzie należeć do nich samych, przepis jedynie zobowiązuje ich do uwzględnienia ostrzeżenia podczas procesu szacowania ryzyka.

Z kolei minister właściwy do spraw informatyzacji będzie mógł wydać w formie decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Polecenie zabezpieczające będzie wydawane w sytuacji zapewnienia koordynacji reakcji na incydent krytyczny oraz konieczności ograniczenia skutków tego incydentu. Zawarte w nim będzie wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Katalog tych zachowań został wskazany w art. 67b ust. 7.

Polecenie zabezpieczające będzie miało charakter decyzji generalnej, a więc będzie skierowane w konkretnej sprawie do podmiotów ustalonych rodzajowo. Przemawia za tym fakt, że niemożliwe jest zidentyfikowanie ile dokładnie podmiotów mogłoby być ofiarami incydentu krytycznego.

Decyzje generalne są znane w prawie administracyjnym państw UE[15], jak również w doktrynie i praktyce w polskim prawie sprzed 1997 r. Decyzja generalna to jeden z rodzajów aktu administracyjnego, a zatem akt stosowania prawa, a nie jego stanowienia (jak np. rozporządzenia czy ustawy)[16]. Ma charakter generalno-konkretny, czyli wymagają poczynienia ustaleń faktycznych i przyporządkowania (podciągnięcia) stanu faktycznego pod daną normę. Odróżnia je to od aktów normatywnych, które wiążą co do zasady wszystkich[17].

Nie jest to nowa forma stanowienia prawa, a raczej specyficzny rodzaj aktu administracyjnego, działający obok, a nie zamiast decyzji administracyjnej. Decyzja administracja charakteryzuje się tzw. podwójną konkretnością (konkretny adresat i konkretna sprawa), natomiast anty normatywne są podwójnie ogólne (generalnie określony adresat i abstrakcyjnie opisana sprawa). Akty generalne charakteryzują się natomiast ogólnie określonym adresatem i konkretnie określoną sprawą.

Decyzje generalne, mimo braku sformalizowanych zasad procedowania, są stosowane w polskim prawie. Przykładem mogą być niektóre uchwały Komisji Nadzoru Finansowego (dawny art. 71 ustawy z dnia 29

[15] Przykładem mogą być: Niemcy, Grecja, Hiszpania i Portugalia oraz – jako przedstawiciel EOG – Norwegia.
[16] Zbigniew Kmieciak (red.), *Raport Zespołu Eksperckiego z prac w latach 2012-2016 – Reforma prawa o postępowaniu administracyjnym*, Warszawa 2017.
[17] E. Szewczyk, M. Szewczyk, *Między indywidualnym aktem administracyjnym a aktem normatywnym,* Warszawa 2014.

sierpnia 1997 r. - Prawo bankowe[18]), Wykaz Produktów Leczniczych Dopuszczonych do Obrotu na terytorium Rzeczypospolitej Polskiej (art. 4 ust. 1 pkt 1 lit. j ustawy z dnia 18 marca 2011 r. o Urzędzie Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych[19]) czy też rozstrzygnięcia Głównego Inspektora Sanitarnego (art. 27 ust. 1 i 2 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej[20]).

Do postępowania nie będą miały zastosowania przepisy art. 10, art. 34, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 Kodeksu postępowania administracyjnego, a inne przepisy Kpa będą stosowane odpowiednio. Wyłączenia ww. przepisów są faktem, że w przypadku decyzji generalnych niemożliwe są do zidentyfikowania wszystkie strony postępowania. Wyłączenia w projekcie nawiązują do poglądów doktryny[21]. Zawiadomienia w sprawie będą doręczane poprzez publiczne obwieszczenie na stronie podmiotowej ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej. Samo polecenie zabezpieczające będzie ogłoszone w dzienniku urzędowym ministra właściwego do spraw informatyzacji oraz na stronie podmiotowej ministra w Biuletynie Informacji Publicznej lub na stronie internetowej urzędu obsługującego ministra.

Wskazane w poleceniu zabezpieczającym określone zachowanie ma być adekwatne do sytuacji – minister nie będzie mógł więc arbitralnie wskazać zachowanie, tylko wybrać takie, które, w świetle analizy, będzie proporcjonalne do sytuacji wywołanej incydentem krytycznym.

Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata, a wygasa z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji lub po upływie czasu, na które zostało wydane.

Z uwagi na konstytucyjną niezależność Narodowego Banku Polskiego nie będą do niego stosowały się przepisy dotyczące wycofania produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka. Nie będzie także zobowiązany do poddania się obowiązkom wynikających z polecenia zabezpieczającego. Minister właściwy do spraw informatyzacji będzie informował Prezesa Narodowego Banku Polskiego o wydaniu decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka oraz o wydaniu polecenia zabezpieczającego. Prezes Narodowego Banku Polskiego zdecyduje zatem czy wycofa

[18] Dz. U. z 2015 r. poz. 128.
[19] Dz.U. z 2020 r. poz. 836
[20] Dz.U. z 2021 r. poz. 195.
[21] Rozdział 7.4 E. Szewczyk, M. Szewczyk, *Generalny akt administracyjny: między indywidualnym aktem administracyjnym a aktem normatywnym*, Wolters Kluwer 2014.

produkty ICT, usługi ICT oraz procesy ICT wskazane w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka.

W art. 67e dodano opcjonalną możliwość przekazania zadań zespołów CSIRT, określonych w art. 26, Ministrowi Obrony Narodowej. Decyzję w tej sprawie podejmie Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa oraz w uzgodnieniu z Ministrem Obrony Narodowej. W decyzji zostaną określone m. in. zakres, czas powierzenia zadań a także fakultatywnie szczegóły współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV.

Fundusz Cyberbezpieczeństwa

Tworzy się Fundusz Cyberbezpieczeństwa – państwowy fundusz celowy, którego dysponentem jest minister właściwy do spraw informatyzacji. Przychodami Funduszu są:

1) dotacje z budżetu państwa;
2) wpływy z kar, o których mowa w art. 73, 75 i 75a;
3) 50% wpływów z opłat za prawo do wykorzystywania zasobów numeracji, o których mowa w art. 184 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
4) darowizny i spadki;
5) środki przekazane przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy w drodze porozumienia z ministrem właściwym do spraw informatyzacji;
6) inne przychody.

Fundusz będzie służył realizacji wyodrębnionych i konkretnie zdefiniowanych zadań, jego środki zostaną przeznaczone na:

1) świadczenie teleinformatyczne, o którym mowa w art. 62a ust. 1 oraz koszty z nim związane;
2) koszty działań związanych ze zwiększeniem poziomu bezpieczeństwa systemów informacyjnych, z wyjątkiem systemów, o których mowa w pkt 3;
3) koszty działań związanych ze zwiększeniem poziomu bezpieczeństwa systemów infrastruktury krytycznej;
4) koszty związane z utrzymaniem i rozwojem systemu, o którym mowa w art. 46;
5) koszty obsługi Funduszu i koszty z nimi związane.

Kolejne ustępy art. 72a oraz art. 72b-72j określają warunki ubiegania się o środki Funduszu Cyberbezpieczeństwa.

Zmiany w zakresie art. 73 obejmują kary dla podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. W szczególności przewidziane zostały kary dla posługiwania się certyfikatem lub deklaracją zgodności w przypadku niespełniania przez dany produkt warunków określonych w programie certyfikacji. Zapewnia to, że próby nadużycia systemu będą spotykały się ze zdecydowaną reakcją. Wysokość

kar administracyjnych została odpowiednio zróżnicowana tak by były one adekwatne do dotyczących ich czynów (art. 73 ust.1a-1c).

Wprowadzono kary dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka a także dla podmiotów, do których zostało skierowane polecenie zabezpieczające. Kara będzie wynosić do 3% całkowitego rocznego światowego obrotu danego podmiotu z poprzedniego roku obrotowego. W przypadku podmiotów publicznych kara będzie wynosić do 100 000 zł. Kary będzie nakładał minister właściwy do spraw informatyzacji. Jest to spowodowane koniecznością zapewnienia jednolitej praktyki orzeczniczej.

Podkreślić należy, że potencjalna kara za niewycofanie sprzętu lub za niedostosowanie się do polecenia zabezpieczającego nie ma na celu naruszenia konstytucyjnej niezależności organów wymienionych w Konstytucji. Nie dotyczy bowiem ich działalności unormowanej w Konstytucji i ustawach. Celem jest jedynie zapewnienia bezpieczeństwa wykonywanych zadań publicznych przez jednostki organizacyjne obsługujące np. Sejm, Senat, Prezydenta, Rzecznika Praw Obywatelskich.

Wprowadzono także karę dla podmiotów publicznych za nie wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Będzie ona wynosić 10 000 zł. Pomimo upływu ponad dwóch lat od uchwalenia ustawy o krajowym systemie cyberbezpieczeństwa wiele podmiotów publicznych nie wyznaczyło tych osób. Wprowadzenie sankcji za niewykonanie tego obowiązku zmotywuje podmioty publiczne do wyznaczenia tych osób. Dodatkowo minister właściwy do spraw informatyzacji będzie mógł nałożyć na kierownika podmiotu publicznego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę, jeżeli nie zostały zgłoszone dwie osoby do kontaktu.

W celu zapewnienia sprawnego przekazywania zgłoszeń incydentów z CSIRT sektorowego czy CSIRT INT do właściwego CSIRT poziomu krajowego wprowadza się karę za nie wykonanie tego obowiązku. Kara będzie nakładana na kierownika CSIRT sektorowego i CSIRT INT w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku.

W załączniku numer 1 w kolumnie „Rodzaj podmiotów” dotyczącej sektora „Ochrona zdrowia” usunięto:

- „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2020 r. poz. 944).”
- „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”

Podmioty lecznicze, w przedsiębiorstwie, których funkcjonują dział farmacji szpitalnej lub apteka szpitalna są faktycznie tożsame z podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. Brak jest jakiegokolwiek uzasadnienia dla istnienia wyodrębnienia takich podmiotów, ponieważ podmioty posiadające dział farmacji lub aptekę szpitalną są podmiotami leczniczymi, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.

W tym samym załączniku nr 1 w kolumnie „Rodzaj podmiotów" odnoszącej się do sektora Infrastruktury cyfrowej dodano nowy podmiot, jakim jest operator strategicznej sieci bezpieczeństwa.

Dział II – Strategiczna sieć bezpieczeństwa

Rozdział 1. Operator strategicznej sieci bezpieczeństwa

Art. 76a. Celem tworzonej strategicznej sieci bezpieczeństwa jest zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w aspekcie telekomunikacyjnym, czyli związanym z nadawaniem, odbiorem lub transmisją informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Podmiotem zobowiązanym do jej uruchomienie oraz zarządzanie jest OSSB.

Art. 76b. Sieć ta będzie zarządzana przez OSSB wskazywanego w zarządzeniu Prezesa Rady Ministrów. Wybór Prezesa Rady Ministrów jest ograniczony do kręgu podmiotów, które spełniają łącznie następujące warunki:

- będących jednoosobową spółką Skarbu Państwa,
- będących przedsiębiorcą telekomunikacyjnym,
- posiadających infrastrukturę telekomunikacyjną niezbędną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego,
- posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
- posiadających świadectwo bezpieczeństwa przemysłowego.

Art. 76c. OSSB świadczy usługi telekomunikacyjne, a także może świadczyć inne usługi (np. w zakresie bezpieczeństwa, czy usługi związane z telekomunikacyjnym procesem inwestycyjnym) w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

OSSB oprócz możliwości korzystania, tak jak wszystkie inne podmioty cywilne, z częstotliwości przeznaczonych dla użytkowania cywilnego, będzie mógł także świadczyć swoje usługi telekomunikacyjne

w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym. Zgodnie z obowiązującymi regulacjami częstotliwości rządowe lub użytkowane jako rządowe w użytkowaniu cywilno-rządowym, mogą być wykorzystywane wyłącznie przez określonych ustawą użytkowników, będących użytkownikami rządowymi.

Wykorzystanie częstotliwości rządowych przez OSSB będzie koordynowane przez Ministra Obrony Narodowej, jednakże koordynacja częstotliwości rządowych w zakresie 703-713 MHz oraz 758-768 MHz w drodze pewnego wyjątku zostaje powierzona Prezesowi Urzędu Komunikacji Elektronicznej (dalej jako „Prezes UKE"). Takie rozwiązanie jest konieczne ze względu na przewidzianą w niniejszej ustawie możliwość współużytkowania, w ramach jednej sieci telekomunikacyjnej, tych częstotliwości z częstotliwościami cywilnymi z zakresu 713-733 MHz oraz 768-788 MHz. W takim przypadku, organ regulacyjny odpowiedzialny za gospodarowanie widmem w Polsce musi mieć realne narzędzia, które umożliwią właściwe, a przede wszystkim niepowodujące szkodliwych zakłóceń, użytkowanie współużytkowanych zakresów widma radiowego. Z tego także powodu wykorzystanie częstotliwości rządowych z zakresu 703-713 MHz oraz 758-768 MHz będzie wymagać uzyskania pozwolenia radiowego, które nie jest wymagane dla użytkowników rządowych.

Art. 76d ust. 1. OSSB będzie świadczył na wniosek usługi telekomunikacyjne podmiotom najważniejszym z punktu widzenia bezpieczeństwa państwa, tj.: Kancelarii Prezydenta RP, Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezesa Rady Ministrów, Biuru Bezpieczeństwa Narodowego, urzędom obsługującym organy administracji rządowej, organy jednostek samorządu terytorialnego oraz instytucjom podległym tym organom lub przez nie nadzorowanym, wykonującym zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności państwa, ochrony granicy państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sprawiedliwości, w tym sądownictwa i prokuratury, Siłom Zbrojnym Rzeczypospolitej Polskiej oraz innym jednostkom organizacyjnym podległym lub nadzorowanym przez Ministra Obrony Narodowej.

Jednocześnie OSSB będzie świadczył usługi telekomunikacyjne także instytucjom wykonującym na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa, również na wniosek tych podmiotów.

Art. 76d ust. 2-3. Projektowane przepisy określają w szczególności zakres usług świadczonych przez OSSB na rzecz Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych oraz ministra

właściwego do spraw zagranicznych.

W przypadku MON zakres tych usług obejmuje utrzymanie, rozbudowę i modyfikację sieci teleinformatycznej na potrzeby obsługi Sił Zbrojnych RP oraz zestawianie i utrzymanie łączy dostępowych do tej sieci. W przypadku ministra właściwego do spraw wewnętrznych zakres świadczonych przez OSSB usług dotyczy utrzymania, rozbudowy i modyfikacji sieci teleinformatycznej na potrzeby obsługi numerów alarmowych, zestawiania i utrzymania łączy dostępowych do tej sieci dla enumeratywnie wskazanych podmiotów, utrzymania i rozbudowy sieci teleinformatycznej na potrzeby rejestru mieszkańców, rejestru zamieszkania cudzoziemców i rejestru stanu cywilnego, sieci GovNet oraz sieci teleinformatycznej na potrzeby rejestru PESEL (PESELNet). Ponadto, OSSB ma zapewniać połączenia centrów powiadamiania ratunkowego z publiczną siecią telekomunikacyjną. Natomiast na rzecz ministra właściwego do spraw zagranicznych, OSSB ma świadczyć usługi telekomunikacyjne w systemie łączności satelitarnej oraz usługi sieci rozległej (WAN).

Projekt zakłada nałożenie na ww. organy obowiązek korzystania z usług telekomunikacyjnych świadczonych przez OSSB w ruchomej publicznej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań w tych podmiotach na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Przyjęcie takiego rozwiązania ma zapewnić bezpieczeństwo informacji przekazywanych przy wykorzystaniu świadczonych przez OSSB usług.

Art. 76d ust. 4-6. Przepis art. 76d ust. 4 przewiduje, że Prezes Rady Ministrów będzie mógł zobowiązać OSSB do świadczenia usług właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także przedsiębiorcom o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców. Wprowadzenie takiego uprawnienia dla Prezesa Rady Ministrów zwiększy elastyczność w reagowaniu na aktualne potrzeby w zakresie zapewnienia bezpiecznej wymiany informacji pomiędzy kluczowymi podmiotami odpowiedzialnymi za realizację zadań z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Z kolei przepis art. 76d ust. 5 ustawy wprowadza możliwość zlecenia OSSB świadczenia usługi wsparcia technicznego przy realizacji zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne oraz Komendę Główną Policji.

Świadczenie usług telekomunikacyjnych, usług wsparcia technicznego oraz innych usług, o których mowa w art. 76c ust. 1 i art. 76d ust. 1 i 2 wymaga zawarcia umowy pomiędzy stronami (art. 76d ust. 6), a umowa to musi odnosić się do jakości usług, co najmniej w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego (art. 76d ust. 7).

Art. 76e. Przepis przesądza, że przy zawieraniu umów dotyczących realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych. Jest to rozwiązanie zgodne z art. 13 lit. a dyrektywy 2009/81/WE, zgodnie z którym nie stosuje się postanowień tejże dyrektywy do zamówień, w przypadku których stosowanie dyrektywy zobowiązałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje się za sprzeczne z jego podstawowymi interesami w zakresie bezpieczeństwa.

Art. 76f. Prezes UKE, na wniosek operatora strategicznej sieci bezpieczeństwa, nakłada w drodze decyzji na przedsiębiorcę telekomunikacyjnego, uprawnionego do dostarczania publicznych sieci telekomunikacyjnych lub świadczenia powiązanych usług, obowiązek kolokacji oraz udostępniania, w tym współkorzystania z infrastruktury telekomunikacyjnej, która została umieszczona na nieruchomości w związku z wykonywaniem uprawnień wynikających z przepisów prawa, wyroku sądu lub decyzji, na rzecz Operatora strategicznej sieci bezpieczeństwa i w celu realizacji zadań. Prezes UKE odmawia nałożenia obowiązku kolokacji lub obowiązku udostępnienie infrastruktury telekomunikacyjnej, jeżeli jest to technicznie niewykonalne, przy czym ciężar dowodu w tym zakresie w ramach postępowania administracyjnego spoczywa na operatorze (art. 76f ust. 1).

Kolokacja lub udostępnienie infrastruktury na rzecz OSSB w związku z decyzją Prezesa UKE, o której mowa w art. 76f ust 1, są odpłatne. Prezes UKE rozstrzyga kwestię opłat w ten sposób, że opłata za rzeczony dostęp umożliwia zwrot proporcjonalnej części poniesionych kosztów powstania udostępnianej infrastruktury oraz ponoszonych przez operatora kosztów jej utrzymania, a także uwzględnia wpływ zapewnienia takiego dostępu na plan biznesowy operatora będącego podmiotem udostępniającym, w szczególności mając na względzie realizowane przez niego inwestycje (art. 76f ust. 2).

Art. 76g. Przepis ustanawia obowiązek po stronie użytkownika wieczystego lub zarządcy nieruchomości stanowiącej własność Skarbu Państwa, a także jednostki samorządu terytorialnego, zapewnienia OSSB dostępu do nieruchomości, w tym do budynku, polegającego na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, a w szczególności nie prowadzi do istotnego zmniejszenia jej wartości nieruchomości. Obowiązek ten jest związany z realizacją zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji przez OSSB (art. 76g ust. 1).

Warunki zapewnienia dostępu, o którym mowa w art. 76g ust. 1, określa umowa pomiędzy OSSB a podmiotem zapewniającym dostęp do nieruchomości, która powinna zostać w formie pisemnej, w terminie 30 dni od dnia wystąpienia przez OSSB z wnioskiem o jej zawarcie (art. 76g ust. 2-3).

Obowiązek dostępu do nieruchomości, o którym mowa w art. 76g ust. 1, jest nieodpłatny, z zastrzeżeniem, że jeżeli podmiotem zobowiązanym do zapewnienia dostępu jest jednostka samorządu terytorialnego, po pierwsze, OSSB pokryje w całości koszty przywrócenia nieruchomości do stanu poprzedniego, a także proporcjonalną część: kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością oraz kosztów które wystąpiły po stronie jednostki samorządu terytorialnego i są konieczne a zaistniały bezpośrednio na skuter zapewnienia dostępu (art. 76g ust. 4).

Art. 76h. Do dostępu związanego z kolokacją i udostępnieniem infrastruktury telekomunikacyjnej na podstawie decyzji Prezesa UKE, o której mowa w ust. 76f ust. 1, jak również do dostępu do nieruchomości użytkownika wieczystego lub zarządcy nieruchomości stanowiącej własność Skarbu Państwa lub jednostki samorządu terytorialnego, o którym mowa w art. 76h ust. 1 stosuje się odpowiednio przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne odnoszące się do: negocjacji związanych z zapewnieniem dostępu; wniosku do Prezesa UKE o rozstrzygnięcie sporu; decyzji Prezesa UKE rozstrzygającej spór; zasad zmiany umowy o dostępie; kwestii związanych z połączeniem sieci, a także obowiązku przekazania umowy o dostępie Prezesowi UKE w terminie 14 dni od jej podpisania.

Art. 76i. Przepis zastrzega dla OSSB pierwszeństwo kupna sieci telekomunikacyjnych na wypadek, gdyby państwowych osoba prawna lub jednostka samorządu terytorialnego sprzedała je osobie trzeciej. Do pierwokupu stosuje się przepisy rozdziału IV księgi III ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny.

Art. 76j. Przepis określa relację co do stosowania przepisów dotyczących OSSB, przesądzając, że zasadą jest stosowanie przepisów ustawy Prawo telekomunikacyjne, w zakresie w jakim postanowienia ustawy o strategicznej sieci bezpieczeństwa nie stanowią wobec niej regulacji o charakterze *lex specialis*.

Art. 76k. Przepis zawiera normę kompetencją Prezesa Rady Ministrów, który może, w przypadku utraty przez OSSB co najmniej jednego z przymiotów niezbędnych do jego wyznaczenia, w drodze zarządzenia odwołać OSSB, oraz wyznaczyć nowego Operatora strategicznej sieci bezpieczeństwa (art. 76k ust. 1), także z określeniem terminu skuteczności obu czynności (art. 76k ust. 2). Kompetencja ta ma charakter fakultatywny, aby zapewnić odpowiednią elastyczność, np. w sytuacji gdyby żaden podmiot w danym momencie nie spełniałby wymogów ustawowych lub w sytuacji gdy spółka wyznaczona jako OSSB przestałaby być w efekcie przekształceń spółką jednoosobową, a w ocenie Prezesa Rady Ministrów istniałaby nieproporcjonalne ryzyko związane ze zmianą OSSB w kontekście zapewnienia ciągłości świadczenia określonych usług w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Art. 76l. Nowy Operator strategicznej sieci bezpieczeństwa, wyznaczony przez Prezesa Rady Ministrów, jest następcą prawnym dotychczasowego Operatora strategicznej sieci bezpieczeństwa w zakresie

realizacji jego zadań. Poprzez przepis szczególny przesądzony jest skutek niektórych stosunków prawnych – umowy o świadczenie usług, do których odnosi się, poprzez odesłanie, art. 76b ust. 4, 10 i 11 ustawy, wygasają z mocy prawa w terminie 3 miesięcy od dnia wydania zarządzenia.

Rozdział 3. Spółka Polskie 5G

Art. 76m. OSSB jest zobowiązany do utworzenia spółki kapitałowej, która będzie pełnić funkcje operatora ogólnopolskiej hurtowej sieci, na częstotliwościach z zakresu 703 – 733 MHz oraz 758 – 788 MHz o nazwie Polskie 5G („Spółka Polskie 5G"). Kapitał zakładowy w pierwotnej wysokości będzie wynosił 1 000 000 zł (jeden miliony złotych). Ponadto, w art. 76m ust. 3 wskazany jest szczególny katalog postanowień Aktu założycielskiego Spółki Polskie 5G.

Art. 76n ust. 1. Udziały lub akcje w Spółce Polskie 5G obejmuje za wkłady pieniężne:

- OSSB (26% lub 52%, jeżeli Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A. nie obejmą udziałów lub akcji),
- Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A. w stosunku 26% – jeżeli zdecyduje/zdecydują się na objęcie udziałów lub akcji,
- przedsiębiorca telekomunikacyjny, któremu zostaną przyznane częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz w stosunku 48%, lub jeżeli częstotliwości te zostaną przyznane konsorcjum przedsiębiorców telekomunikacyjnych – każdemu z nich w częściach równych po zakończeniu przetargu.

Art. 76n ust. 2. OSSB oraz – o ile objął lub objęły udziały lub akcje – Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A. dysponują na zgromadzeniu wspólników albo na walnym zgromadzeniu akcjonariuszy liczbą głosów co najmniej równą ilości posiadanych udziałów w Spółce Polskie 5G. Przepis ten wprost uzależnia liczbę głosów przysługujących ww. wspólnikom od wartości ich udziału.

Art. 76n ust. 3-4. Przepisy te odnoszą się do dwóch organów Spółki 5G – Rady nadzorczej Spółki Polskie 5G oraz Zarządu Spółki Polskie 5G. Kadencje obu organów trwają 3 lata.

Rada nadzorcza składa się z pięciu członków. Trzech członków rady nadzorczej jest powoływanych przez OSSB i Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A., natomiast dwóch członków przez przedsiębiorcę telekomunikacyjnego lub konsorcjum przedsiębiorców telekomunikacyjnych, którym zostały przyznane częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz.

Zarząd składa się z 4 członków. Prezesa zarządu oraz jednego członka powołuje OSSB i Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A., natomiast kolejnych dwóch członków zarządu powoływanych jest przez przedsiębiorcę telekomunikacyjnego lub konsorcjum przedsiębiorców telekomunikacyjnych, którym zostały przyznane częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz.

Art. 76n ust. 5. Przez „ogólnopolską hurtową sieć 5G" należy rozumieć udostępnioną przez akcjonariuszy Spółki Polskie 5G infrastrukturę telekomunikacyjną oraz własną nowo wybudowaną, nabytą lub udostępnianą przez podmioty trzecie infrastrukturę telekomunikacyjną korzystającą, w tym współkorzystającą, z częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz.

Art. 76n ust. 6**.** Spółka Polskie 5G obowiązana do:

- oferowania odpłatnych usług telekomunikacyjnych na warunkach hurtowych,
- udostępniania odpłatnie usług telekomunikacyjnych na rzecz OSSB w celu świadczenia przez niego usług telekomunikacyjnych i innych usług służących zapewnieniu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, oraz
- zapewnienia pokrycia całego terytorium kraju zasięgiem sieci hurtowej oraz zapewnienia szczególnego poziomu bezpieczeństwa w interesie publicznym w zakresie sieci oraz usług.

Pierwszy z obowiązków wiąże się z przygotowaniem oferty dotyczącej usług telekomunikacyjnych świadczonych na rynkach hurtowych. Drugi z obowiązku oznacza obowiązek odpłatnego udostępnienia usług telekomunikacyjnych OSSB, natomiast trzeci określa obowiązek, który jest głównym celem Spółki Polskie 5G – zapewnienie pokrycia całego terytorium kraju zasięgiem sieci hurtowej oraz zapewnienie ochrony interesu publicznego poprzez zapewnienie szczególnego poziomu bezpieczeństwa sieci oraz usług.

Rozdział 4. Przyznanie częstotliwości z zakresu 703 – 733 MHz oraz 758 – 788 MHz

11 marca 2013 r., na podstawie art. 4 ust. 2 Decyzji o spektrum radiowym[22] Komisja Europejska udzieliła Europejskiej Konferencji Administracji Pocztowych i Telekomunikacyjnych (*European Conference of Postal and Telecommunications Administrations* - CEPT) zlecenia na opracowanie zharmonizowanych warunków technicznych dla pasma 700 MHz na potrzeby bezprzewodowych usług szerokopasmowej łączności elektronicznej w Unii oraz na potrzeby innych zastosowań, wspierających priorytety unijnej polityki

[22] Decyzja Nr 676/2002/WE Parlamentu Europejskiego i Rady Z dnia 7 marca 2002 r. w sprawie ram regulacyjnych dotyczących polityki spektrum radiowego we Wspólnocie Europejskiej.

widma radiowego. W ramach tego zlecenia, CEPT przedstawił sprawozdania nr 53[23] (w 2014 r.) i 60[24] (w 2016 r.), które stanowią podstawę technicznej harmonizacji pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w Europie. Komisja Europejska w komunikacie pt. „Strategia jednolitego rynku cyfrowego dla Europy"[25] przedstawiła wizję powszechnego dostępu do łączności wysokiej jakości dla przedsiębiorstw i obywateli. Strategia ta zapowiadała konkretne wnioski ustawodawcze Komisji, dotyczące m.in. skoordynowanego zwalniania zakresu 694-790 MHz. Bazując na sprawozdaniach CEPT, oraz biorąc pod uwagę prace legislacyjne nad decyzją zmieniającą przeznaczenia pasma 700 MHz w Unii, 28 kwietnia 2016 r. Komisja Europejska wydała Decyzję harmonizacyjną odnośnie zakresu częstotliwości 694-790 MHz[26]. Tym samym zapewniono ujednolicone warunki techniczne, umożliwiające użytkowanie pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej i innych zastosowań zgodnie z priorytetami polityki widma radiowego na szczeblu unijnym i krajowym. 17 maja 2017 r. Parlament Europejski i Rada wydały Decyzję w sprawie wykorzystania zakresu częstotliwości 470-790 MHz w Unii Europejskiej[27] (dalej: Decyzja o zmianie przeznaczenia), na mocy której Państwa Członkowskie UE zostały zobowiązane do udostępnienia pasma 700 MHz na potrzeby usług szerokopasmowych do 30 czerwca 2020 r. lub w uzasadnionych przypadkach najpóźniej do 30 czerwca 2022 r.

Zgodnie z Krajowym Planem Działań zmiany przeznaczenia pasma 700 MHz w Polsce, którego przyjęcie wymagane było Decyzją o zmianie przeznaczenia, 28 grudnia 2018 r. na podstawie z art. 1. ust. 1. Decyzji Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii, Polska wystąpiła do Komisji Europejskiej z informacją o konieczności odsunięcia terminu udostępnienia pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej do 30 czerwca 2022 r. Wskazanym przez Polskę uzasadnionym powodem odroczenia dopuszczenia do korzystania z częstotliwości z pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewnienia usług bezprzewodowej

[23] *Report A from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 28 November 2014 by the ECC*.

[24] *Report B from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 01 March 2016 by the ECC*.

[25] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia jednolitego rynku cyfrowego dla Europy z dnia 6 maja 2015 r. (COM(2015) 192 final)

[26] Decyzja Wykonawcza Komisji (UE) 2016/687 z dnia 28 kwietnia 2016 r. w sprawie harmonizacji zakresu częstotliwości 694-790 MHz na potrzeby systemów naziemnych zapewniających bezprzewodowe szerokopasmowe usługi łączności elektronicznej oraz na potrzeby elastycznego użytkowania na poziomie krajowym w Unii (notyfikowana jako dokument nr C(2016) 2268).

[27] Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii.

szerokopasmowej łączności elektronicznej po dniu 30 czerwca 2020 r. (art. 1 ust. 1) były nierozwiązane problemy dotyczące koordynacji transgranicznej skutkujące szkodliwymi zakłóceniami. Brak informacji ze strony Federacji Rosyjskiej, Republiki Białorusi oraz Ukrainy o wyłączeniu do 30 czerwca 2020 r. naziemnej telewizji, działającej w paśmie 700 MHz na terenie tych krajów, uniemożliwiłby de facto w sposób niezakłócony uruchomienie pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej na terenie Polski w wymaganym terminie tj. do 30 czerwca 2020 r.

Ramy krajowych działań wyznaczane są przez decyzje Unii Europejskiej oraz regulacje Międzynarodowego Związku Telekomunikacyjnego (International Telecommunications Union - ITU) stąd Krajowy Plan Działań zmiany przeznaczenia pasma 700 MHz w Polsce, stanowiący podstawę do dalszych decyzji ustawodawczych nie przesądza o kierunkach i sposobie wykorzystania tego zasobu. Z punktu widzenia realizacji Decyzji o zmianie przeznaczenia kluczowa jest więc zgodność podejmowanych działań na szczeblu krajowym z uwarunkowaniami Decyzji harmonizacyjnej. Zgodnie z tą Decyzją użytkowanie pasma 700 MHz do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej będzie opierało się o zharmonizowaną w skali europejskiej „podstawową aranżację" kanałów 2x30 MHz w zakresach 703- 733 MHz (FDD - Frequency Division Duplex łącze „w górę") oraz 758-788 MHz (FDD - Frequency Division Duplex łącze „w dół"). W myśl Decyzji harmonizacyjnej ww. zakresy pasma 700 MHz powinny być użytkowane do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w oparciu o zharmonizowaną aranżację kanałów (jako tzw. „aranżacja podstawowa") oraz powiązane wspólne najmniej restrykcyjne warunki techniczne, jeżeli państwa członkowskie wyznaczą je do użytkowania w zastosowaniach innych niż przez sieci radiodyfuzyjne o dużej mocy.

Niemniej jednak państwa członkowskie UE mają swobodę decyzji w zakresie użytkowania części pasma częstotliwości 700 MHz w celu zaspokojenia szczególnych potrzeb krajowych. Oprócz naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej powyższe obejmuje również użytkowanie zgodnie z priorytetami sektorowymi unijnej polityki widma radiowego, w szczególności na potrzeby Programme Making and Special Events (PMSE, bezprzewodowe urządzenia do transmisji sygnałów akustycznych), Public Protection and Disater Relief (PPDR, łączność radiowa na potrzeby ochrony publicznej i pomocy w przypadku klęsk żywiołowych) i Internet of Things (IoT, Internet Rzeczy)) i w celu zapewnienia efektywnego użytkowania widma.

Art. 76o ust. 1-3. Przepis ustawy zobowiązuje Prezesa UKE do przydzielenia, w drodze decyzji administracyjnej, OSSB określonego zakresu częstotliwości, przeznaczonego do użytkowania rządowego. Do decyzji Prezesa UKE odpowiednio należy stosować przepisy ustawy Prawo telekomunikacyjne dotyczące

rezerwacji częstotliwości, regulujące między innymi okres, na który jest ona wydawana oraz jej treść. Jednocześnie w decyzji tej Prezes UKE obligatoryjnie określi zobowiązania pokryciowe czyli nałożone na OSSB wymogi w zakresie pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o te częstotliwości.

Decyzja harmonizacyjna w tym kontekście wyraźnie wskazuje, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa PPDR, należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.

Art. 76p ust. 1. Przepis ustawy wprowadza możliwość zadecydowania przez niezależnego regulatora rynku telekomunikacyjnego o szczególnym przeznaczeniu częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz. Prezes UKE może przyznać ten zakres widma przedsiębiorcy telekomunikacyjnemu lub konsorcjum przedsiębiorców telekomunikacyjnych w celu świadczenia wyłącznie usług hurtowych. Propozycja ma na celu zapewnienie Prezesowi UKE odpowiednich mechanizmów, które mogą w przyszłości doprowadzić do zintensyfikowania działań mających na celu realizację przez Rzeczpospolitą Polską celów w zakresie zapewnienia dostępu do usług szerokopasmowych każdemu obywatelowi Unii Europejskiej. Ambitne zamierzenia wynikające z unijnych dokumentów programowych, takich jak Europejska Agenda Cyfrowa, oraz Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego wskazują na konieczność realizacji celów w zakresie dostępu do sieci o bardzo dużej przepustowości, w tym dotyczące pokrycia tymi sieciami m.in. głównych szlaków komunikacyjnych do roku 2025. Projektowane zmiany przewidują możliwość przeznaczenia przez Prezesa UKE zasobów częstotliwości, które będą mogły być przydzielone dla przedsiębiorcy telekomunikacyjnego (lub konsorcjum), który świadczyć będzie usługi na warunkach hurtowych. Oznacza to, że częstotliwości te zostaną w praktyce przeznaczone na potrzeby budowy jednej sieci, co znacząco obniży koszty działania sieci 5G zarówno dla podmiotów państwowych, jak i operatorów komercyjnych, co w konsekwencji wprost przełoży się także niższe koszty dla obywateli.

Art. 76p ust. 2 i 3. W przypadku podjęcia przez Prezesa UKE decyzji o przyznaniu częstotliwości cywilnych z zakresu 713-733 MHz oraz 768-788 MHz na potrzeby świadczenia usług hurtowych, a zatem w praktyce budowy do ich wykorzystania jednej sieci telekomunikacyjnej, ich rozdysponowanie odbędzie się w drodze przetargu określonego w przepisach ustawy Prawo telekomunikacyjne. Należy zauważyć, że zgodnie z regulacjami prawa telekomunikacyjnego rozdysponowanie częstotliwości na potrzeby świadczenia usług

innych niż rozpowszechnianie w sposób cyfrowy lub rozprowadzanie programów radiofonicznych lub telewizyjnych, w przypadku braku dostatecznych zasobów częstotliwości, może zostać dokonane w drodze jednego z dwóch rodzajów postępowań selekcyjnych – aukcji lub przetargu. Istotną różnicą pomiędzy tymi postępowaniami jest to, że jedynym kryterium oceny ofert w aukcji jest cena. W przetargu, oprócz ceny, uwzględnia się także zachowanie warunków konkurencji i inne kryteria, które mogą zostać określone przez organ regulacyjny w dokumentacji. Przesądzenie w niniejszej ustawie, że w tym przypadku zastosowanie znajdzie wyłącznie przetarg wynika zatem wprost z celu przedmiotowej regulacji, którym jest zapewnienie jak najszerszego pokrycia kraju siecią 5G i jak najefektywniejsze wykorzystanie widma radiowego, które jest zasobem ograniczonym.

Jednocześnie, ze względu na fakt, że mówimy o jednej sieci oraz o zobowiązaniu do świadczenia usług hurtowych, szczególne znaczenie mają kwestie bezpieczeństwa tej sieci i jej niezawodności. Dlatego też ustawa wprowadza dodatkowe, w stosunku do regulacji ustawy Prawo telekomunikacyjne, obligatoryjne kryterium przetargowe, którym będzie zapewnienie przy świadczeniu usług odpowiedniego poziomu bezpieczeństwa oraz niezawodności sieci i usług. Także to kryterium, obok kryteriów wynikających z ustawy Prawo telekomunikacyjne, będzie mogło zostać wskazane przez Prezesa UKE w dokumentacji przetargowej jako najistotniejsze kryterium oceny ofert w przetargu.

Należy podkreślić, że rozdysponowanie wskazanych częstotliwości w drodze przetargu, określonego w ogólnych ramach regulujących gospodarkę częstotliwościami w Polsce, zapewni pełną zgodność z unijnymi ramami regulacyjnymi, które wymagają aby przeznaczenie widma radiowego na użytek sieci i usług łączności elektronicznej odbywały się według obiektywnych, przejrzystych, sprzyjających konkurencji, niedyskryminacyjnych i proporcjonalnych kryteriów, w oparciu o otwarte, obiektywne, przejrzyste, niedyskryminacyjne i proporcjonalne procedury.

Art. 76r ust. 1-3. Przepis daje Prezesowi UKE uprawnienie do określenia bardziej szczegółowych zasad użytkowania częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz oraz zakresu 703-713 MHz oraz 758-768 MHz. Regulacje dotyczące możliwości nałożenia, zarówno w decyzji rezerwacyjnej w odniesieniu do częstotliwości cywilnych, jak i decyzji przydzielających częstotliwości rządowe dla OSSB, obowiązku współużytkowania częstotliwości, a także ich wykorzystania w ramach jednej sieci telekomunikacyjnej zmierzają przede wszystkim do zapewnienia jak największej efektywności wykorzystania przedmiotowych zasobów, co przełoży się bezpośrednio na zwiększenie zasięgu sieci i usług.

Art. 76s ust. 1-3. Przepis reguluje kwestię zmiany podmiotu, któremu przydzielono częstotliwości rządowe z zakresu 703-713 MHz oraz 758-768 MHz w przypadku odwołania lub zmiany podmiotu będącego OSSB. W takim przypadku nowy OSSB wstępuje w prawa i obowiązki związane z przydziałem tego zakresu częstotliwości określone w ustawie oraz decyzji Prezesa UKE. Takie rozwiązanie zapewni dalsze

niezakłócone funkcjonowanie sieci i prawidłową realizację usług strategicznych.

Rozdział 5. Fundusz celowy na rzecz strategicznej sieci bezpieczeństwa

Art. 76t. Tworzy się państwowy fundusz celowy, którego dysponentem jest minister właściwy do spraw aktywów państwowych – Fundusz celowy na rzecz strategicznej sieci bezpieczeństwa (dalej „Fundusz"). Ustawa określa przychody Funduszu oraz jego wydatki. Przewidziana jest również delegacja ustawowa dla Rady Ministrów, do określenia w drodze rozporządzenia trybu i zasad pobierania, ewidencjonowania, przekazywania i rozliczania przychodów Funduszu: opłat jednorazowych za rezerwacje częstotliwości w zakresie 713-733 MHz, 68-788 MHz i 3,4 – 3,8 GHz, jak również opłat rocznych za prawo do dysponowania częstotliwością.

Rozdział 6. Przepisy przejściowe i końcowe

Art. 76u ust. 1-2. Przepis ustala harmonogram kluczowych z perspektywy wdrożenia postanowień ustawy okoliczności:

- wyznaczenia przez Prezesa Rady Ministrów OSSB (w terminie do 30 dni od wejścia w życie ustawy),
- powołania przez OSSB Spółki Polskie 5G (w terminie do 60 dni od wyznaczenia OSSB).

Art. 76u ust. 3**.** Zgodnie z regulacją wynikającą z art. 76u ust. 3, od momentu ogłoszenia przetargu, której przedmiotem będą rezerwacje częstotliwości w zakresie 713-733 MHz oraz 768-788, do czasu objęcia akcji lub udziałów w Spółce Polskie 5G przez przedsiębiorcę telekomunikacyjnego lub konsorcjum przedsiębiorców telekomunikacyjnych nie jest możliwa zmiana aktu założycielskiego spółki. Rozwiązanie to ma zapobiec sytuacji, w której po ogłoszeniu przetargu możliwa byłaby jakakolwiek zmiana aktu założycielskiego, bez udziału wspólnika (wspólników), o których mowa w art. 76u ust. 1 pkt 3.

Zmiany w obowiązujących przepisach

Przedmiotowa ustawa, w art. 2, wprowadza również zmiany w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27 i 2320), które wynikają z faktu, iż CSIRT GOV jest umiejscowiony w strukturze organizacyjnej Agencji Bezpieczeństwa Wewnętrznego, a zadania realizowane przez CSIRT GOV wykonują funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, wobec których w kwestii uposażenia zastosowanie mają przepisy ustawy pragmatycznej.

Zmiany w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu polegają na wprowadzeniu przepisów umożliwiających przyznanie dodatkowego świadczenia pieniężnego ekspertom zatrudnionym albo pełniącym służbę w Agencji Bezpieczeństwa Wewnętrznego realizującej zadania CSIRT GOV. Przedmiotowa regulacja umożliwi przyznawanie funkcjonariuszom

Agencji Bezpieczeństwa Wewnętrznego świadczenia teleinformatycznego. Regulowany jest również proces przyznawania tego świadczenia oraz szczegóły związane z jego wypłacaniem. Wskazują za jaki okres nie przysługuje to świadczenia a także kiedy jest wypłacane. Przyjęcie tych przepisów umożliwi rozpoczęcie wypłacania nowego świadczenia w pierwszym możliwym terminie.

Zmieniane przepisy w sposób kompleksowy regulują kwestie przyznawania świadczenia teleinformatycznego, jego wypłacania oraz cofania. Kształt projektowanych regulacji bezpośrednio wskazuje, iż przedmiotowe świadczenie nie będzie składnikiem uposażenia funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego, które jest uregulowane w art. 115 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Zmiany w:

- ustawie z dnia 10 grudnia 1993 r. o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin (Dz. U. z 2020 r. poz. 586) oraz

- ustawie z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin (Dz.U. 2020 r. poz. 723 i 2320), wskazują, że świadczenia teleinformatycznego nie wlicza się do podstawy wymiaru emerytury lub renty inwalidzkiej.

Art. 2-8 regulują zagadnienie świadczenia teleinformatycznego dla funkcjonariuszy:

- Centralnego Biura Antykorupcyjnego,
- Służby Kontrwywiadu Wojskowego.
- Służby Wywiadu Wojskowego,
- wojska,
- Straży Granicznej.

Regulacje te są analogiczne do tych wprowadzanych do ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Art. 9 dodaje nowy przepis do ustawy o z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych. Przepis ten zmienia źródła finansowania Funduszu Szerokopasmowego wskazując, że zamiast 100% wpływów z opłat za prawo do wykorzystywania zasobów numeracji, do Funduszu Szerokopasmowego będzie trafiać 50% tych wpływów. Zmiana ta wynika z powołania Funduszu

Cyberbezpieczeństwa, do którego zostanie przeniesiona połowa wpływów z tych opłat. Rosnące znaczenie cyberbezpieczeństwa i jego wpływ na funkcjonowanie państwa sprawia, że konieczne jest zwiększenie nakładów w celu realizacji zadań z tego zakresu, uzasadniających częściowego przesunięcia źródeł wpływu pomiędzy funduszami, których dysponentem jest minister właściwy ds. informatyzacji.

Zgodnie z art. 10 w ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzaniu mieniem państwowym w art. 13 ust. 1 dodaje się pkt 31 w brzmieniu: „podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa". Ta zmiana jest konsekwencją wprowadzenia do polskiego porządku prawnego operatora strategicznej sieci bezpieczeństwa, który nie powinien zbywać akcji lub prawa z akcji należące do Skarbu Państwa.

Art. 11 reguluje kwestie związane z podłączeniem operatorów usług kluczowych do systemu S46. W ustawie wprowadzony został obowiązek korzystania z tego systemu. Podłączenie do tego systemu wiąże się jednak z określonymi kosztami oraz czasem. W związku z tym dla obecnych operatorów usług kluczowych datą graniczną na rozpoczęcie korzystania z tego systemu będzie 1 stycznia 2023. Z kolei podmioty wyznaczone na operatorów od 1 lipca 2022 będą miały 6 miesięcy na rozpoczęcie korzystania z tego systemu. Przepis ten gwarantuje ochronę interesów podmiotów prywatnych, dając im wystarczający czas na podłączenie do systemu.

Celem art. 12 jest uregulowanie kwestii rozstrzygnięcia postępowań wszczętych o udzielenie zamówienia publicznego. Przepis przejściowy wprost rozstrzyga o stosowaniu do tych postępowań ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym niniejszą ustawą, jeżeli zostały one wszczęte przed dniem wejścia w życie niniejszej ustawy, a jednocześnie nie zakończyły się wyborem wykonawcy albo unieważnieniem postępowania przed dniem opublikowania informacji o wydaniu decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, przy czym relewantną datą jest data publikacji w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

Art. 13 reguluje kwestie związane z utworzeniem Funduszu Cyberbezpieczeństwa. Ze względu na to, że Fundusz powinien jak najszybciej rozpocząć swe działania, tak aby zapewnić wzrost poziomu cyberbezpieczeństwa w całym systemie konieczne jest wyposażenie go w odpowiednie środki na rozpoczęcie działalności. Środki te będą przekazane z Funduszu Szerokopasmowego, budżetu państwa oraz ewentualnie środków Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego. Należy podkreślić, że w zakresie w jakim ustawa nakłada możliwość przekazania środków przez instytut badawczy, jest przepisem o charakterze *lex specialis*, a środki, które byłyby przekazane są środkami w kwocie, które nie wpłynęłyby negatywnie na funkcjonowanie NASK – PIB, za to przyczyniła się do osiągnięcia ważnych celów Funduszu Cyberbezpieczeństwa.

Art. 14 stanowi przepis przejściowy regulujący zgłaszanie incydentów przez podmioty krajowego systemu cyberbezpieczeństwa do czasu utworzenia CSIRT-ów sektorowych oraz CSIRT-u INT. Zgodnie z nowymi przepisami operatorzy usług kluczowych i niektóre podmioty publiczne będą zgłaszać incydenty do tych podmiotów, a nie do CSIRT-ów poziomu krajowego. Konieczne było uregulowanie kwestii zgłaszania incydentów do czasu powstania CSIRT-ów sektorowych i CSIRT INT. Będą one dalej zgłaszane do CSIRT GOV, CSIRT MON i CSIRT NASK do czasu osiągnięcia gotowości operacyjnej przez nowe podmioty. Gwarantuje to zachowanie ciągłości działań w ramach krajowego systemu cyberbezpieczeństwa.

Zgodnie z art. 15 narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK-PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała. Narzędzia te przekazywane są przez NASK-PIB najważniejszym osobom w państwie w ramach szkoleń z cyberbezpieczeństwa. Narzędzia te są ściśle spersonalizowane i ich ponowne wykorzystanie przez inne osoby nie będzie możliwe. W związku z tym należy uregulować kwestie własności tych przedmiotów. Jako, że nie da się ich ponownie wykorzystać powinny przejść na własność osób, które je otrzymały.

Art. 16 ust. 1 zawiera przepisy dostosowujące, według których:

1) dotychczas powołane w ramach operatora usługi kluczowej wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo stają się SOC powołanymi w ramach operatora usługi kluczowej;

2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;

3) dotychczas powołany sektorowy zespół cyberbezpieczeństwa (CSIRT KNF) staje się CSIRT sektorowym.

Podmioty publiczne wyznaczają osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

Operatorzy usług kluczowych:

- rozpoczną realizowanie obowiązków, o których mowa w art. 11 ust. 3 pkt 1-3 od momentu ogłoszenia komunikatu o osiągnięciu zdolności operacyjnej przez CSIRT sektorowy;

- po raz pierwszy zgłoszą 2 osoby kontaktowe do właściwego CSIRT poziomu krajowego w terminie 14 dni od dnia wejścia w życie ustawy.

Przewidziano termin 18 miesięcy od dnia wejścia w życie ustawy na powołanie przez organy właściwe do spraw cyberbezpieczeństwa CSIRT sektorowych.

Powyższy przepis przejściowy jest niezbędny na przeprowadzenie organizacji tych zespołów, w tym na zapewnienie środków w nowej ustawie budżetowej, jak również przygotowanie niezbędnych składników materialnych i pozyskanie wysoko kwalifikowanej kadry ekspertów.

Art. 18-22 reguluje kwestie związane z wyznaczeniem Operatora strategicznej sieci bezpieczeństwa. Regulacje te wskazują jak będzie on wyznaczany, a także kwestie związane z przyznawaniem częstotliwości oraz powołaniem Spółki Polskie 5G. Wszystkie wskazane regulacje mają umożliwić jak najszybsze rozpoczęcie działalności przez Operatora.

Utrzymane zostanie rozporządzenie z art. 10 ust. 5 do czasu wydania nowego rozporządzenia.

Termin vacatio legis wynosi 30 dni od dnia ogłoszenia.

Pozostałe informacje

Wpływ projektu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 4 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa[28] projekt został zamieszczony w wykazie prac legislacyjnych.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa oraz § 138 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów[29] projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Projektowana regulacja będzie poddana notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych[30].

[28] Dz. U. z 2017 r. poz. 248.
[29] Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów M.P. z 2016 r. poz. 1006 i 1204, z 2018 r. poz. 114 i 278, z 2019 r. poz. 137 i 1192, z 2020 r. poz. 1113.
[30] Dz. U. poz. 2039, z późn. zm.