

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

**Komisja
Cyfryzacji,
Innowacyjności
i Nowoczesnych
Technologii**

■ **PODKOMISJI STAŁEJ DO SPRAW
CYBERBEZPIECZEŃSTWA
(NR 2)
z dnia 30 lipca 2026 r.**

Pełny zapis przebiegu posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii – podkomisji stałej do spraw cyberbezpieczeństwa (nr 2)

30 lipca 2026 r.

Podkomisja stała do spraw cyberbezpieczeństwa, obradująca pod przewodnictwem posła **Pawła Bliźniuka (KO)**, przewodniczącego podkomisji, rozpatrzyła:

- **informację ministra cyfryzacji na temat stanu wdrażania ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, w szczególności w zakresie wydawania przepisów wykonawczych, przygotowania podmiotów objętych ustawą do realizacji nowych obowiązków oraz harmonogramu dalszych działań wdrożeniowych.**

W posiedzeniu udział wzięli: **Paweł Olszewski** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikiem, **Przemysław Kuna** prezes Urzędu Komunikacji Elektronicznej wraz ze współpracownikami, **Sebastian Wilk** zastępca dyrektora Centralnego Ośrodka Informatyki, **Grzegorz Gontarz** główny specjalista w Biurze Rzecznika Małych i Średnich Przedsiębiorców, **Jacek Łęgiewicz** członek Rady Nadzorczej Związku Cyfrowy Lewiatan Konfederacji Lewiatan, **Krzysztof Trzaskom** ekspert Izby Gospodarczej Elektroniki i Telekomunikacji oraz **Joanna Karczewska** członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKApw.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Jakub Konecki** i **Magdalena Krzymowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dzień dobry, witam serdecznie.

Otwieram posiedzenie podkomisji stałej do spraw cyberbezpieczeństwa. Stwierdzam kworum.

Witam panią i pana posła. Myślę, że w trakcie posiedzenia jeszcze dotrze kolejna część członków podkomisji. Witam pana ministra Pawła Olszewskiego, sekretarza stanu w Ministerstwie Cyfryzacji, oraz pana Marcina Wysockiego, zastępcę dyrektora Departamentu Cyberbezpieczeństwa w resorcie cyfryzacji, witam serdecznie; witam prezesa Urzędu Komunikacji Elektronicznej, pana Przemysława Kunę, wraz ze współpracownikami; witam pana Sebastiana Wilka, zastępcę dyrektora Centralnego Ośrodka Informatyki, dzień dobry; witam reprezentację Biura Rzecznika Małych i Średnich Przedsiębiorców; witam przedstawicieli strony społecznej: Konfederacji Lewiatan, Polskiego Towarzystwa Informatycznego, Związku Cyfrowa Polska, Polskiej Izby Informatyki i Telekomunikacji, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, Forum STEM, Polskiego Towarzystwa Telemedycyny, Stowarzyszenia @ELKApw oraz Centrum Europejskiego Uniwersytetu Warszawskiego. Witam wszystkich państwa bardzo serdecznie.

Porządek dzisiejszego posiedzenia przewiduje przedstawienie informacji ministra cyfryzacji na temat stanu wdrażania ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, w szczególności w zakresie wydawania przepisów wykonawczych, przygotowania podmiotów objętych ustawą do realizacji nowych obowiązków oraz harmonogramu dalszych działań wdrożeniowych. Czy są uwagi do porządku obrad? Nie widzę.

Przystępujemy do jego realizacji. Proszę o zabranie głosu pana ministra Pawła Olszewskiego.

Sekretarz stanu w Ministerstwie Cyfryzacji Paweł Olszewski:

Dzień dobry, witam państwa bardzo serdecznie; witam, panie przewodniczący.

Szanowni państwo, materia jest niezwykle złożona i niezwykle obszerna, więc jeśli pozwolą państwo, to na tyle, na ile można, w sposób w miarę zwięzły postaram się państwu przedstawić te informacje. Całość informacji uszczegółowionej przekażę państwu na piśmie,

bowiem naprawdę dużo się dzieje, dużo tych procesów jest, a wiem, że mamy też ograniczenia czasowe, jeśli chodzi o salę.

Więc tak – ustawa o krajowym systemie cyberbezpieczeństwa, jak państwo doskonale wiedzą, bo uczestniczyli w tym procesie i wspierali ten proces, która ma zasadnicze znaczenie, jeśli chodzi o KSC i bezpieczeństwo Polek i Polaków, weszła w życie 3 kwietnia 2026 r. Obecnie trwają różne procesy związane z praktycznym wdrożeniem tej ustawy, począwszy od aktów wykonawczych, co jest zawarte w temacie podkomisji, jak i organizacyjnych, jak i wspierających, szkoleniowych, informacyjnych etc.

Jeśli chodzi o zasadnicze kwestie, czyli kwestie terminów, obecnie trwa okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych. Termin na wpis do wykazu podmiotów kluczowych i ważnych wynosi 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. W przypadku podmiotów, które spełniają przesłanki podmiotu kluczowego lub podmiotu ważnego, w dniu wejścia w życie ustawy termin ten upływa 3 października 2026 r. Na podłączenie do systemu S46, czyli tego jednego okienka, gdzie zgłaszamy między innymi incydenty, mają czas 12 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub ważny. Wdrożenie obowiązków w zakresie zarządzania bezpieczeństwem informacji to jest 12 miesięcy. Termin ten upływa 3 kwietnia 2027 r., czyli dokładnie rok po wejściu w życie ustawy. Obecnie trwa okres samoidentyfikacji podmiotów kluczowych i ważnych. Są one obowiązane wpisać się do wykazu podmiotów kluczowych i ważnych, który jest prowadzony przez ministra cyfryzacji za pośrednictwem specjalnego systemu rejestracyjnego, o którym już wcześniej powiedziałem, czyli systemu S46. Natomiast podmioty publiczne, przedsiębiorcy telekomunikacyjni, dostawcy usług zaufania oraz podmioty krytyczne wpisywane są z urzędu, czyli z automatu, przez ministra cyfryzacji. Nie będę już podawał może statystyk, to będzie w piśmie, które do państwa skieruję po podkomisji.

Jeśli chodzi o akty wykonawcze, procedowanych jest kilka obligatoryjnych, wynikających bezpośrednio z ustawy o KSC, czyli projekt rozporządzenia Rady Ministrów w sprawie progów uznania incydentu za poważny. Obecnie rozpatrywany jest przez Zespół do Spraw Programowania Prac Rządu. Oczywiście później, jeśli wejdzie już w proces legislacyjny, będzie konsultowany publicznie. Kolejny projekt rozporządzenia Rady Ministrów – w sprawie zakresu działania oraz trybu pracy Kolegium ds. Cyberbezpieczeństwa – podlega obecnie uzgodnieniom międzyresortowym i opiniowaniu do 3 sierpnia. Projekt tego rozporządzenia nie wpływa na sektor prywatny, jest to kwestia stricte wewnętrzna. Kolejny projekt rozporządzenia Rady Ministrów – w sprawie oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty KSC – w sierpniu zostanie skierowany wniosek do wykazu prac legislacyjnych i programowych Rady Ministrów. Również w sierpniu rozpoczną się konsultacje publiczne tego projektu. Będziemy rozsyłali te projekty, oczywiście wszystkie, które są konsultowane i dotyczą rynku, do ponad 90 podmiotów, izb gospodarczych rynku, tak aby uzyskać feedback i jak najbardziej się uzgodnić. Zgodnie z tym, co obiecywaliśmy, jak procedowaliśmy ustawę o KSC, że wszystkie projekty i wszystkie rozwiązania, które będziemy wdrażali, będziemy tak implementowali, aby rynek miał kluczową rolę, i tak aby ta ustawa naprawdę zapewniała bezpieczeństwo i wspierała przedsiębiorców we wdrażaniu tych rozwiązań. Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie – obecnie ten projekt jest konsultowany w ministerstwie. W sierpniu również będzie skierowany do prac legislacyjnych rząd. Zarządzenie pełnomocnika w sprawie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa zostało opublikowane 22 lipca. W sprawie trybu pracy jest to również akt wewnętrzny, wszedł w życie 24 lipca. O zestawieniu wymagań dokumentów normalizacyjnych może nie będę mówił, ale tutaj również będą konsultacje międzyresortowe. W ramach ministerstwa, tak jak też obiecywaliśmy, tak zrobiliśmy – na stronach ministerstwa jest specjalna zakładka Q&A, gdzie są pytania, odpowiedzi. Przedsiębiorcy, osoby zainteresowane, które zgłaszają wątpliwości, nie mają wiedzy, nie wiedzą, jak interpretować przepisy: każde to pytanie jest na tej stronie. Jest pytanie, jest odpowiedź, wyjaśnienie i procedury, jak postępować.

Uczestniczymy oczywiście również w formacie europejskim, jeśli chodzi o rewizję NIS2. Jesteśmy tu bardzo aktywni. Chcemy, aby nasze rozwiązania, które my wdrożyliśmy w sposób bardzo kompleksowy, również znalazły odzwierciedlenie w przepisach unijnych. Uczestniczymy w szeregu wydarzeń i organizujemy szereg wydarzeń informacyjnych, zarówno na konferencjach Cyfrowy Samorząd. Wspieramy samorządy, podmioty, które z naszej perspektywy są istotne, aby je informować. Dokonaliśmy również zmian organizacyjnych w Ministerstwie Cyfryzacji.

Powołaliśmy CSIRT Cyfra zgodnie z ustawą. Robimy również ankietę bezpieczeństwa łańcucha dostaw. 9 marca wysłałem do czterech operatorów sieci mobilnych, czyli Orange, P4, T-Mobile i Polkomtel, zaproszenie do współpracy merytorycznej nad opracowaniem ram bezpieczeństwa łańcucha dostaw. To jest kluczowe, jeśli chodzi o kwestie związane z bezpieczeństwem państwa. Współpracujemy również z Urzędem Zamówień Publicznych. Odbyliśmy spotkania zarówno na poziomie roboczym, jak i z panią prezes, jeśli chodzi o uelastycznienie przepisów dotyczących zamówień publicznych w zakresie cyberbezpieczeństwa, uwzględniając bezpieczeństwo z jednej strony, z drugiej strony uelastycznienie pewnych zapisów, tak aby te zakupy, których będziemy dokonywali – nie tylko my, ale również inne CSIRT sektorowe i podmioty – postawiły akcent głównie na bezpieczeństwo. Cena nie może być podstawowym wyznacznikiem, bo tu bezpieczeństwo ma pierwszeństwo, o czym wielokrotnie z państwem na ten temat rozmawialiśmy, między innymi przy tej ustawie.

Będziemy wprowadzali szereg różnych innych programów, jak choćby lokalne centra cyberbezpieczeństwa. To jest prawie 300 mln zł. Jest to program dedykowany do samorządów. Jak wiecie, 1,5 mld zł przeznaczyliśmy na „Cyberbezpieczny samorząd”, prawie 300 mln zł na „Cyberbezpieczny rząd”. Wprowadziliśmy program również de facto dla samorządów – „Cyberbezpieczny wodociąg” – za ponad 700 mln zł. Wszystkie podmioty, które się zgłosiły, podobnie jak przy „Cyberbezpiecznym samorządzie”, otrzymały to wsparcie. Prowadzimy również szeroko... Aha, jeszcze jedna ważna rzecz – będziemy budowali Centrum Cyberbezpieczeństwa w NASK. Ośrodek, który będzie wspierał również samorządy, ale będzie to chyba jeden z najnowocześniejszych i najlepszych ośrodków cyberbezpieczeństwa w Europie. Na to przeznaczyliśmy również kwotę ponad 360 mln zł. Będzie to na warszawskiej Pradze.

Prowadzimy również szeroko zakrojone akcje edukacyjne, zarówno przez Departament Cyberbezpieczeństwa, jak i Centrum Rozwoju Kompetencji Cyfrowych w ramach twardego cyber, KSC, EDU, SecureV. Część z państwa z tym programem mogła mieć do czynienia. Ja bym chciał, żeby wszyscy mieli do czynienia, bowiem szkolimy takie osoby jak posłowie, ministrowie, osoby ważne z punktu widzenia bezpieczeństwa państwa w administracji publicznej. Szkolimy również dzieci, nauczycieli, prowadzimy cyberlekcje 3.0. Tych działań naprawdę jest bardzo dużo. Prowadzimy również publikacje, zarówno my jako ministerstwo, jak i NASK, jeśli chodzi o poradniki z rekomendacjami, w jaki sposób się zachowywać, w jaki sposób wdrażać ustawę o KSC. Więc zgodnie z tym, o czym dyskutowaliśmy podczas procedowania ustawy, idziemy zgodnie z harmonogramem. Dotrzymujemy w tym zakresie również słowa, jeśli chodzi o stronę społeczną. Prowadzimy dialog, więc z mojej perspektywy zespół MC w 100% wywiązuje się z zobowiązań, również politycznych, podchodząc oczywiście merytorycznie i urzędniczo.

Dziękuję serdecznie. Jeśli są pytania, to oczywiście służymy odpowiedzią. Jeśli pan dyrektor by chciał coś dodać, to proszę bardzo.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Marcin Wysocki:

Bardzo dziękuję, panie ministrze. Panie przewodniczący, Wysoka Podkomisjo, jest dokładnie tak, jak powiedział w skrócie pan minister. O tych projektach oczywiście moglibyśmy mówić bardzo długo. Również w tym materiale, który zapowiedział pan minister, będzie szereg konkretnych danych, daty, liczby. Dziękuję.

Sekretarz stanu w MC Paweł Olszewski:

Tak, oczywiście niezwłocznie po podkomisji prześlemy państwu cały materiał. Nie chciałem zarzucać statystykami, liczbami, bo to jest ulotne, a jednak lepiej mieć to na papierze i móc się pochylić, mieć refleksję w tym zakresie.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dziękuję, panie ministrze; dziękuję, panie dyrektorze. Otwieram dyskusję. Pozwolę sobie jako pierwszy zabrać głos.

Podczas procedowania KSC w ramach Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii wielokrotnie mówiliśmy, że samo uchwalenie nawet najlepszych przepisów bez prawidłowego wdrożenia, bez zagwarantowania odpowiednich zasobów, kompetencji, ale też środków finansowych i zapewnienia czasu będzie połowicznym sukcesem. I tak ta ustawa została opracowana – w ramach również pracy na naszej Komisji wydłużyliśmy pewne terminy, jeżeli chodzi o dostosowanie tych przepisów ustawy do realiów naszej rzeczywistości. W ramach

podkomisji, która już została powołana, jednym z naszych głównych tutaj zdefiniowanych, zdiagnozowanych zadań będzie monitorowanie procesu wdrażania tych przepisów w życie. To jest duże wyzwanie.

Więc mam takie pierwsze pytanie do pana ministra, jak pan definiuje te największe wyzwania związane z wdrażaniem w ogóle KSC? Tutaj mówię nie tylko o przepisach, ale też stojącą za nimi koncepcją w ogóle ciągłego podnoszenia poziomu bezpieczeństwa w naszym kraju? Cieszę się, że te prace dotyczące wdrażania są prowadzone w dialogu ze stroną społeczną, bo to było też bardzo ważne. Ta ustawa była szeroko konsultowana, zanim weszła w życie. Rozmawialiśmy o niej też na Komisji w bardzo taki otwarty sposób. Więc z tej rozmowy podczas procedowania tego projektu ustawy wynikało, że rzeczywiście będzie i jest potrzeba tego ciągłego dialogu i dobrze, że ten dialog ze stroną społeczną się odbywa, ale też z tymi podmiotami, które dzisiaj się autodefiniują jako te, które muszą wdrażać pewne standardy związane z cyberbezpieczeństwem. Myślę, że tutaj też ta kampania informacyjna, wyciągnięta dłoń i gotowość ze strony resortu jest bardzo ważna i potrzebna. Też cieszy ta informacja o tym centrum z punktu widzenia samorządów, gdzie zagwarantowanie samych kompetencji jest naprawdę dużym wyzwaniem. O tym też wielokrotnie na Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii już mówiliśmy. Dobrze, żeby taki punkt, gdzie będą te kompetencje i będzie można czerpać wiedzę i czasami wyjaśniać pewne wątpliwości, będzie w niedalekiej przyszłości zorganizowany. Więc z mojej strony pytanie dotyczące tego, jak pan minister definiuje główne punkty, główne wyzwania związane jeszcze z wdrażaniem tej ustawy, to po pierwsze.

I po drugie, jaka refleksja płynie z tego dialogu, na razie wstępnego, bo jesteśmy na razie na początku wdrażania tych przepisów, w trakcie przygotowywania przepisów wykonawczych, ale też pewnych czynności, które muszą podejmować podmioty określone i sparametryzowane w tej ustawie? Jakie tutaj główne wyzwania resort cyfryzacji definiuje, jeżeli chodzi o ten proces? Może oddam od razu głos. I też zachęcam państwa posłów i stronę społeczną do udziału w tej dyskusji.

Sekretarz stanu w MC Paweł Olszewski:

Poza tym Centrum Cyberbezpieczeństwa, które nie tylko będzie obsługiwało i wspierało samorządy, ale również administrację rządową, tak jak powiedziałem wcześniej, jutro będziemy ogłaszali nabór, konkurs na lokalne centra cyberbezpieczeństwa.

To jest niezwykle istotny projekt z punktu widzenia samorządów, bowiem w tym konkursie będą mogły wystartować konsorcja samorządów, czyli nie pojedyncze gminy, ale chcemy doprowadzić do sytuacji, gdzie gminy wspólnie się porozumiewają i tworzą lokalne centra, żeby zabezpieczać swoją infrastrukturę i dostępność usług publicznych.

Jeśli chodzi, co jest najtrudniejsze – sami wiecie doskonale, jak pracowaliśmy nad tą ustawą, jak jest to złożona materia, zarówno od strony technicznej, jak i od strony takiej geopolitycznej, że tak to nazwę. Nie jest to prosta ustawa. Największy problem, który dostrzegamy, który ja dostrzegam osobiście – być może pan dyrektor to uszczegółowi – to są kwestie interpretacyjne. Co ustawodawca miał na myśli, stąd ten bieżący dialog ze stroną społeczną, stąd kwestie wyjaśniające. Departament na bieżąco, ciągle – może nie w trybie 24-godzinny, ale non stop – odpowiada na pytania. Więc z mojego punktu widzenia najtrudniejsze na chwilę obecną jest pokazywanie krok po kroku, co poszczególne podmioty powinny zrobić, jak się samoidentyfikować, jakie są kryteria, jaką ścieżkę muszą przejść, czyli te wszystkie kwestie takie, aby spełnić wymogi formalne i znaleźć się, bądź nie, w KSC.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dziękuję. O głos poprosiła pani przewodnicząca Wicha.

Posel Joanna Wicha (Lewica):

Tak, bardzo dziękuję za udzielenie głosu. Chciałabym zapytać o to, jak wdrażanie tych systemów cyberbezpieczeństwa przebiega w szpitalach i innych placówkach medycznych, POZ? Bo pamiętam, że na samym początku, kiedy ta propozycja się pojawiła i to, że będziemy uszczelniać nasze bezpieczeństwo, to taka dyskusja rozgorzała w przestrzeni publicznej, że szpitale nie będzie stać na wprowadzenie tych systemów, że one są drogie, że szpitale i tak są bardzo mocno zadłużone i że bardzo ciężko będzie dyrektorom szpitali wygospodarować środki. Drugi problem, jaki się pojawiał, to oczywiście osoby, które będą obsługiwały te systemy i że to też jest oczywiście zatrudnienie kolejnych osób, które nie są tanimi – w cudzysłowie – osobami

na rynku pracy, bo jednak muszą to być osoby, które są bardzo dobrze zorientowane, wykształcone i nadążające za tymi nowymi technologiami. Chciałabym zapytać, na jakim jesteśmy etapie, jeśli chodzi o ochronę zdrowia? Dziękuję.

Sekretarz stanu w MC Paweł Olszewski:

Jeśli chodzi o ochronę zdrowia i inne CSIRT sektorowe, jak państwo doskonale wie, w tej ustawie powołaliśmy nowe CSIRT sektorowe.

Są na to środki. Zawsze potrzeby są nieograniczone, środki są w jakimś sensie ograniczone, więc kwestią służby zdrowia zajmuje się CSIRT sektorowy. My natomiast jesteśmy po posiedzeniu Kolegium do Spraw Cyberbezpieczeństwa. Ja również zapowiedziałem, że będziemy się zwracać najpierw z pismem, z prośbą o przedstawienie przez poszczególne CSIRT sektorowe, w jaki sposób i na jakim etapie są, czego im brakuje, tak abyśmy mieli wiedzę, abyśmy mieli tę fotografię rzeczywistości, w jaki sposób ewentualnie możemy pomóc i w jaki sposób wesprzeć poszczególne CSIRT sektorowe. Na wrzesień planujemy spotkanie z poszczególnymi CSIRT, więc w tym zakresie staramy się pełnić rolę koordynacyjno-doradczą i to jest w procesie.

Jeśli chodzi o specjalistów, to jak pani poseł przewodnicząca doskonale wie, jest fundusz cyberbezpieczeństwa, czyli fundusz na dodatki teleinformatyczne. Obecnie projektowane są założenia do budżetu. Walczymy o jak największe środki, bowiem zdajemy sobie sprawę, że specjaliści od cyberbezpieczeństwa są bardzo poszukiwani na rynku, w szczególności biorąc pod uwagę sytuację geopolityczną. Ataki cyber, zarówno te o charakterze politycznym, przeprowadzane przez służby specjalne obcych nam i wrogich krajów, jak i ataki o charakterze fraudowym, biznesowym, ukierunkowane na firmy, więc my jako administracja rządowa, administracja publiczna musimy mieć wysoko wykwalifikowanych i dobrze opłacanych specjalistów. Taka była intencja powołania funduszu i dzisiaj walczymy o jak największe środki w tym zakresie.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dziękuję, panie ministrze. Pan przewodniczący Osmalak.

Poseł Łukasz Osmalak (Polska2050):

Dziękuję bardzo, panie przewodniczący. Panie ministrze, pani przewodnicząca już w pewnym sensie przed chwilą powiedziała o tym, o czym w jakimś stopniu ja też chciałem powiedzieć i na co chciałem zwrócić uwagę. Myślę, że bardzo ważne w aspekcie cyberbezpieczeństwa, jeśli chodzi o sytuację geopolityczną, o to, co się dzieje dzisiaj w całym kraju, jest kwestia współpracy z samorządami. To znaczy, o ile część instytucji, o których my rozmawiamy, i jeżeli patrzymy na cyberbezpieczeństwo z poziomu kraju, to oczywiście w dużej mierze to są instytucje, które są instytucjami takimi ogólnokrajowymi i które współpracują bezpośrednio z ministerstwami na jakimś poziomie, ale myślę, że bardzo wiele zagrożeń to będą zagrożenia, które będą się też pojawiały właśnie na poziomie samorządów. Stricte samorządów jako jednostek samorządowych i jednostek, które są tym samorządom podległe. Wydaje mi się, że tutaj to, co jest bardzo ważne, na co musimy w sposób szczególny zwrócić uwagę, to kompetencje osób, które będą pracowały w samorządach, które będą odpowiedzialne za te procesy. Dlatego, że jeżeli tam będą pracować osoby, które będą kompetentne, które będą dobrze wyszkolone, które będą miały wiedzę, to one będą w stanie dobrze o to wszystko zadbać. Wiem, że z jednej strony mówię coś, co jest zupełnie oczywiste, natomiast wydaje mi się, że my musimy po prostu położyć duży nacisk na to, żeby te osoby wesprzeć. Bo to, że oni są bardzo pożądanymi na rynku, to wszyscy doskonale o tym wiemy, bo każdy specjalista, między innymi od cyberbezpieczeństwa, bez problemu znajdzie pracę na rynku i to pracę za dobre pieniądze. Więc wydaje mi się, że my też musimy się w dużej mierze skupić na tym, żeby te osoby, które już pracują w samorządach w branży IT, dostały jak największe wsparcie właśnie merytoryczne, szkolenia, ale też narzędzia, i co za tym idzie – oczywiście pieniądze. Dziękuję bardzo.

Przewodniczący poseł Paweł Bliźniuk (KO):

Proszę bardzo, panie ministrze.

Sekretarz stanu w MC Paweł Olszewski:

W pełni się zgadzam. Już jakby ten wątek zająłem, że realizujemy szereg działań zmierzających do wzmocnienia nie tylko – w cudzysłowie – sprzętowego samorządów, ale również kompetencyjnego. Lokalne centra cyberbezpieczeństwa, „Cyberbezpieczny Samorząd”, „Cyberbezpieczny Wodociąg”. Na jesieni również będziemy z jednej strony edukowali i szkolili

podmioty i osoby w samorządach, które będą odpowiadały za cyberbezpieczeństwo w ramach ustawy, ale również przez ten drugi departament, czyli Centrum Rozwoju Kompetencji Cyfrowych, będziemy prowadzili dla samorządowców szkolenia nie tylko z cyberbezpieczeństwa. To będzie jeden z komponentów, ale również dezinformacji, higieny cyfrowej, kwestii związanych bezpośrednio z tym, w jaki sposób poruszać się bezpiecznie w środowisku internetowym. Więc te działania koordynujemy, one się wzajemnie uzupełniają, więc sam sprzęt, samo oprogramowanie nie wystarczy. Zdajemy sobie z tego sprawę, stąd liczne projekty i programy o charakterze szkoleniowym i edukacyjnym, bo na koniec dnia w każdym systemie to człowiek jest najważniejszy, jego zdolności, umiejętności i potencjalne słabości, stąd też duży nacisk na to, aby w tym zakresie również wspierać samorządy. Ale nie tylko samorządy, bowiem prowadzimy też liczne i będziemy prowadzili szkolenia dla mikro, małych, średnich przedsiębiorców, co jest niezwykle istotne, bowiem oni są bardzo często mega ambitni, ale potrzebują wsparcia, więc w tym zakresie również działaliśmy i będziemy działali. Staramy się w ramach możliwości finansowych objąć w zasadzie wszystkie grupy społeczne i podmioty, które mają wpływ na szeroko pojęte bezpieczeństwo, w tym cyberbezpieczeństwo i bezpieczeństwo informacyjne, walkę z dezinformacją etc.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dziękuję. Czy są jakieś pytania też ze strony naszych serdecznych gości? Proszę bardzo, pani profesor. Proszę się przedstawić do protokołu.

**Członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKApw
Joanna Karczevska:**

Tak, oczywiście – nazywam się Joanna Karczevska, jestem absolwentką Wydziału Elektroniki Politechniki Warszawskiej, zajmuję się cyberbezpieczeństwem, bezpieczeństwem informacji, ochroną danych osobowych.

Obecnie jestem w trakcie wsparcia dla jednostki samorządowej, a konkretnie dla placówki oświatowej, która jest w likwidacji. I cały proces cyfrowej likwidacji placówki oświatowej obnaża wszystkie – nawet niespodziewane – luki w cyberbezpieczeństwie. Mówię tu zarówno o przepisach, umowach, jak i różnych procedurach. Tu okazuje się, że kompetencje cyfrowe niewiele pomagają, wręcz przeciwnie, nawet stanowią przeszkodę, bo każdemu po drugiej stronie wydaje się, że już tutaj sprawa jest załatwiona, a okazuje się, że nie. Mówię, to jest począwszy od ministerstw, po różne firmy i rozwiązania własne. Ponad 30 już w tej chwili systemów, z których musimy zniknąć. To jest coś strasznego, mówiłam o tym już wczoraj.

Natomiast w kwestii ustawy chciałabym zwrócić uwagę na dwa problemy, które dostrzegam. Jeden dotyczy szkoleń dla kierowników podmiotu – to jest art. 8e. Kierownik podmiotu raz w roku kalendarzowym przechodzi szkolenie i szkolenie musi być udokumentowane – już znalazłam pierwsze oferty takich szkoleń i muszę powiedzieć, że włos na głowie się jeży, szczególnie jeśli widzę, że ma to być szkolenie zdalne. To już widzę, jak cały dzień komputer jest włączony, szkolenie leci, a na przykład wójt, burmistrz, starosta – skoro mówimy o samorządach – i tak ma co robić. Pamiętajmy, że zbliża się kolejna kampania wyborcza i będzie od tej strony dużo czasu trzeba będzie poświęcić na inne działania, więc jeżeli mogę doradzić... Proszę?

Poseł Patryk Gabriel (KO):

Samorządowcy w przyszłym roku nie mają.

**Członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKApw
Joanna Karczevska:**

Nie? Ale jest to polityka. Mówię, może nie sami samorządowcy, ale trzeba to uwzględnić, więc ja proponuję i zalecam śledzenie bacznie oferty szkoleniowej. Znalazłam nawet szkolenie dwudniowe. Nie wyobrażam sobie, żeby kierownik bardzo poważnego podmiotu, typu bank czy inna duża firma, dwa dni siedział i na dodatek, jak patrzę na zakres szkolenia, to jest dość zastanawiający. Tak się składa, że już w 2015 r. staraliśmy się pomóc właśnie osobom kierującym i wraz z dwoma osobami ze stowarzyszenia ISACA przetłumaczyłam materiał amerykański, który zawierał sześć podstawowych pytań, które każdy zarząd powinien zadać swoim komórkom, nie tylko informatycznym, ale generalnie pytań, które dotyczą właśnie cyberbezpieczeństwa. Sześć pytań – można na nie odpowiedzieć, powiedzmy, w ciągu godziny, a nie siedzieć jeden lub dwa dni i słuchać, jakie są zagrożenia ze strony sztucznej inteligencji chociażby, ponieważ kierownicy jednostek, podmiotów, czyli osoby, które mają rządzić, a nie zarządzać cyberbezpieczeństwem, powinny mieć wskazane, jak zrobić to; właśnie jakie pytania zadawać i jak

interpretować wyniki. Oni nie będą siedzieć razem z cyberbezpiecznikiem i ustawiać systemów. Więc radzę uważnie śledzić, szczególnie NASK, właśnie dwudniowe szkolenie za 3900 zł netto, naprawdę, i skorzystać też z metodyki, w której opracowaniu uczestniczyłam, czyli metodyki właśnie rządzenia i zarządzania systemami informatycznymi, całą informatyką w firmie. Tam są też elementy cyberbezpieczeństwa. To jest do wykorzystania, ale należy się skupić przede wszystkim na rządzeniu cyberbezpieczeństwem. Wiem to z praktyki, bo zarówno szkoliłam samorządy, przeprowadzałam audyty w samorządach.

Przewodniczący poseł Paweł Bliźniuk (KO):

Proszę zmierzać do konkluzji, bo chciałbym...

**Członek Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKApw
Joanna Karczevska:**

Dobrze, oczywiście. Druga kwestia, to chciałam spytać, bo w ustawie o KSC w art. 62 są wymienione wskaźniki, że wskaźniki zostaną opracowane z udziałem organów administracji publicznej itd. Czy takie wskaźniki już są dostępne? Ponieważ sprawdzałam strategię cyberbezpieczeństwa i tam są tylko mierniki, nie ma wskaźników.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dobrze, mamy dwa pytania o wskaźniki z artykułu wspomnianego przez panią plus szkolenia. Ja tylko, jeszcze zanim tutaj ministerstwo udzieli odpowiedzi, powiem też ze swojej praktyki, że jeżeli chodzi o administrację samorządową, to bardzo ważna, jeżeli chodzi o kierownictwo, jest sama świadomość zagrożeń. Stąd też szkolenia wpisane do ustawy mają tę wartość, że powtarzane co rok też będą budowały świadomość. Ta świadomość pomaga budować kompetencje, ale też ułatwia osobom zajmującym się cyberbezpieczeństwem w takich jednostkach podejmowanie dobrych decyzji przez tych, którzy tymi jednostkami kierują. Mamy wszyscy też wiedzę i tę świadomość, jak funkcjonuje samorząd terytorialny, jak wieloma rzeczami taki kierownik jednostki samorządu musi się zajmować na co dzień. Natomiast jeżeli ta świadomość się pojawia, i też świadomość ryzyk, zagrożeń i odpowiedzialności tej osoby, to wtedy łatwiej się pewne rzeczy egzekwuje tym, którzy odpowiadają już wprost służbowo za ten obszar. Więc tutaj tylko odpowiedź jeszcze może dotycząca tych wskaźników i czy są jeszcze jakieś zgłoszenia, to za chwilę. Pan minister, może pan dyrektor?

Sekretarz stanu w MC Paweł Olszewski:

Jeśli chodzi o wskaźniki, to na bieżąco analizujemy, oceniamy w ramach pełnomocnika do spraw cyberbezpieczeństwa, jak i Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, i na bieżąco szacujemy ryzyko.

Natomiast jeśli chodzi o ten pierwotny i pierwszy wywód pani profesor, która skupiła się na jakiejś komercyjnej części szkoleń, które są oferowane na rynku – tak jak ze szkołami, jedne są lepsze, drugie są gorsze; jeden nauczyciel jest lepszy, drugi gorszy; jeden profesor jest lepszy, drugi gorszy, więc nie ma obowiązku dla podmiotów, aby korzystać z komercyjnych szkoleń. Po pierwsze, w ramach ministerstwa nasi specjaliści oferują bezpłatne szkolenia dla podmiotów, które wchodzi w skład KSC, więc nie trzeba wydawać pieniędzy, a wystarczy się zwrócić do ministerstwa. Gwarantujemy profesjonalizm, gwarantujemy jakość i gwarantujemy bezpłatność.

Zastępca dyrektora departamentu MC Marcin Wysocki:

Panie przewodniczący, Wysoka Podkomisjo, z konkretów – 30 września, po wakacjach szkolenie z cyberhigieny, świetni eksperci z NASK i dokładnie tak, jak powiedział pan minister, podmioty KSC przyjmują zaproszenie. My tam bijemy rekordy, to znaczy w tych szkoleniach prowadzonych przez ekspertów NASK, naszych partnerów w cyberbezpieczeństwie udział biorą setki i – proszę państwa, nie mylę się – tysiące uczestników online, oczywiście w formule bezpłatnej. Przepraszam za to wtrącenie, panie ministrze, dziękuję.

Sekretarz stanu w MC Paweł Olszewski:

Nie ma problemu. Pan dyrektor mnie zwolnił z kontynuowania odpowiedzi.

Przewodniczący poseł Paweł Bliźniuk (KO):

Dobrze, czyli wszyscy chętni zanotowali termin. Moja prośba o przesłanie mailowo informacji do podkomisji, to też zainteresowanym prześlemy...

Sekretarz stanu w MC Paweł Olszewski:

Tak, prześlemy. Możemy. Też zbierzemy...

Przewodniczący poseł Paweł Bliźniuk (KO):

...i fakt, że są bezpłatne te szkolenia, wypełniające tę dyspozycję z przepisu ustawy – myślę, że również warto o tym głośno mówić, że tutaj po prostu można korzystać z wiedzy i kompetencji tych, którzy naprawdę na tym się znają, więc to jest bardzo ważna informacja. Dlatego też rozmawiamy dzisiaj o tym na podkomisji, bo dostosowywanie czy też wdrażanie przepisów to nie tylko papierologia, ale też kwestie organizacyjne. Jak widać, ministerstwo zapewnia też te wątki związane z budowaniem kompetencji w jednostkach czy podmiotach objętych KSC. To bardzo ważne, bo to było też zobowiązanie z okresu, kiedy nad tę ustawą pracowaliśmy również na poziomie Komisji czy też na poziomie samego Sejmu.

Czy są jeszcze jakieś inne wnioski o zabranie głosu, czy głosy w dyskusji, pytania z państwa strony? Mówię tu o stronie społecznej. Czy ze strony państwa posłów? Nie ma. Zobowiązałem się też do tego, że podkomisja będzie bardzo rzeczowo i tak dynamicznie prowadzona, więc nie będziemy przedłużać. W związku z tym zamykam dyskusję.

Na tym wyczerpaliśmy porządek dzienny posiedzenia. Dziękuję wszystkim państwu za obecność i udział w dyskusji. Zamykam posiedzenie podkomisji. Dziękuję.